ระบบตรวจสอบลายนิ้วมือแบบอัตโนมัติเพื่อประมวลผลบนสมาร์ตคาร์ด

นายชัยรัตน์ องค์วิศิษฐ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2548
ISBN 974-17-3637-1

AUTOMATIC FINGERPRINT VERIFICATION SYSTEM ON SMART CARD

Mr. Chairat Onkvisit

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering Program in Computer Engineering

Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University

Academic Year 2005

ISBN 974-17-3637-1

หัวข้อวิทยานิพนธ์	ระบบตรวจสอบลายนิ้วมือแบบอัตโนมัติเพื่อประมวลผลบนสมาร์ตคาร์ด
โดย	นายชัยรัตน์ องค์วิศิษฐ์
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร.สาธิต วงศ์ประทีป

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ชูชีพ ฉิมวงษ์)

..... อาจารย์ที่ปรึกษา
(รองศาสตราจารย์ ดร.สาธิต วงศ์ประทีป)

..... กรรมการ
(อาจารย์ ดร.อาทิตย์ ทองทักษ์)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.เกรียงไกร ปอแก้ว)

นายชัยรัตน์ องค์วิศิษฐ์ : ระบบตรวจสอบลายนิ้วมือแบบอัตโนมัติเพื่อประมวลผลบนสมาร์ตคาร์ด. (AUTOMATIC FINGERPRINT VERIFICATION SYSTEM ON SMART CARD) อ.ที่ปรึกษา: รศ.ดร.สาธิต วงศ์ประทีป, 130 หน้า. ISBN 974-17-3637-1.

ในปัจจุบันระบบตรวจสอบลายนิ้วมือได้ถูกนำมาใช้งานกันอย่างแพร่หลาย การนำระบบตรวจสอบลายนิ้วมือไปประยุกต์ใช้งานร่วมกับสมาร์ตคาร์ด โดยออกแบบให้สมาร์ตคาร์ดทำการประมวลผลขั้นตอนการเปรียบเทียบลายนิ้วมือเอง จะทำให้ระบบโดยรวมมีความปลอดภัยสูง เนื่องจากในการตรวจสอบลายนิ้วมือ จะทำโดยส่งข้อมูลลายนิ้วมือที่ต้องการตรวจสอบไปตรวจสอบภายในสมาร์ตคาร์ด ทำให้ไม่มีการจัดส่งแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำของสมาร์ตคาร์ดออกมาภายนอก จึงทำให้ปลอดภัยต่อการถูกดักจับหรือการปลอมแปลงได้

วิทยานิพนธ์นี้นำเสนอการพัฒนาขั้นตอนการเปรียบเทียบลายนิ้วมือ (Fingerprint Matching) เพื่อให้สามารถประมวลผลบนสมาร์ตคาร์ดแบบ 8 บิต ที่มีขนาดหน่วยความจำชั่วคราวเล็กกว่าข้อมูลลายนิ้วมือทั้งหมดได้ และลดเวลาที่ใช้ในการประมวลผลลง โดยเมื่อข้อมูลภาพลายนิ้วมือที่ต้องการตรวจสอบได้ผ่านขั้นตอนการทำ Feature Extraction แล้ว จะถูกแบ่งออกเป็น 3 ส่วนเท่าๆ กัน เพื่อส่งไปเปรียบเทียบกับแม่แบบลายนิ้วมือที่เก็บไว้ภายในสมาร์ตคาร์ด โดยจะเริ่มต้นเปรียบเทียบจากส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือ (Minutiae) มากที่สุด ไปยังน้อยที่สุด และได้ออกแบบให้มีค่าขีดแบ่ง (Threshold) ย่อยๆ ตามแต่ละขั้นตอนการทำงาน โดยในขั้นตอนแรก และขั้นตอนที่สอง จะมีการใช้ค่าขีดแบ่งระดับบน (Upper Threshold) และค่าขีดแบ่งระดับล่าง (Lower Threshold) เพื่อพิจารณาลายนิ้วมือว่าเป็นของบุคคลเดียวกันหรือต่างบุคคล หรือควรจะนำข้อมูลภาพลายนิ้วมือส่วนอื่นมาประมวลผลเพิ่มเติมต่อไป โดยที่ค่าขีดแบ่งระดับบน จะช่วยลดเวลาในบางกรณีของภาพลายนิ้วมือที่รับเข้ามาเป็นบุคคลเดียวกัน และค่าขีดแบ่งระดับล่าง จะช่วยลดเวลาในกรณีของภาพลายนิ้วมือที่รับเข้ามาต่างบุคคลกันมีตำแหน่ง และชนิดของจุดสำคัญบนเส้นลายนิ้วมือ ที่แตกต่างกันระหว่างภาพที่รับเข้ามากับแม่แบบลายนิ้วมือ

ภาควิชา.... วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต.....

สาขาวิชา....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่ออาจารย์ที่ปรึกษา.....

ปีการศึกษา .....2548.....

4570282721 : MAJOR Computer Engineering

KEY WORD: FINGERPRINT MATCHING / SMART CARD / MINUTIAE / FINGERPRINT VERIFICATION

CHAIRAT ONKVISIT : AUTOMATIC FINGERPRINT VERIFICATION SYSTEM ON SMART CARD. THESIS ADVISOR : ASSOC. PROF. DR. SARTID VONGPRADHIP 130 pp. ISBN 974-17-3637-1.

At present, fingerprint verification system has gained increasingly broader applications. The verification can be processed on smart cards which contribute to better security for the system. By transmitting data to be verified onto smartcard, fingerprint template stored inside the smartcard can then be protected from being leaked outside to avoid detection or counterfeit risks.

This study has been designed to develop Fingerprint Matching Algorithm for processing directly on 8-bit smartcard having Random Access Memory's capacity less than the entire fingerprint data. This approach seeks to classify fingerprint data already undergone Feature Extraction by dividing them into 3 equal portions for comparison with the fingerprint template stored inside the smartcard, by comparing them with the highest and lowest threshold values. These values are applied to determine whether fingerprint data belong to the same or otherwise different person, and whether additional fingerprint data are required for further verification. The upper one helps lessen verification time should incoming fingerprint images belong to the same person, whereas the lower one helps lessen such time should they belong to different persons having different type and position of minutiae between incoming images and fingerprint template.

Department..... Computer Engineering.... Student's signature.....

Field of study.... Computer Engineering.... Advisor's signature.....

Academic year .....2005.....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี เนื่องมาจากความช่วยเหลือ และความกรุณาของคณาจารย์ทุกท่าน โดยเฉพาะอย่างยิ่งรองศาสตราจารย์ ดร. สาธิต วงศ์ประทีป ซึ่งได้ให้ความกรุณารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ และให้คำแนะนำตั้งแต่หัวข้อการทำวิทยานิพนธ์ ตลอดจนแนวคิด, คำชี้แนะ, ข้อควรปรับปรุงของระบบที่ได้พัฒนาขึ้น และข้อแนะนำสำหรับผลการทดลอง ซึ่งเป็นสิ่งสำคัญอย่างยิ่งสำหรับการทำวิทยานิพนธ์ฉบับนี้

ขอขอบพระคุณ บิดา มารดา รวมทั้งครอบครัวของข้าพเจ้าที่ให้การสนับสนุนให้ความช่วยเหลือในทุกๆ ด้าน และให้กำลังใจโดยเสมอ

ขอขอบคุณน้องๆ นิสิตปริญญาตรี, เพื่อนๆ พี่ๆ นิสิตปริญญาโททุกท่าน โดยเฉพาะอย่างยิ่ง นายภานุพันธ์ นันทนาวุฒิ, นางสาว เบญจวรรณ ตระบันพฤกษ์ ที่ให้ความกรุณาชี้แนะสำหรับข้อสงสัยต่างๆ ในระหว่างการจัดทำวิทยานิพนธ์ และให้ความช่วยเหลือในการตรวจทานความถูกต้อง รูปแบบของเอกสารต่างๆ พร้อมทั้งให้ข้อแนะนำอันเป็นประโยชน์อย่างยิ่งในการปรับปรุงระบบที่ได้พัฒนาขึ้น และวิทยานิพนธ์ฉบับนี้

ขอขอบคุณ นายชยวัชน์ วงศกิตติรักษ์ สำหรับคำแนะนำ และความช่วยเหลือต่างๆ ที่จำเป็นอย่างยิ่ง ในระหว่างการพัฒนาโปรแกรมตรวจสอบลายนิ้วมือ

ขอขอบคุณภาควิชาวิศวกรรมคอมพิวเตอร์ และเจ้าหน้าที่ภายในภาควิชาทุกๆ ท่าน ที่ให้ความกรุณา และให้ความช่วยเหลืออย่างดียิ่ง ในการตอบข้อสงสัยต่างๆ ให้คำแนะนำอันเป็นประโยชน์ และออกเอกสารที่จำเป็นต่างๆ ที่จำเป็น ในระหว่างการจัดทำวิทยานิพนธ์ของข้าพเจ้า ตลอดจนอุปกรณ์ สถานที่

ขอขอบคุณอาสาสมัครในการเก็บข้อมูลลายนิ้วมือทุกท่าน ที่ให้ความกรุณาสละเวลาอันมีค่ายิ่ง ในการเก็บข้อมูลลายนิ้วมือ เพื่อใช้ในวิทยานิพนธ์ฉบับนี้

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง
บทคัดย่อภาษาอังกฤษ ..... จ
กิตติกรรมประกาศ ..... ฉ
สารบัญ ..... ช
สารบัญภาพ ..... ญ
สารบัญตาราง ..... ฒ
บทที่
1 บทนำ 1
1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์ 5
1.3 ขอบเขตงานวิจัย 5
1.4 ขั้นตอนและวิธีดำเนินงานวิจัย 6
1.5 ประโยชน์ที่คาดว่าจะได้รับ 7
1.6 ลำดับการจัดเรียงเนื้อหาในวิทยานิพนธ์ 8
1.7 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์ 8
2 ทฤษฎีเบื้องต้นและงานวิจัยที่เกี่ยวข้อง 9
2.1 ความรู้และทฤษฎีเบื้องต้น 9
2.1.1 ระบบตรวจสอบลายนิ้วมือ (Fingerprint Matching) 9
2.1.2 รูปแบบของลายนิ้วมือ 10
2.1.3 จุดสำคัญบนเส้นลายนิ้วมือ (Minutiae) 14
2.1.4 วิธีการที่ใช้ในการตรวจสอบลายนิ้วมือ 16
2.1.5 สมาร์ตคาร์ด (บัตรเก่ง) 17
2.1.6 การเชื่อมต่อของสมาร์ตคาร์ด 22
2.2 งานวิจัยที่เกี่ยวข้อง 26
2.2.1 Collaborative Fingerprint Authentication by Smartcard and a Trusted Host 26
2.2.2 Moving-Window Algorithm For Fast Fingerprint Verification 27
2.2.3 Logical Templates for Feature Extraction in Fingerprint Images 28

บทที่ หน้า

2.2.4 การประมวลลายพิมพ์นิ้วมือเบื้องต้นสำหรับระบบตรวจพิสูจน์ลายนิ้วมือ อัตโนมัติ 32
2.2.5 Adaptive image normalisation based in block processing for enhancement of fingerprint image 35
3 ระบบตรวจสอบลายนิ้วมือที่ได้พัฒนาขึ้นใหม่ 40
3.1 การประมวลผลภาพเบื้องต้น (Image preprocessing) 41
3.1.1 การทำให้เรียบและการลดสัญญาณรบกวน (Smoothing & Noise reduction) ... 41
3.1.2 การปรับ Normalisation และความแปรปรวนของภาพ (Variant) 41
3.1.3 การเลือกส่วนของภาพที่ใช้ในการประมวลผล (Select region of interest) 42
3.1.4 การปรับค่าฮีสโตแกรมของภาพลายนิ้วมือ (Histogram Equalization) 42
3.1.5 การแปลงเป็นภาพสองระดับ (Binarization) 44
3.1.6 การหาทิศทางและการปรับแต่งเส้นลายนิ้วมือ 44
3.1.7 การทำลายเส้นให้บาง 47
3.2 การค้นหาลักษณะสำคัญ (Feature Extraction) 47
3.3 การเปรียบเทียบลักษณะสำคัญ (Feature Matching) 50
3.3.1 แนวคิดและหลักการทำงาน 51
3.3.2 วิธีการที่ใช้ในการเปรียบเทียบข้อมูลจุดสำคัญบนเส้นลายนิ้วมือของแต่ละส่วนย่อย 55
3.3.3 ขั้นตอนการเปรียบเทียบลายนิ้วมือระหว่างโฮสต์กับสมาร์ตคาร์ด 57
3.3.4 ขั้นตอนการทำงานของระบบตรวจสอบลายนิ้วมือ 59
3.4 การเพิ่มความปลอดภัยของการเก็บแม่แบบลายนิ้วมือบนสมาร์ตคาร์ด 65
4 การออกแบบเครื่องอ่าน/เขียนสมาร์ตคาร์ด (Smartcard Reader/Writer) 67
4.1 รูปแบบการเชื่อมต่อระหว่างเครื่องอ่าน/เขียนสมาร์ตคาร์ด กับเครื่องคอมพิวเตอร์ 68
4.2 ความถี่สัญญาณนาฬิกาที่ใช้กับเครื่องอ่าน/เขียนสมาร์ตคาร์ด 69
4.3 IC Voltage Regulator ที่ใช้ในเครื่องอ่าน/เขียนสมาร์ตคาร์ด 73
4.4 การออกแบบวงจรเชื่อมต่อระหว่างไอซี MAX232 กับสมาร์ตคาร์ด 76
4.5 วงจรตรวจสอบว่ามีสมาร์ตคาร์ดเสียบเข้ากับเครื่องอ่าน/เขียนสมาร์ตคาร์ดหรือไม่ (Card Detect Switch) 78

บทที่ หน้า

5 การทดลอง 80
5.1 หลักการทำงานของเครื่องอ่านลายนิ้วมือแบบใช้แสงชนิด Frustrated Total Internal Reflection (FTIR) 80
5.2 เครื่องอ่านลายนิ้วมือที่ใช้ในการเก็บข้อมูล 82
5.2.1 เครื่องอ่านลายนิ้วมือแบบแสง ชนิด FTIR รุ่น U.are.U 2000 82
5.2.2 เครื่องอ่านลายนิ้วมือแบบแสง ชนิด FTIR รุ่น U.are.U 4000B 83
5.3 การเก็บภาพลายนิ้วมือจากอาสาสมัคร 83
5.3.1 ปัญหาที่พบจากเก็บข้อมูลภาพลายนิ้วมือจากอาสาสมัคร 84
5.4 สมาร์ตคาร์ดที่ใช้ในงานวิจัย 86
5.4.1 คุณสมบัติหลักของไมโครคอนโทรลเลอร์ PIC16F876 86
5.4.2 การโปรแกรมข้อมูลของโปรแกรมเปรียบเทียบลายนิ้วมือลงบนสมาร์ตคาร์ด 86
5.5 การเพิ่มความเร็วในการประมวลผลของสมาร์ตคาร์ดโดยเพิ่มความถี่สัญญาณนาฬิกา . 88
5.6 ผลการทดลอง 89
6 สรุปผลการวิจัยและข้อเสนอแนะ 106
6.1 สรุปผลการวิจัย 106
6.2 ข้อเสนอแนะ 108
รายการอ้างอิง 109
ภาคผนวก 111
ก ตัวอย่างภาพลายนิ้วมือบางส่วนที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือ U.are.U 4000B 112
ข ตัวอย่างภาพลายนิ้วมือบางส่วนที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือ U.are.U 2000 121
ประวัติผู้เขียนวิทยานิพนธ์ 130

สารบัญภาพ

ภาพประกอบ หน้า

รูปที่ 1.1 จุดเด่นต่างๆ ของระบบตรวจสอบลายนิ้วมือ เปรียบเทียบกับระบบตรวจสอบโดยใช้อวัยวะหรือลักษณะสำคัญอื่นๆ 2

รูปที่ 1.2 ความแพร่หลายของการนำระบบยืนยันตัวบุคคลมาใช้งานร่วมกับสมาร์ตคาร์ดเพื่อใช้เป็นบัตรประจำตัวบุคคลในประเทศต่างๆ 2

รูปที่ 2.1 ภาพลายนิ้วมือแบบโค้งราบ 10

รูปที่ 2.2 ภาพลายนิ้วมือแบบโค้งกระโจม 11

รูปที่ 2.3 ภาพลายนิ้วมือแบบมัดหวายปัดขวา 11

รูปที่ 2.4 ภาพลายนิ้วมือแบบมัดหวายปัดซ้าย 12

รูปที่ 2.5 ภาพลายนิ้วมือแบบมัดหวายคู่ 12

รูปที่ 2.6 ภาพลายนิ้วมือแบบก้นหอยธรรมดา 13

รูปที่ 2.7 ภาพลายนิ้วมือแบบก้นหอยกระเป๋ากลางปัดขวา 13

รูปที่ 2.8 ภาพลายนิ้วมือแบบก้นหอยกระเป๋าข้างปัดซ้าย 14

รูปที่ 2.9 ภาพลายนิ้วมือแบบซับซ้อน 14

รูปที่ 2.10 จุดสำคัญบนเส้นลายนิ้วมือ (Minutiae) พื้นฐาน 15

รูปที่ 2.11 ลักษณะต่าง ๆ ที่มีปรากฏบนเส้นลายนิ้วมือ 15

รูปที่ 2.12 จุดสำคัญบนเส้นลายนิ้วมือ 2 ชนิดหลัก 17

รูปที่ 2.13 ด้านที่มีขาสัญญาณของบัตรโทรศัพท์ชนิดที่เป็นสมาร์ตคาร์ดแบบมีหน่วยความจำเพียงอย่างเดียว 18

รูปที่ 2.14 ด้านที่ไม่มีขาสัญญาณของบัตรโทรศัพท์ชนิดที่เป็นสมาร์ตคาร์ดแบบมีหน่วยความจำเพียงอย่างเดียว 18

รูปที่ 2.15 ด้านที่มีขาสัญญาณของซิมการ์ด 20

รูปที่ 2.16 ด้านที่ไม่มีขาสัญญาณของซิมการ์ด 20

ภาพประกอบ หน้า

รูปที่ 2.17 ด้านที่มีขาสัญญาณ (ด้านหน้า) ของบัตรประชาชนแบบสมาร์ตคาร์ด 20
รูปที่ 2.18 ด้านที่ไม่มีขาสัญญาณ (ด้านหลัง) ของบัตรประชาชนแบบสมาร์ตคาร์ด 21
รูปที่ 2.19 ด้านที่มีขาสัญญาณของสมาร์ตคาร์ดที่ใช้ในระบบถอดรหัสสัญญาณของระบบโทรทัศน์บอกรับสมาชิก 21
รูปที่ 2.20 ด้านที่ไม่มีขาสัญญาณของสมาร์ตคาร์ดที่ใช้ในระบบถอดรหัสสัญญาณของระบบโทรทัศน์บอกรับสมาชิก 21
รูปที่ 2.21 ด้านหน้าของสมาร์ตคาร์ดแบบไม่มีหน้าสัมผัส..... 22
รูปที่ 2.22 ด้านหน้าของสมาร์ตคาร์ดแบบมีหน้าสัมผัส 22
รูปที่ 2.23 ข้อกำหนดบางส่วนตามมาตรฐาน ISO 7816-1..... 23
รูปที่ 2.24 ข้อกำหนดบางส่วนตามมาตรฐาน ISO 7816-2 24
รูปที่ 2.25 ข้อกำหนดต่างๆ ตามมาตรฐาน AFNOR เปรียบเทียบกับมาตรฐาน ISO 7816 25
รูปที่ 2.26 Logical template..... 30
รูปที่ 2.27 ฟิลเตอร์แบบมัธยฐาน ขนาด 3×3 33
รูปที่ 2.28 จุดแบ่งของค่าขีดแบ่งที่เหมาะสมเมื่อพิจารณาจากเส้นโค้งความถี่ 34
รูปที่ 3.1 ตัวอย่างภาพลายนิ้วมือที่มีรอยบาด 44
รูปที่ 3.2 หน้าต่างทิศทาง จำนวน 8 ทิศ 45
รูปที่ 3.3 ตัวอย่างโครงสร้างความสัมพันธ์ระหว่างจุดสำคัญบนเส้นลายนิ้วมือหลักกับจุดสำคัญบนเส้นลายนิ้วมือที่ใกล้เคียงมากที่สุด 5 จุด..... 49
รูปที่ 3.4 ตัวอย่างรูปแบบในการเก็บข้อมูลระหว่างจุดสำคัญบนเส้นลายนิ้วมือหลักกับจุดสำคัญบนเส้นลายนิ้วมือรอบข้าง..... 49
รูปที่ 3.5 ตัวอย่างการนำข้อมูลจุดสำคัญบนเส้นลายนิ้วมือจากข้อมูลภาพลายนิ้วมือสองรูปที่มีการเปลี่ยนตำแหน่งมาเปรียบเทียบ 50
รูปที่ 3.6 ตัวอย่างข้อมูลลายนิ้วมือที่ถูกแบ่งเป็น 3 ส่วน 51

ภาพประกอบ หน้า

รูปที่ 3.7 ตำแหน่งข้อมูลลายนิ้วมือในแต่ละส่วน 51
รูปที่ 3.8 ขั้นตอนการทำงานของระบบตรวจสอบลายนิ้วมือ กรณีต้องการลงทะเบียนลายนิ้วมือ 61
รูปที่ 3.9 ขั้นตอนการทำงานของระบบตรวจสอบลายนิ้วมือ กรณีต้องการเปรียบเทียบลายนิ้วมือ63
รูปที่ 3.10 Flowchart การทำงานของระบบทั้งหมด..... 64
รูปที่ 4.1 แนวคิดการทำงานของ เครื่องอ่าน/เขียนสมาร์ตคาร์ด..... 67
รูปที่ 4.2 ขาสัญญาณต่างๆ ของไอซี MAX232 และวงจรในการใช้งานทั่วไป..... 68
รูปที่ 4.3 การต่อไอซี MAX232 กับพอร์ต RS-232 ชนิด DB9 69
รูปที่ 4.4 คุณสมบัติบางประการของมาตรฐาน ISO 7816-3 70
รูปที่ 4.5 วงจรในส่วนของตัวกำเนิดความถี่สัญญาณนาฬิกาให้กับสมาร์ตคาร์ด..... 71
รูปที่ 4.6 ตำแหน่งของตัวอินเวอร์เตอร์ภายในไอซี 74HC04 ทั้ง 6 ตัว และตำแหน่งขาที่ต่อ
กับภายนอกของอินเวอร์เตอร์แต่ละตัว 72
รูปที่ 4.7 คุณสมบัติบางส่วนของไอซี 74HC04 72
รูปที่ 4.8 ลักษณะรูปร่างของไอซี MC78L05ACP และรายละเอียดของขาที่ติดต่อกับภายนอก . 73
รูปที่ 4.9 การนำไอซี MC78L05ACP ไปใช้งานมาตรฐานทั่วไป 74
รูปที่ 4.10 วงจรที่ใช้งานจริงของเครื่องอ่าน/เขียนสมาร์ตคาร์ดในส่วนของภาคจ่ายไฟ..... 74
รูปที่ 4.11 ภาพขยายวงจรส่วนของจัมเปอร์และอินเวอร์เตอร์ 76
รูปที่ 4.12 ภาพขยายวงจรในส่วนของการติดต่อกับขาข้อมูล (I/O) ของสมาร์ตคาร์ด..... 77
รูปที่ 4.13 วงจรตรวจสอบว่ามีสมาร์ตคาร์ดเสียบเข้ากับเครื่องอ่าน/เขียนสมาร์ตคาร์ดหรือไม่ 78
รูปที่ 4.14 วงจรที่สมบูรณ์ โดยรวมทุกส่วนของวงจรที่ได้กล่าวไว้ข้างต้น 79
รูปที่ 4.15 เครื่องอ่าน/เขียนสมาร์ตคาร์ด ที่ประกอบเสร็จเรียบร้อย..... 79
รูปที่ 5.1 ขั้นตอนการทำงานของเครื่องอ่านลายนิ้วมือ 80
รูปที่ 5.2 หลักการทำงานที่ใช้ในเครื่องอ่านลายนิ้วมือแบบ FTIR 81
รูปที่ 5.3 เครื่องอ่านลายนิ้วมือแบบแสง รุ่น U.are.U 2000 82

ภาพประกอบ หน้า

รูปที่ 5.4 ภาพลายนิ้วมือที่อ่านได้จากเครื่องอ่านลายนิ้วมือรุ่น U.are.U 2000 82
รูปที่ 5.5 เครื่องอ่านลายนิ้วมือแบบแสง รุ่น U.are.U 4000B 83
รูปที่ 5.6 ภาพลายนิ้วมือที่อ่านได้จากเครื่องอ่านลายนิ้วมือรุ่น U.are.U 4000B 83
รูปที่ 5.7 โปรแกรมที่ใช้ในการเก็บข้อมูลภาพลายนิ้วมือจากอาสาสมัคร 84
รูปที่ 5.8 ตัวอย่างภาพลายนิ้วมือจากนิ้วที่แห้งเกินไป 85
รูปที่ 5.9 ตัวอย่างภาพลายนิ้วมือจากนิ้วที่เปียกเกินไป 85
รูปที่ 5.10 ภายในของสมาร์ตคาร์ด PIC16F876 + 24C64 87
รูปที่ 5.11 การเชื่อมต่อภายในสมาร์ตคาร์ด PIC16F876 + 24LC64 87
รูปที่ 5.12 ด้านที่มีขาสัญญาณของสมาร์ตคาร์ด PIC16F876 + 24C64 88
รูปที่ 5.13 ด้านที่ไม่มีขาสัญญาณของสมาร์ตคาร์ด PIC16F876 + 24C64 88
รูปที่ 5.14 ตัวอย่างภาพลายนิ้วมือจากฐานข้อมูล FVC2002 90
รูปที่ 5.15 ภาพลายนิ้วมือที่ผ่านขั้นตอนการเลือกส่วนของภาพที่ใช้ประมวลผล 90
รูปที่ 5.16 ภาพลายนิ้วมือที่ผ่านการปรับค่าฮีสโตแกรม 90
รูปที่ 5.17 ภาพลายนิ้วมือที่ผ่านการแปลงภาพเป็นสองระดับ 90
รูปที่ 5.18 ภาพลายนิ้วมือที่ผ่านการหาทิศทางและปรับแต่งเส้นลายนิ้วมือ 91
รูปที่ 5.19 ภาพลายนิ้วมือที่ผ่านการทำลายเส้นให้บาง 91
รูปที่ 5.20 ตัวอย่างภาพลายนิ้วมือจากอาสาสมัคร จากเครื่องอ่าน U.are.U 2000 91
รูปที่ 5.21 ภาพลายนิ้วมือที่ผ่านขั้นตอนการเลือกส่วนของภาพที่ใช้ประมวลผล 91
รูปที่ 5.22 ภาพลายนิ้วมือที่ผ่านการปรับค่าฮีสโตแกรม 92
รูปที่ 5.23 ภาพลายนิ้วมือที่ผ่านการแปลงภาพเป็นสองระดับ 92
รูปที่ 5.24 ภาพลายนิ้วมือที่ผ่านการหาทิศทางและปรับแต่งเส้นลายนิ้วมือ 92
รูปที่ 5.25 ภาพลายนิ้วมือที่ผ่านการทำลายเส้นให้บาง 92
รูปที่ 5.26 ตัวอย่างภาพลายนิ้วมือจากอาสาสมัคร จากเครื่องอ่าน U.are.U 4000B 93

ภาพประกอบ หน้า

รูปที่ 5.27 ภาพลายนิ้วมือที่ผ่านขั้นตอนการเลือกส่วนของภาพที่ใช้ประมวลผล..... 93
รูปที่ 5.28 ภาพลายนิ้วมือที่ผ่านการปรับค่าฮีสโตแกรม 93
รูปที่ 5.29 ภาพลายนิ้วมือที่ผ่านการแปลงภาพเป็นสองระดับ..... 93
รูปที่ 5.30 ภาพลายนิ้วมือที่ผ่านการหาทิศทางและปรับแต่งเส้นลายนิ้วมือ..... 94
รูปที่ 5.31 ภาพลายนิ้วมือที่ผ่านการทำลายเส้นให้บาง 94

สารบัญตาราง

ตาราง หน้า

ตารางที่ 5.1 ตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากภาพลายนิ้วมือที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือรุ่น U.are.U 2000 96

ตารางที่ 5.2 ตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากภาพลายนิ้วมือที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือรุ่น U.are.U 4000B 99

ตารางที่ 5.3 ตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากฐานข้อมูล FVC2002 DB1 102

ตารางที่ 5.4 ตัวอย่างผลการทดลองบางส่วนของการทดลองเปลี่ยนค่าขีดแบ่งทั้ง 5 ค่าเป็นค่าต่างๆ 105

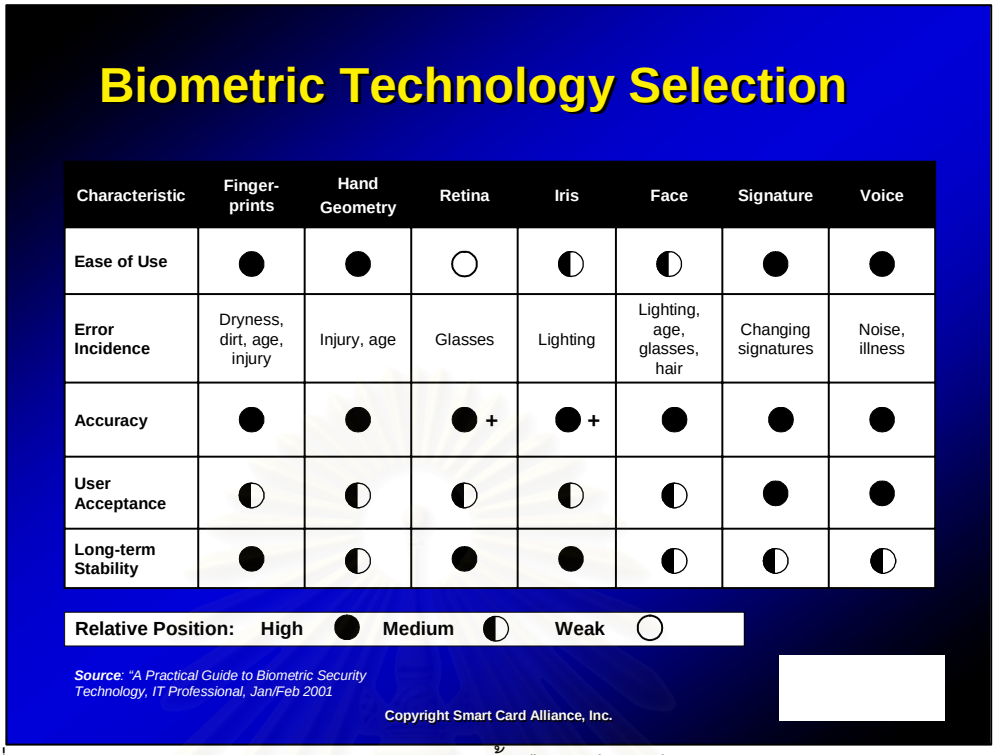
บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันระบบการตรวจสอบยืนยันความเป็นตัวตน (Authentication) ได้มีการนำอวัยวะ และลักษณะสำคัญในส่วนต่างๆ ของร่างกาย มาใช้ในการตรวจสอบเพื่อยืนยันความเป็นตัวตนที่แท้จริง อาทิ เช่น การตรวจสอบโดยการอ่านลายนิ้วมือ, ม่านตา, โครงหน้า, เสียง เป็นต้น เนื่องจากมีข้อดีหลายประการ อาทิ ยากต่อการปลอมแปลง ไม่สามารถลืมหรือสูญหายได้

การตรวจสอบยืนยันความเป็นตัวตนโดยใช้ลายนิ้วมือในการตรวจสอบ เป็นวิธีที่มีการใช้งานมาอย่างยาวนานและแพร่หลาย และได้รับการยอมรับถึงความถูกต้องของผลลัพธ์ที่ได้ ซึ่งจุดเด่นของการตรวจสอบยืนยันความเป็นตัวตนโดยใช้ลายนิ้วมือในการตรวจสอบคือ ลายนิ้วมือของแต่ละบุคคลจะมีลักษณะเฉพาะตัว แม้แต่ฝาแฝดที่เกิดจากไข่ใบเดียวกันก็มีลายนิ้วมือที่แตกต่างกันออกไป, มีความง่ายในการใช้งาน, ลายนิ้วมือจะอยู่คงทนไม่เปลี่ยนแปลงไปตามกาลเวลา และปลอมแปลงได้ยาก โดยได้แสดงการเปรียบเทียบระหว่างระบบตรวจสอบลายนิ้วกับระบบที่ใช้ในการยืนยันความเป็นตัวตนโดยใช้ลักษณะสำคัญอื่นๆ ในรูปที่ 1.1

การนำสมาร์ตคาร์ดมาประยุกต์ใช้งานร่วมกับระบบตรวจสอบลายนิ้วมือ โดยออกแบบให้สมาร์ตคาร์ดทำการเก็บแม่แบบลายนิ้วมือไว้ภายใน มีข้อดีหลายประการ เช่น ระบบตรวจสอบลายนิ้วสามารถทำงานได้โดยไม่ต้องเชื่อมต่อกับฐานข้อมูลกลาง , ไม่มีข้อจำกัดในด้านจำนวนผู้ใช้งานบนฐานข้อมูลกลาง เนื่องจากแม่แบบลายนิ้วมือของแต่ละบุคคลจะถูกเก็บไว้บนสมาร์ตคาร์ดแต่ละใบ ตัวอย่างการนำระบบตรวจสอบลายนิ้วมือไปประยุกต์ใช้งานกับสมาร์ตคาร์ดอย่างแพร่หลาย ได้แก่ การนำระบบตรวจสอบลายนิ้วมือไปใช้งานร่วมกับบัตรประจำตัวในประเทศต่างๆ อาทิ สหรัฐอเมริกา มาเลเซีย สเปน บรูไน ดังแสดงตัวอย่างในรูปที่ 1.2



Biometric Technology Selection

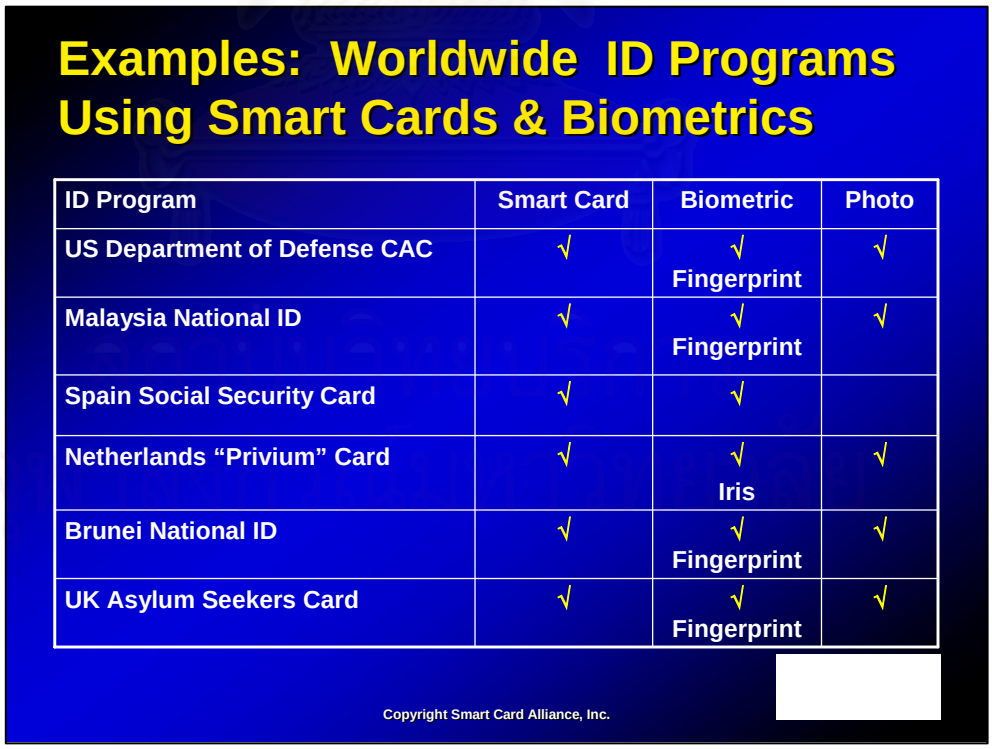
Characteristic	Finger-prints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	●	●	○	◐	◐	●	●
Error Incidence	Dryness, dirt, age, injury	Injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, illness
Accuracy	●	●	● +	● +	●	●	●
User Acceptance	◐	◐	◐	◐	◐	●	●
Long-term Stability	●	◐	●	●	◐	◐	◐

Relative Position: High ● Medium ◐ Weak ○

Source: "A Practical Guide to Biometric Security Technology, IT Professional, Jan/Feb 2001

Copyright Smart Card Alliance, Inc.

รูปที่ 1.1 จุดเด่นต่างๆ ของระบบตรวจสอบลายนิ้วมือ เปรียบเทียบกับระบบตรวจสอบโดยใช้อวัยวะหรือลักษณะสำคัญอื่นๆ ที่มา: Smart Card Alliance, Inc [1]



Examples: Worldwide ID Programs Using Smart Cards & Biometrics

ID Program	Smart Card	Biometric	Photo
US Department of Defense CAC	√	√ Fingerprint	√
Malaysia National ID	√	√ Fingerprint	√
Spain Social Security Card	√	√	
Netherlands "Privium" Card	√	√ Iris	√
Brunei National ID	√	√ Fingerprint	√
UK Asylum Seekers Card	√	√ Fingerprint	√

Copyright Smart Card Alliance, Inc.

รูปที่ 1.2 ความแพร่หลายของการนำระบบยืนยันตัวบุคคลมาใช้งานร่วมกับสมาร์ตคาร์ดเพื่อใช้เป็นบัตรประจำตัวบุคคลในประเทศต่างๆ ที่มา: Smart Card Alliance, Inc [1]

ในปัจจุบันได้มีการนำสมาร์ตคาร์ดมาใช้งานร่วมกับระบบตรวจสอบลายนิ้วมือ ซึ่งแบ่งออกเป็น 3 แนวคิดหลัก ดังนี้

1) การเก็บแม่แบบลายนิ้วมือ (Template) ไว้ที่ฐานข้อมูลกลาง (Central Database) และใช้ข้อมูลภายในสมาร์ตคาร์ด เป็นตัวชี้ดรรชนี (Index Key) เพื่อเลือกแม่แบบลายนิ้วมือจากฐานข้อมูลนั้น โดยโฮสต์ (Host) จะนำข้อมูลภาพลายนิ้วมือที่รับเข้ามาจากเครื่องอ่านลายนิ้วมือ (Fingerprint Sensor) ส่งไปตรวจสอบที่ฐานข้อมูลกลาง

2) การเก็บแม่แบบลายนิ้วมือไว้ในหน่วยความจำของสมาร์ตคาร์ด (Store-on-Card) [2] โดยนำข้อมูลจากสมาร์ตคาร์ดไปตรวจสอบลายนิ้วมือบนโฮสต์

3) การออกแบบให้หน่วยประมวลผลของสมาร์ตคาร์ด สามารถประมวลผลการตรวจสอบเปรียบเทียบลายนิ้วมือได้บนสมาร์ตคาร์ดเอง (Match-on-Card) [2] โดยเก็บแม่แบบลายนิ้วมือไว้ในหน่วยความจำของสมาร์ตคาร์ด

จาก 3 แนวคิดที่ได้กล่าวในข้างต้น พบว่าแนวคิดที่ 1 มีข้อเสีย คือ ระบบจะต้องมีการเชื่อมต่อแบบออนไลน์กับฐานข้อมูลกลางตลอดเวลา และหากฐานข้อมูลกลางเสียหายก็จะทำให้ข้อมูลลายนิ้วมือทั้งหมดสูญหาย ส่วนแนวคิดที่ 2 มีข้อเสีย คือ มีการส่งแม่แบบลายนิ้วมือออกมาภายนอกสมาร์ตคาร์ดเพื่อตรวจสอบที่โฮสต์ จึงอาจถูกดักจับหรือปลอมแปลงข้อมูลลายนิ้วมือระหว่างทางได้ ในขณะที่แนวคิดที่ 3 แม่แบบลายนิ้วมือที่เก็บไว้ในสมาร์ตคาร์ดจะมีความปลอดภัยสูงที่สุด เนื่องจากทำการตรวจสอบลายนิ้วมือบนหน่วยประมวลผลของสมาร์ตคาร์ด ทำให้ไม่มีการส่งแม่แบบลายนิ้วมือออกมาภายนอกสมาร์ตคาร์ด และแม่แบบลายนิ้วมือของสมาร์ตคาร์ดจะถูกปกป้องจากคุณสมบัติของสมาร์ตคาร์ดที่ออกแบบให้หน่วยความจำของสมาร์ตคาร์ด ไม่สามารถเข้าถึงได้โดยตรงจากภายนอก

ตัวอย่างรูปแบบการทำงานในแนวคิดที่ 3 สมาร์ตคาร์ดจะทำการรับข้อมูลลายนิ้วมือที่ต้องการตรวจสอบเข้ามาเปรียบเทียบกับแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำของสมาร์ตคาร์ด โดยใช้หน่วยประมวลผลภายในสมาร์ตคาร์ดเป็นตัวตรวจสอบ หากผลลัพธ์ในการตรวจสอบพบว่า ข้อมูลลายนิ้วมือที่รับเข้ามาเป็นของบุคคลเดียวกับแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำ สมาร์ตคาร์ดจะทำการปล่อยข้อมูลสำคัญที่เก็บไว้ภายใน

สมาร์ตคาร์ดออกมา เช่น ใบรับรองอิเล็คทรอนิคส์ หรือ Private Key สำหรับ Digital Signature เป็นต้น

ดังนั้นในงานวิจัยนี้จึงสนใจที่จะศึกษาและพัฒนาระบบตรวจสอบลายนิ้วมือ โดยใช้แนวคิดที่ 3 เป็นแนวทางในการออกแบบ เพื่อให้สามารถทำการเปรียบเทียบข้อมูลลายนิ้วมือบนหน่วยประมวลผลของสมาร์ตคาร์ด ซึ่งทำให้การตรวจสอบลายนิ้วมือไม่ต้องมีการส่งแม่แบบลายนิ้วมือออกมาภายนอกสมาร์ตคาร์ด จึงปลอดภัยต่อการถูกดักจับหรือการปลอมแปลงข้อมูลแม่แบบลายนิ้วมือได้

ในการนำระบบตรวจสอบลายนิ้วมือมาประมวลผลบนสมาร์ตคาร์ดนั้น มีปัญหาสำคัญหลายประการที่จะต้องพิจารณาดังต่อไปนี้

1. **อัตราเร็วในการประมวลผลของหน่วยประมวลผลบนสมาร์ตคาร์ด**

   เนื่องจากหน่วยประมวลผลบนสมาร์ตคาร์ด (CPU: Central Processing Unit) ส่วนใหญ่มักเป็นไมโครคอนโทรลเลอร์ ขนาด 8–32 บิต และทำงานตามความถี่สัญญาณนาฬิกาที่จ่ายให้กับสมาร์ตคาร์ด โดยทั่วไปตามมาตรฐาน ISO 7816 [3] จะเท่ากับ 3.57 MHz ซึ่งนับว่าต่ำมากเมื่อเทียบกับหน่วยประมวลผลบนเครื่องคอมพิวเตอร์

2. **ความสามารถในการคำนวณฟังก์ชันทางคณิตศาสตร์ที่ซับซ้อน**

   เนื่องจากหน่วยประมวลของสมาร์ตคาร์ด ส่วนใหญ่มีขนาด 8–32 บิต และทำงานที่ความถี่สัญญาณนาฬิกาต่ำ จึงมีข้อจำกัดในเรื่องขนาดของข้อมูลที่นำมาประมวลผลแต่ละครั้ง และความเร็วในการทำงาน ซึ่งไม่เหมาะกับการคำนวณทางคณิตศาสตร์ที่ซับซ้อน และในสมาร์ตคาร์ดบางชนิด มีข้อจำกัดทางด้านการคำนวณ

3. **ขนาดของหน่วยความจำชั่วคราว** (RAM : Random Access Memory)

โดยทั่วไปหน่วยความจำชั่วคราวของสมาร์ตคาร์ดจะมีขนาดเล็ก ซึ่งในกรณีที่หน่วยความจำชั่วคราวของสมาร์ตคาร์ดมีขนาดเล็กกว่าขนาดข้อมูลภาพลายนิ้วมือทั้งหมด จะทำให้ไม่สามารถที่จะรับข้อมูลภาพลายนิ้วมือได้หมดในครั้งเดียว

4. **ความเร็วในการส่งผ่านข้อมูลระหว่างสมาร์ตคาร์ดกับโฮสต์**

เนื่องจากการติดต่อกับสมาร์ตคาร์ดเป็นแบบสื่อสารสองทางครึ่งอัตรา (Half-duplex) และตามมาตรฐาน ISO 7816 [3] ได้กำหนดสัญญาณนาฬิกาที่ใช้ในการติดต่อกับสมาร์ตคาร์ด เท่ากับ 3.57 MHz ซึ่งมีความเร็วเท่ากับ 9600 baud โดยเป็นความเร็วที่ต่ำ ไม่เหมาะกับการส่งผ่านข้อมูลภาพลายนิ้วมือระดับเทา (gray scale) ที่มีความละเอียดสูง

1.2 วัตถุประสงค์

1. เพื่อพัฒนาระบบการตรวจสอบลายนิ้วมือแบบอัตโนมัติ ให้สามารถประมวลผลบนสมาร์ตคาร์ดที่ใช้หน่วยประมวลผลแบบ 8 บิต ที่มีความเร็วในการประมวลผลต่ำ และมีหน่วยความจำชั่วคราวขนาดเล็กได้

2. เพิ่มความปลอดภัยของการเก็บแม่แบบลายนิ้วมือบนสมาร์ตคาร์ด

1.3 ขอบเขตงานวิจัย

ในงานวิจัยนี้จะศึกษาหลักการและอัลกอริทึมของการตรวจสอบลายมือในงานวิจัยต่างๆ ก่อนหน้านี้ เพื่อทำการพัฒนาอัลกอริทึมในส่วนของการเปรียบเทียบข้อมูลลายนิ้วมือขึ้นมาใหม่ เพื่อให้สามารถประมวลผลบนหน่วยประมวลผลของสมาร์ตคาร์ดแบบ 8 บิต ที่มี

ความเร็วในการประมวลผลต่ำ และมีขนาดของหน่วยความจำชั่วคราวเล็กกว่าข้อมูลภาพลายนิ้วมือทั้งหมดได้ โดยมีขอบเขต ดังนี้

1. อัลกอริทึมจะทำงานภายใต้เงื่อนไข ดังต่อไปนี้
   1.1 เครื่องอ่านลายนิ้วมือ (Fingerprint Sensor) ทำงานตามปกติ
   1.2 นิ้วมือที่ใช้ในการตรวจสอบอยู่ในสภาพสมบูรณ์และสะอาดตามปกติ
   1.3 นิ้วมือที่ใช้ในการเก็บข้อมูลเพื่อสร้างเป็นแม่แบบลายนิ้วมือ จะต้องเป็นนิ้วเดียวกับที่ใช้ตรวจสอบกับเครื่องอ่านลายนิ้วมือ

2. เพื่อค้นหาวิธีในการปรับปรุงความเร็วในการส่งผ่านข้อมูลลายนิ้วมือที่ต้องการตรวจสอบลายนิ้วมือไปยังสมาร์ตคาร์ด

3. ทำการทดสอบอัลกอริทึม, คำนวณหาประสิทธิภาพของการประมวลผลและความถูกต้องในการทำงานของอัลกอริทึม โดยทำการทดสอบกับฐานข้อมูลที่ได้คัดเลือกมาจาก FVC2002 [4] และภาพลายนิ้วมือที่ได้คัดเลือกมาจากฐานข้อมูลภาพลายนิ้วมือที่ทำการเก็บข้อมูลจากอาสาสมัคร จำนวน 70 คน

1.4 ขั้นตอนและวิธีดำเนินงานวิจัย

1. ศึกษาหลักการ และอัลกอริทึมของการตรวจสอบลายมือในงานวิจัยต่างๆ ก่อนหน้านี้

2. ศึกษาถึงคุณสมบัติต่างๆ ของสมาร์ตคาร์ดแต่ละรุ่น เพื่อคัดเลือกสมาร์ตคาร์ดที่เหมาะสมมาใช้ในการทดสอบอัลกอริทึมในงานวิจัยนี้

3. ศึกษาถึงรูปแบบการเขียนโปรแกรมในการติดต่อกับเครื่องอ่านลายนิ้วมือ เพื่อใช้ในการเขียนโปรแกรมรับภาพลายนิ้วมือจากเครื่องอ่านลายนิ้วมือ

4. ศึกษาถึงโปรโตคอลที่ใช้ในสมาร์ตคาร์ด เพื่อใช้เป็นแนวทางการเขียนโปรแกรมติดต่อระหว่างสมาร์ตคาร์ดกับโฮสต์และรูปแบบของคำสั่งต่างๆที่ใช้ในการเขียนโปรแกรมลงบนสมาร์ตคาร์ด

5. ทำการพัฒนาอัลกอริทึมในส่วนของการเปรียบเทียบข้อมูลลายนิ้วมือขึ้นมาใหม่ เพื่อให้สามารถประมวลผลบนหน่วยประมวลผลของสมาร์ตคาร์ดแบบ 8 บิต ที่มีความเร็วในการประมวลผลต่ำ และมีหน่วยความจำชั่วคราวขนาดเล็กกว่าข้อมูลภาพลายนิ้วมือทั้งหมดได้

6. ทำการเขียนโปรแกรมเพื่อติดต่อกับเครื่องอ่านลายนิ้วมือ และทำการเก็บภาพลายนิ้วมือจากอาสาสมัคร จำนวน 70 คน

7. ทำการทดสอบอัลกอริทึมที่ได้พัฒนาขึ้นมา โดยใช้ภาพลายนิ้วมือที่ได้คัดเลือกมาจากฐานข้อมูล FVC2002[4] และภาพลายนิ้วมือที่ได้คัดเลือกมาจากฐานข้อมูลภาพลายนิ้วมือที่ทำการเก็บข้อมูลจากอาสาสมัคร จำนวน 70 คน นำผลการทดสอบที่ได้มาทำการปรับปรุงอัลกอริทึมและโปรแกรมตรวจสอบลายนิ้วมือเพื่อให้ได้ผลลัพธ์ที่ดีที่สุด

8. สรุปผลการทดลองและเขียนวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้อัลกอริทึมในส่วนของการเปรียบเทียบข้อมูลลายนิ้วมือขึ้นมาใหม่ ที่สามารถประมวลผลบนหน่วยประมวลผลของสมาร์ตคาร์ดแบบ 8 บิต ที่มีความเร็วในการประมวลผลต่ำ และมีหน่วยความจำชั่วคราวขนาดเล็กกว่าข้อมูลภาพลายนิ้วมือทั้งหมดได้ จากเดิมที่อัลกอริทึมทั่วไปไม่สามารถประมวลผลได้

2. ลดต้นทุนของระบบตรวจสอบลายนิ้วมือบนสมาร์ตคาร์ด เนื่องจากสามารถเลือกใช้สมาร์ตคาร์ดที่มีหน่วยประมวลผลแบบ 8 บิต และมีขนาดของหน่วยความจำชั่วคราวเล็กลงได้

3. สามารถนำไปประยุกต์ใช้งานกับระบบที่มีการใช้งานสมาร์ตคาร์ดแบบมีหน่วยประมวลที่มีอยู่เดิม โดยเพิ่มระบบตรวจสอบลายนิ้วมือเข้าไปได้

4. นำไปพัฒนาต่อเพื่อประยุกต์ใช้กับสมาร์ตคาร์ดที่มีข้อจำกัดทางด้านความเร็วในการประมวลผลเนื่องจากพลังงานไฟฟ้าที่จำกัด หรือมีความเร็วในการส่งผ่านข้อมูลต่ำ

1.6 ลำดับการจัดเรียงเนื้อหาในวิทยานิพนธ์

วิทยานิพนธ์นี้แบ่งเนื้อหาออกเป็น 6 บทดังนี้ บทที่ 1 เป็นบทนำซึ่งกล่าวถึงที่มาและความสำคัญของปัญหา วัตถุประสงค์ของงานวิจัย ขอบเขตงานวิจัย ขั้นตอนและวิธีดำเนินงานวิจัย ตลอดจนประโยชน์ที่คาดว่าจะได้รับ บทที่ 2 กล่าวถึง ทฤษฎีเบื้องต้นและงานวิจัยที่เกี่ยวข้อง บทที่ 3 นำเสนอระบบตรวจสอบลายนิ้วมือที่ได้พัฒนาขึ้นใหม่ บทที่ 4 กล่าวถึงการออกแบบเครื่องอ่าน/เขียนสมาร์ตคาร์ด (Smartcard Reader/Writer) บทที่ 5 กล่าวถึงการเก็บข้อมูลลายนิ้วมือจากอาสาสมัคร, การเพิ่มความเร็วในการประมวลผลของสมาร์ตคาร์ดโดยเพิ่มความถี่สัญญาณนาฬิกา และการทดลองในการทดสอบการทำงานของระบบตรวจสอบลายนิ้วมือที่ได้พัฒนาขึ้นมาใหม่ และบทที่ 6 สรุปผลการวิจัยและข้อเสนอแนะ

1.7 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้รับการตีพิมพ์เป็นบทความทางวิชาการในหัวข้อเรื่อง “การพัฒนาอัลกอริทึมเปรียบเทียบลายนิ้วมือเพื่อใช้ประมวลผลบนสมาร์ตคาร์ด”, “Development of Fingerprint Matching Algorithm for Processing on Smart card” โดย ชัยรัตน์ องค์วิศิษฐ์ และสาธิต วงศ์ประทีป ในงานประชุมวิชาการ “The 7th National Computer Science and Engineering Conference (NCSEC2003)” ซึ่งจัดโดยภาควิชาวิทยาศาสตร์คอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา 169 ถนนลงหาดบางแสน ตำบลแสนสุข อำเภอเมือง จังหวัดชลบุรี ในระหว่างวันที่ 28-30 ตุลาคม 2546

บทที่ 2
ทฤษฎีเบื้องต้นและงานวิจัยที่เกี่ยวข้อง

ในบทนี้ จะได้กล่าวถึงความรู้และทฤษฎีเบื้องต้นที่เกี่ยวข้องกับชนิดของระบบตรวจสอบลายนิ้วมือ, รูปแบบต่างๆ ของลายนิ้วมือ, หลักการและลักษณะสำคัญต่างๆ ที่ใช้ในการตรวจสอบลายนิ้วมือ, ชนิดของสมาร์ตคาร์ด, การเชื่อมต่อของสมาร์ตคาร์ด, มาตรฐานที่เกี่ยวข้องกับสมาร์ตคาร์ด ตลอดจนงานวิจัยที่เกี่ยวข้องกับระบบตรวจสอบลายนิ้วมือ

2.1 ความรู้และทฤษฎีเบื้องต้น

2.1.1 ระบบตรวจสอบลายนิ้วมือ (Fingerprint Matching) สามารถแบ่งออกได้เป็น 2 ประเภทหลักๆ ดังนี้

1. **การตรวจสอบลายนิ้วมือแบบเปรียบเทียบกันในลักษณะ 1 ต่อ 1**

เป็นการตรวจสอบลายนิ้วมือ ในลักษณะเปรียบเทียบ 1 ต่อ 1 (one to one) กล่าวคือ ระบบจะตรวจสอบโดยการเปรียบเทียบลายนิ้วมือ จากข้อมูลลายนิ้วมือ 2 ชุด ระหว่างข้อมูลภาพลายนิ้วมือที่ต้องการตรวจสอบกับแม่แบบลายนิ้วมือ เพื่อตรวจสอบว่าเป็นลายนิ้วมือที่มาจากบุคคลเดียวกันหรือไม่

2. **การตรวจสอบลายนิ้วมือแบบเปรียบเทียบกันในลักษณะ 1 ต่อหลายๆ ชุด**

เป็นการตรวจสอบลายนิ้วมือ ในลักษณะเปรียบเทียบ 1 ต่อ หลายๆ ชุด (one to many) กล่าวคือ ระบบจะนำข้อมูลภาพลายนิ้วมือที่ต้องการตรวจสอบมาเปรียบเทียบกับฐานข้อมูลที่มีการเก็บข้อมูลลายนิ้วมือหลายๆ ชุด เพื่อตรวจสอบว่าลายนิ้วมือที่รับเข้ามาตรงกับลายนิ้วมือของบุคคลใดที่เก็บในฐานข้อมูลหรือไม่

โดยทั่วไปแล้วระบบการตรวจสอบลายนิ้วมือแบบเปรียบเทียบ 1 ต่อ หลายๆ ชุด จะมีความซับซ้อนมากกว่าระบบตรวจสอบลายนิ้วมือแบบเปรียบเทียบ 1 ต่อ 1 และใช้เวลาในการประมวลผลนานกว่า

2.1.2 **รูปแบบของลายนิ้วมือ**

รูปแบบของลายนิ้วมือสามารถวิเคราะห์ ได้ออกเป็น 4 ประเภทหลัก ดังต่อไปนี้

1. **แบบเส้นโค้ง** (Arch) สามารถแบ่งออกเป็น 2 ชนิดย่อย ดังนี้

1.1 แบบโค้งราบ (Plain Arch)

ตัวเส้นลายนิ้วมือจะวิ่งหรือไหลออกไปข้างหนึ่ง โดยจะไม่เกิดมุมแหลม หรือพุ่งขึ้นตรงกลาง

Arch (A)

รูปที่ 2.1 ภาพลายนิ้วมือแบบโค้งราบ

1.2 **แบบโค้งกระโจม** (Tented Arch)

ตัวเส้นลายนิ้วมือตรงกลางจะเกิดเป็นลายเส้นพุ่งขึ้นจากแนวนอนเป็นมุมแหลมหรือมุมฉาก

Tented Arch (T)

รูปที่ 2.2 ภาพลายนิ้วมือแบบโค้งกระโจม

2. **แบบมัดหวาย** (Loop)

เป็นแบบของลายนิ้วมือที่สามารถพบได้มากที่สุดประมาณ 65 % ของลายนิ้วมือทั้งหมด สามารถแบ่งออกเป็น 3 ชนิดย่อย ดังนี้

2.1 **แบบมัดหวายปัดขวา** (Right Loop)

ลายนิ้วมือจะมีจุดสันดอนเพียงจุดเดียว และมีเส้นวกหลักที่สมบูรณ์อย่างน้อย 1 เส้น โดยมีทิศทางไปทางขวา

Right Loop (R)

รูปที่ 2.3 ภาพลายนิ้วมือแบบมัดหวายปัดขวา

2.2 แบบมัดหวายปัดซ้าย (Left Loop)

ลายนิ้วมือจะมีจุดสันดอนเพียงจุดเดียว และมีเส้นวกหลักที่สมบูรณ์อย่างน้อย 1 เส้น โดยมีทิศทางไปทางซ้าย

Left Loop (L)

รูปที่ 2.4 ภาพลายนิ้วมือแบบมัดหวายปัดซ้าย

2.3 แบบมัดหวายคู่ (Twin Loop **หรือ** Double Loop)

ลายนิ้วมือจะมีลักษณะคล้ายกับลายนิ้วมือแบบมัดหวายทั้งสองชนิดที่ได้กล่าวมาในข้างต้น แต่จะมากอดกันจนทำให้เกิดสันดอน 2 จุด โดยมัดหวายแต่ละอันไม่จำเป็นต้องมีขนาดเท่ากัน

Twin Loop (W)

รูปที่ 2.5 ภาพลายนิ้วมือแบบมัดหวายคู่

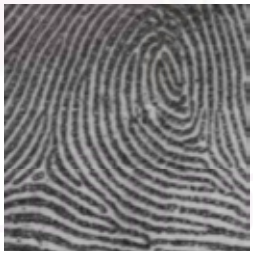
3. **แบบก้นหอย** (Whorl)

สามารถพบได้ประมาณ 30 % จากลายนิ้วมือทั้งหมด ซึ่งสามารถสังเกตได้โดยจะมีเส้นลายนิ้วมืออย่างน้อย 1 เส้นที่เป็นเส้นเวียนรอบเป็นวงจร ลักษณะเหมือนลานนาฬิกา, รูปไข่, วงกลม หรือลักษณะอื่นๆ แบ่งออกเป็น 3 ชนิดย่อย ดังต่อไปนี้

3.1 **แบบก้นหอยธรรมดา** (Plain Whorl)

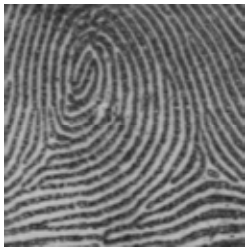
รูปที่ 2.6 ภาพลายนิ้วมือแบบก้นหอยธรรมดา

3.2 **แบบก้นหอยกระเป๋ากลางปัดขวา** (Right Central Pocket)



รูปที่ 2.7 ภาพลายนิ้วมือแบบก้นหอยกระเป๋ากลางปัดขวา

3.3 **แบบก้นหอยกระเป๋าข้างปัดซ้าย** (Left Lateral Pocket)



รูปที่ 2.8 ภาพลายนิ้วมือแบบก้นหอยกระเป๋าข้างปัดซ้าย

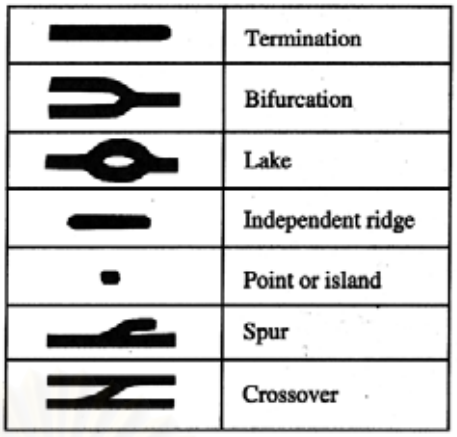
4. **แบบซับซ้อน** (Accidental Whorl)

เป็นลายนิ้วมือที่มีรูปแบบลักษณะพิเศษ ที่ไม่จัดเข้าเป็นลายนิ้วมือชนิดหนึ่งชนิดใดโดยเฉพาะ อาจจะประกอบด้วยลายนิ้วมือ 2 แบบมาผสมกัน และมีสันดอน 2 สันดอน หรือมากกว่า หรือไม่สามารถเข้ากับลายนิ้วมือในทั้งสามกลุ่มหลักข้างต้นเลย ซึ่งมีรูปแบบที่ไม่แน่นอน

รูปที่ 2.9 ภาพลายนิ้วมือแบบซับซ้อน ที่มา: [5]

2.1.3 **จุดสำคัญบนเส้นลายนิ้วมือ** (Minutiae)

ในภาพลายนิ้วมือหนึ่งๆ จะประกอบไปด้วยจุดสำคัญบนเส้นลายนิ้วมือมากมาย และภาพลายนิ้วมือแต่ละภาพที่มาจากต่างบุคคลหรือมาจากต่างนิ้วมือก็จะมีจุดสำคัญบนเส้นลายนิ้วมือที่แตกต่างกันออกไป โดยจุดสำคัญบนเส้นลายนิ้วมือเกิดจากการพิจารณาลักษณะสำคัญบนเส้นลายนิ้วมือ ซึ่งได้แสดงลักษณะของจุดสำคัญบนเส้นลายนิ้วมือชนิดพื้นฐานไว้ในรูปที่ 2.10 และ 2.11



รูปที่ 2.10 จุดสำคัญบนเส้นลายนิ้วมือ (Minutiae) พื้นฐาน ที่มา: [6]

รูปที่ 2.11 ลักษณะต่าง ๆ ที่มีปรากฏบนเส้นลายนิ้วมือ

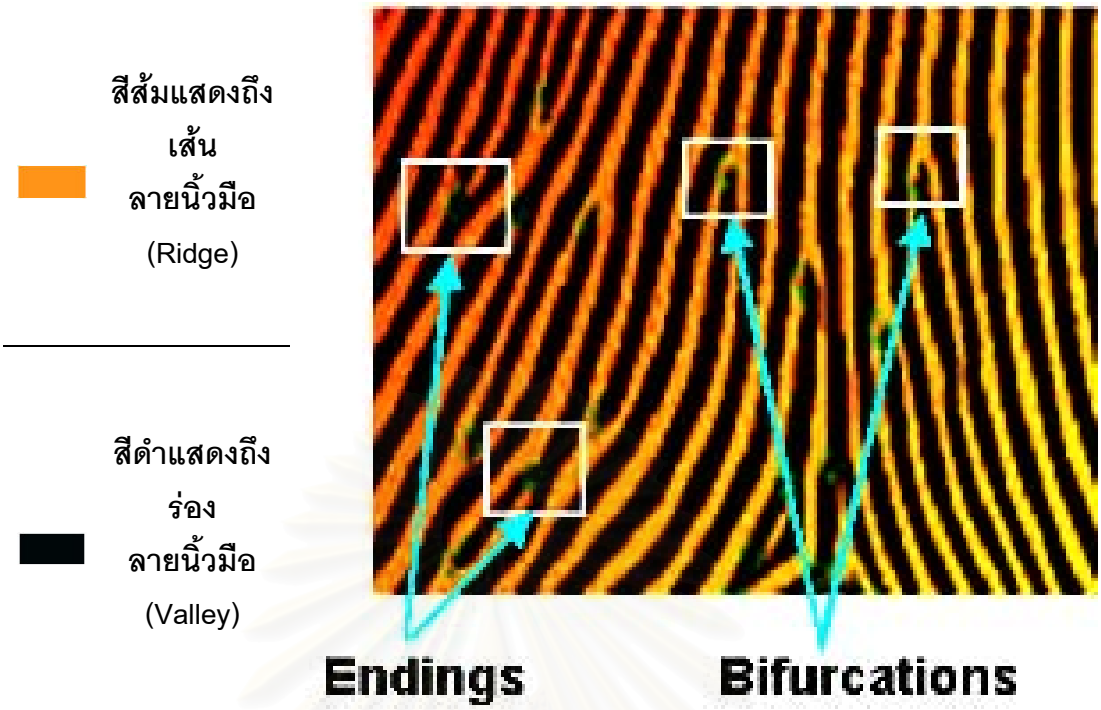
1. **Ridge ending (Termination)** เป็นลักษณะที่เส้นลายนิ้วมือสิ้นสุดโดยทันทีทันใด
2. **Bifurcation** เป็นลักษณะที่เส้นลายนิ้วมือเดินทางมาจาก 1 เส้นแล้วแตกแยกออกเป็น 2 เส้นหรือมากกว่า 2 เส้น
3. **Enclosure (Lake)** เป็นลักษณะที่เส้นลายนิ้วมือเดินทางมาจาก 1 เส้นแล้วแยกออกและมารวมกันอีกครั้งจนเกิดเป็นพื้นที่ปิด

4. **Independent ridge** เป็นลักษณะที่เส้นลายนิ้วมืออยู่อย่างอิสระ ไม่เชื่อมต่อกับเส้นอื่น มีลักษณะค่อนข้างสั้น แต่ไม่สั้นจนถือว่าเป็น Ridge dot
5. **Ridge dot (Point or island)** เป็นลักษณะที่เส้นลายนิ้วมือสั้นมากจนสามารถเปรียบเทียบได้ว่าเป็นจุด
6. **Spur** เป็นลักษณะที่เส้นลายนิ้วมือ 1 เส้นมีเส้นลายนิ้วมืออีกเส้นแยกออกมาเพียงเล็กน้อย คล้ายกับลักษณะเดือยไก่
7. **Crossover** เป็นลักษณะที่เส้นลายนิ้วมือ 2 เส้นซึ่งวิ่งมาคู่กันมีเส้นลายนิ้วมือเล็กๆ แยกออกมาเชื่อมทั้งสองเส้นเข้าด้วยกัน

2.1.4 **วิธีการที่ใช้ในการตรวจสอบลายนิ้วมือ**

ในงานวิจัยชิ้นนี้ได้นำวิธีตรวจสอบลายนิ้วมือจากจุดสำคัญบนเส้นลายนิ้วมือ (Minutiae-based) มาใช้งาน วิธีการนี้ใช้การตรวจสอบเปรียบเทียบจากจุดสำคัญบนเส้นลายนิ้วมือ ซึ่งจุดสำคัญบนเส้นลายนิ้วมือ จะแบ่งออกได้หลายชนิดตามลักษณะของเส้นลายนิ้วมือ ดังที่ได้กล่าวไว้แล้วในหัวข้อที่ 2.1.3 โดยในงานวิจัยชิ้นนี้จะนำจุดสำคัญบนเส้นลายนิ้วมือ 2 ชนิดหลักมาใช้งาน ดังแสดงในรูปที่ 2.12 ดังนี้

1. จุดสิ้นสุดของเส้นลายนิ้วมือ (Ridge ending)
2. จุดที่เส้นลายนิ้วมือ 1 เส้น มีการแยกเป็น 2 เส้นหรือมากกว่า (Ridge bifurcation)



รูปที่ 2.12 จุดสำคัญบนเส้นลายนิ้วมือ 2 ชนิดหลัก

โดยสีส้มแสดงถึงส่วนที่เป็นเส้นลายนิ้วมือ ส่วนสีดำแสดงถึงส่วนที่เป็นร่อง

2.1.5 สมาร์ตคาร์ด (บัตรเก่ง)

สมาร์ตคาร์ด มีคุณสมบัติเด่นที่แตกต่างจากบัตรชนิดอื่นๆ เป็นอย่างมาก อาทิ เช่น ป้องกันการปลอมแปลงได้ดี, ข้อมูลที่เก็บในบัตรมีความปลอดภัยสูง, มีความคงทนต่อสนามแม่เหล็กสูง, หน่วยความจำมีความจุสูงกว่าบัตรชนิดอื่นหลายเท่าตัว และในกรณีของสมาร์ตคาร์ดชนิดไมโครโพรเซสเซอร์ จะมีหน่วยประมวลภายในตัวเอง ซึ่งทำให้สามารถประมวลผลข้อมูลต่างๆ ได้ภายในตัวสมาร์ตคาร์ดเอง โดยสมาร์ตคาร์ดสามารถแบ่งออกได้เป็น 2 ประเภทหลักๆ ดังนี้

2.1.5.1 **แบบที่มีหน่วยความจำเพียงอย่างเดียว** (Memory card **หรือ** Synchronous Smart card)

ภายในสมาร์ตคาร์ดจะประกอบด้วยหน่วยความจำเพียงอย่างเดียว สำหรับเก็บข้อมูลต่างๆ โดยทั่วไปมักนำไปประยุกต์ใช้กับงานที่ไม่ต้องใช้การประมวลผลข้อมูลจากสมาร์ตคาร์ด หรืองานที่ต้องการเก็บข้อมูลอย่างเดียว อาทิ การนำไปประยุกต์ใช้เป็นบัตรโทรศัพท์ โดยมีความปลอดภัยในระดับหนึ่ง เนื่องจากหน่วยความจำที่ใช้ในบัตรส่วนใหญ่จะเป็นแบบ Security Memory ซึ่งจะมีส่วนที่ป้องกันการอ่านข้อมูลจากหน่วยความจำแบบ Sequential Reading ทำให้ไม่สามารถคัดลอกบัตรโดยตรงได้

รูปที่ 2.13 ด้านที่มีขาสัญญาณของบัตรโทรศัพท์ชนิดที่เป็นสมาร์ตคาร์ดแบบมีหน่วยความจำเพียงอย่างเดียว

รูปที่ 2.14 ด้านที่ไม่มีขาสัญญาณของบัตรโทรศัพท์ชนิดที่เป็นสมาร์ตคาร์ดแบบมีหน่วยความจำเพียงอย่างเดียว

2.1.5.2 **แบบมีหน่วยประมวลผลภายในตัว** (Microprocessor Card **หรือ** Asynchronous Smart card)

โดยทั่วไปแล้ว ภายในสมาร์ตคาร์ดจะประกอบไปด้วยหน่วยประมวลผลหลัก (CPU: Central Processing Unit), หน่วยความจำชั่วคราว (RAM: Random Access Memory), หน่วยความจำส่วนที่ใช้ในการเก็บข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ด และหน่วยความจำข้อมูลแบบ EEPROM (Electrically Erasable Programmable Read-Only Memory)

สมาร์ตคาร์ด ชนิดนี้จะมีความปลอดภัยของข้อมูลที่ค่อนข้างสูง เนื่องจากโดยทั่วไปหน่วยความจำภายในสมาร์ตคาร์ดจะถูกออกแบบให้ไม่มีการติดต่อกับขาสัญญาณภายนอกของสมาร์ตคาร์ดโดยตรง การติดต่อกับหน่วยความจำจะต้องทำการติดต่อผ่านทางหน่วยประมวลผลหลักของบัตรเท่านั้น จึงทำให้มีความปลอดภัยของข้อมูลที่สูง

ตัวอย่างของสมาร์ตคาร์ดแบบมีหน่วยประมวลผลภายในตัว ที่มีใช้งานกันทั่วไป มีดังนี้

- ซิมการ์ด (SIM: Subscriber Identity Module) ที่นำมาใช้งานในโทรศัพท์เคลื่อนที่ระบบจีเอสเอ็ม (GSM: Global System For Mobile Communication) และ R-UIM (Removable User Identity Module) ในระบบ CDMA (Code Division Multiple Access)

รูปที่ 2.15 ด้านที่มีขาสัญญาณของซิมการ์ด

รูปที่ 2.16 ด้านที่ไม่มีขาสัญญาณของซิมการ์ด

- บัตรประชาชน แบบสมาร์ตคาร์ด

รูปที่ 2.17 ด้านที่มีขาสัญญาณ (ด้านหน้า) ของบัตรประชาชนแบบสมาร์ตคาร์ด ที่มา: [7]

รูปที่ 2.18 ด้านที่ไม่มีขาสัญญาณ (ด้านหลัง) ของบัตรประชาชนแบบสมาร์ตคาร์ด ที่มา: [7]

- สมาร์ตคาร์ด ที่ใช้ในระบบถอดรหัสสัญญาณของระบบโทรทัศน์บอกรับสมาชิกต่างๆ

รูปที่ 2.19 ด้านที่มีขาสัญญาณของสมาร์ตคาร์ดที่ใช้ในระบบถอดรหัสสัญญาณของระบบโทรทัศน์บอกรับสมาชิก

รูปที่ 2.20 ด้านที่ไม่มีขาสัญญาณของสมาร์ตคาร์ดที่ใช้ในระบบถอดรหัสสัญญาณของระบบโทรทัศน์บอกรับสมาชิก

2.1.6 **การเชื่อมต่อของสมาร์ตคาร์ด** สามารถแบ่งออกได้เป็น 2 ประเภทหลักๆ ดังนี้

2.1.6.1 **สมาร์ตคาร์ดแบบไม่มีหน้าสัมผัส** (Contactless Smart card)

รูปที่ 2.21 ด้านหน้าของสมาร์ตคาร์ดแบบไม่มีหน้าสัมผัส

สมาร์ตคาร์ดชนิดนี้จะไม่มีหน้าสัมผัสของขาสัญญาณบนตัวบัตร แต่จะใช้การเชื่อมต่อเพื่อติดต่อแลกเปลี่ยนข้อมูลกับเครื่องอ่าน/เขียน สมาร์ตคาร์ด โดยผ่านตัวกลางแบบไร้สาย (Wireless) เช่น คลื่นวิทยุ (Radio Frequency)

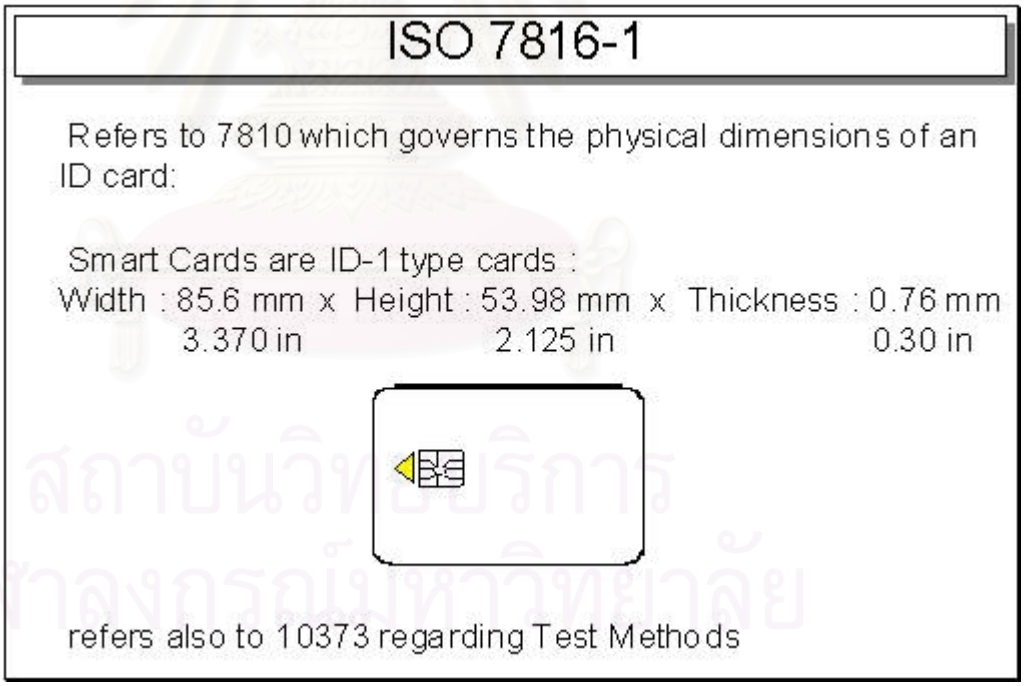
2.1.6.2 **สมาร์ตคาร์ดแบบมีหน้าสัมผัส** (Contact Smart card)

รูปที่ 2.22 ด้านหน้าของสมาร์ตคาร์ดแบบมีหน้าสัมผัส

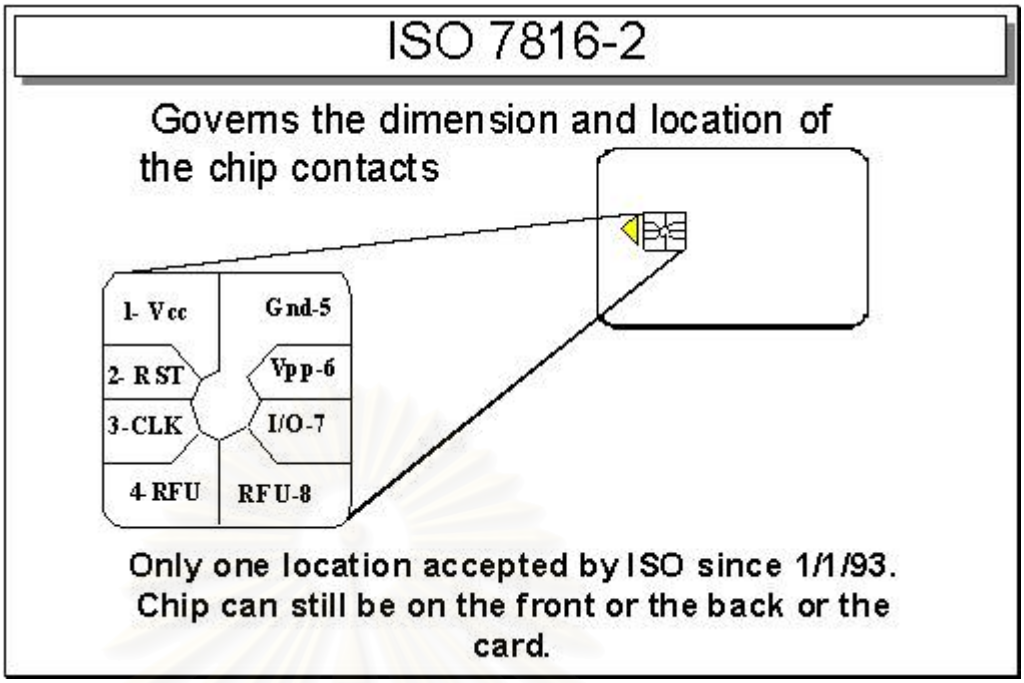
สมาร์ตคาร์ดชนิดนี้ จะมีรูปแบบที่ใช้ในการติดต่อสื่อสารข้อมูลกับเครื่องอ่าน/เขียนสมาร์ตคาร์ด โดยผ่านทางขั้วนำสัญญาณแถบโลหะที่อยู่ทางด้านหน้าของบัตร ซึ่งตำแหน่งหน้าสัมผัสของขาสัญญาณต่างๆ ที่อยู่บนสมาร์ตคาร์ด ที่มีใช้งานกันในปัจจุบัน สามารถแบ่งออกเป็น 2 มาตรฐาน ดังนี้

2.1.6.2.1 **มาตรฐาน** ISO7816 [3]

เป็นรูปแบบการเชื่อมต่อที่ได้กำหนดไว้ใน ISO 7816 [3] ซึ่งใช้ในสมาร์ตคาร์ดที่พบเห็นส่วนใหญ่ในปัจจุบัน อาทิ ซิมการ์ด ที่ใช้ในโทรศัพท์เคลื่อนที่ระบบ GSM, บัตรแทนเงินสดแบบสมาร์ตคาร์ด, บัตรประชาชนแบบสมาร์ตคาร์ด, บัตรประจำตัวนักศึกษาแบบสมาร์ตคาร์ด จะใช้มาตรฐานนี้ โดยสมาร์ตคาร์ด และเครื่องอ่าน/เขียนสมาร์ตคาร์ด ที่ใช้ในงานวิจัยชิ้นนี้จะยึดถือตามมาตรฐานนี้



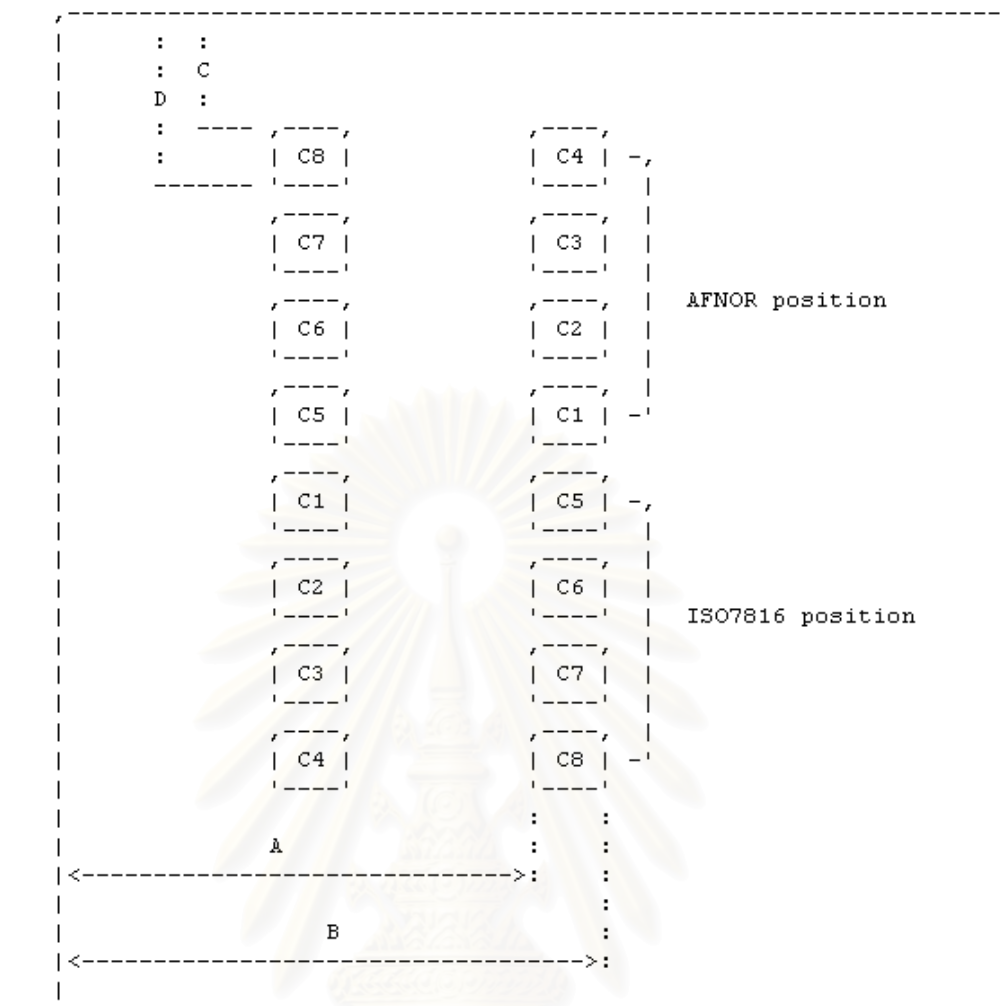
รูปที่ 2.23 ข้อกำหนดบางส่วนตามมาตรฐาน ISO 7816-1 ที่มา: ISO 7816 [3]



รูปที่ 2.24 ข้อกำหนดบางส่วนตามมาตรฐาน ISO 7816-2 ที่มา: ISO 7816 [3]

2.1.6.2.2 **มาตรฐาน** AFNOR

มีขาสัญญาณเหมือนกับ มาตรฐาน ISO 7816 จะแตกต่างกันตรงที่การจัดเรียงลำดับของขาสัญญาณ และตำแหน่งของขาสัญญาณ โดยในรูปที่ 2.25 จะแสดงถึงรูปแบบการจัดเรียงของขาสัญญาณ และตำแหน่งหน้าสัมผัสของขาสัญญาณ (Pin contact) บนตัวสมาร์ตคาร์ด เปรียบเทียบระหว่างแบบ ISO 7816 กับแบบ AFNOR



Pin Assignement:
C1 : Vcc = 5V
C2 : Reset
C3 : Clock
C4 : RFU
C5 : Gnd
C6 : Vpp
C7 : I/O
C8 : RFU

Contact Location:

All the sizes are in milimeters

	ISO7816 location				AFNOR location			
	A	B	C	D	A	B	C	D
C1	10.25	12.25	19.23	20.93	17.87	19.87	16.69	18.39
C2	10.25	12.25	21.77	23.47	17.87	19.87	14.15	15.85
C3	10.25	12.25	24.31	26.01	17.87	19.87	11.61	13.31
C4	10.25	12.25	26.85	28.55	17.87	19.87	9.07	10.77
C5	17.87	19.87	19.23	20.93	10.25	12.25	16.69	18.39
C6	17.87	19.87	21.77	23.47	10.25	12.25	14.15	15.85
C7	17.87	19.87	24.31	26.01	10.25	12.25	11.61	13.31
C8	17.87	19.87	28.85	28.55	10.25	12.25	9.07	10.77

NB: The AFNOR location is transitional, and has been used for compatibility reasons with existing magnetic stripe cards.

รูปที่ 2.25 ข้อกำหนดต่างๆ ตามมาตรฐาน AFNOR เปรียบเทียบกับมาตรฐาน ISO 7816

ที่มา: ISO 7816 [3]

โดยในงานวิจัยชิ้นนี้ ได้ใช้สมาร์ตคาร์ดแบบมีหน่วยประมวลผลในตัว แบบมีหน้าสัมผัสตามมาตรฐาน ISO 7816 [3] เนื่องจากต้องใช้หน่วยประมวลผลในการประมวลผลตรวจสอบลายนิ้วมือ

2.2 งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยต่างๆ ที่เกี่ยวข้องกับงานวิจัยนี้พบว่ามีการออกแบบระบบตรวจสอบลายนิ้วมือให้สามารถประมวลบนสมาร์ตคาร์ดได้ แต่ยังคงมีข้อจำกัดอยู่บางประการ อาทิ ชนิดของหน่วยประมวลที่ใช้ในการตรวจสอบลายนิ้วมือบนสมาร์ตคาร์ดต้องใช้แบบ 32 บิต ซึ่งเป็นหน่วยประมวลที่มีขนาดใหญ่ มีราคาแพง และใช้ระยะเวลาในการประมวลผลเป็นเวลานาน เป็นต้น

2.2.1 Collaborative Fingerprint Authentication by Smartcard and a Trusted Host [2]

ในงานวิจัยนี้ได้พัฒนาระบบตรวจสอบลายนิ้วมือบนจาวาสมาร์ตคาร์ดที่ความเร็ว 5 MHz ซึ่งเป็นสมาร์ตคาร์ดที่มีตัวแปลภาษาจาวาอยู่ภายใน โดยมีส่วนที่น่าสนใจคือการออกแบบให้มีการคำนวณข้อมูลในการเปรียบเทียบก่อนบางส่วนบนโฮสต์ เพื่อลดการคำนวณของสมาร์ตคาร์ดลง โดยเมื่อทำการสร้างแม่แบบลายนิ้วมือผู้ใช้ที่แท้จริง (Master template) จะมีการคำนวณหาค่าตำแหน่งเฉลี่ย (Average position) ของแม่แบบลายนิ้วมือผู้ใช้ที่แท้จริง โดยจะเรียกค่าที่คำนวณได้ว่าค่า MP และคำนวณหาค่ามุมทิศทางในการวางตัว (Orientation) ของจุดในแม่แบบลายนิ้วมือผู้ใช้ที่แท้จริง โดยจะเรียกค่าที่คำนวณได้ว่าค่า MO และเก็บค่าทั้งสองไว้ในแม่แบบลายนิ้วมือภายในสมาร์ตคาร์ด

ในระหว่างการตรวจสอบลายนิ้วมือเมื่อระบบได้รับแม่แบบลายนิ้วมือที่ต้องการตรวจสอบเข้ามา (Live template) แล้ว จะทำการคำนวณหาค่าตำแหน่งเฉลี่ยของแม่แบบลายนิ้วมือที่ต้องการตรวจสอบ โดยจะเรียกค่าที่คำนวณได้ว่าค่า LP และคำนวณหาค่ามุม

ทิศทางในการวางตัวของจุดในแม่แบบลายนิ้วมือที่ต้องการตรวจสอบ โดยจะเรียกค่าที่คำนวณได้ว่าค่า LO จากนั้นค่า MP และ MO ที่เก็บไว้ในสมาร์ตคาร์ดจะถูกส่งมายังโฮสต์ และโฮสต์จะทำการเปลี่ยนตำแหน่งของจุดที่อยู่ในแม่แบบลายนิ้วมือที่ต้องการตรวจสอบที่ได้รับเข้ามาจากผู้ใช้แล้ว ตามค่าความแตกต่างระหว่าง (MP-LP) และ (MO-LO) จากนั้นแม่แบบลายนิ้วมือที่ต้องการตรวจสอบที่ผ่านขั้นตอนการเปลี่ยนตำแหน่งแล้ว จะถูกส่งไปยังสมาร์ตคาร์ดเพื่อทำการเปรียบเทียบระหว่างจุดต่อจุด ด้วยวิธีการดังกล่าวนี้จะทำให้สมาร์ตคาร์ดไม่ต้องคำนวณการเปลี่ยนตำแหน่งและการหมุน อีกต่อไป

ข้อสังเกตของงานวิจัยนี้ คือ การหมุนของภาพลายนิ้วมือที่รับเข้ามาจะต้องถูกจำกัดโดยการติดตั้งตัวนำทางนิ้วมือบนเครื่องอ่านลายนิ้วมือ

2.2.2 Moving-Window Algorithm For Fast Fingerprint Verification [8]

ในงานวิจัยนี้ได้นำเสนออัลกอริทึมโดยใช้วิธีบันทึกพื้นที่รอบๆ จุดสำคัญบนเส้นลายนิ้วมือ โดยใช้พื้นที่ซึ่งใกล้จุดกึ่งกลางมากที่สุดเป็นหน้าต่างสำหรับติดตาม (Tracking window) เพื่อใช้ปรับมุมของภาพลายนิ้วมือที่รับเข้ามาให้ตรงกับแม่แบบลายนิ้วมือที่เก็บไว้ จากนั้นทำการเปรียบเทียบแบบ Pattern matching โดยใช้วิธีเลื่อนหน้าต่าง (Moving-Windows) ซึ่งในงานวิจัยชิ้นนี้มุ่งเน้นในการปรับปรุงเวลาที่ใช้ในการตรวจสอบให้ประมวลผลได้รวดเร็วขึ้น

ข้อสังเกตของงานวิจัยนี้ คือ การหมุนของภาพลายนิ้วมือที่รับเข้ามาจะต้องถูกจำกัดโดยการติดตั้งตัวนำทางนิ้วมือบนเครื่องอ่านลายนิ้วมือ ซึ่งจะช่วยจำกัดให้มุมไม่เปลี่ยนแปลงเกิน 5 องศา

2.2.3 Logical Templates for Feature Extraction in Fingerprint Images [9]

ในบทความ [9] ได้นำ Logical template มาใช้งานในขั้นตอนการค้นหาลักษณะสำคัญ (Feature Extraction) เพื่อให้การค้นหาจุดสำคัญบนเส้นลายนิ้วมือ ในภาพลายนิ้วมือที่มีคุณภาพต่ำ มีความเชื่อถือได้ โดยส่วนที่น่าสนใจมีดังนี้

1. **ทำการสร้าง** Orientation Image

   1.1 นำเอาภาพลายนิ้วมือที่รับเข้ามาทำให้เรียบขึ้นโดยใช้ 5×5 Gaussian Kernel of standard deviation 1.0

   1.2 แบ่งภาพออกเป็น 16×16 บล็อก โดยให้มีหนึ่งพิกเซลซ้อนทับกัน เพื่อทำการหาตำแหน่งทิศทางของเส้น (Ridge orientation)

2. **ทำการสร้างภาพของเส้นลายนิ้วมือ** (Ridge) **และร่อง** (Valley)

   ภาพที่สร้างจะเป็นภาพชนิดสองระดับ โดยในส่วนของพิกเซลที่มีค่าเป็น 1 ในกรณีของภาพเส้นลายนิ้วมือ หมายถึงเส้นลายนิ้วมือ และในกรณีของภาพร่องหมายถึงส่วนที่เป็นร่อง นำภาพลายนิ้วมือที่รับเข้ามาผ่านขั้นตอนการทำให้เรียบโดยใช้ค่าที่ได้จากขั้นตอนที่ 1 จุดประสงค์ของการทำให้เรียบเพื่อกำจัดรายละเอียดที่มากเกินไป เช่น จุดที่เส้นลายนิ้วมือสั้นมากจนสามารถเปรียบเทียบได้ว่าเป็นจุด (Island) และทำการรวมเส้นย่อยที่อยู่ใกล้เคียงกันมากเข้าด้วยกัน

   ในการทำลายเส้นให้บาง (Thinned) กรณีของเส้นลายนิ้วมือทำได้โดยหาค่าต่ำสุดสัมพัทธ์ (Local minima) และกรณีของร่อง หาโดยใช้ค่าสูงสุดสัมพัทธ์ (Local maxima) เพื่อหาทิศทางของเส้น ในการแก้ปัญหาที่มีพิกเซลของเส้นลายนิ้วมือ (หรือร่อง) จำนวนเล็กน้อยที่จะสูญหายในบางครั้ง ที่บริเวณใกล้กับจุดที่เส้นลายนิ้วมือแยกออกจากกัน โดยจุดที่สูญหายไปควรจะเป็นจุดที่มีระดับความเทาใกล้เคียงกับจุดของเส้นลายนิ้วมือ (หรือร่อง) ในภาพที่ถูกทำให้เรียบแล้ว การทำลายเส้นให้บางมีขั้นตอน

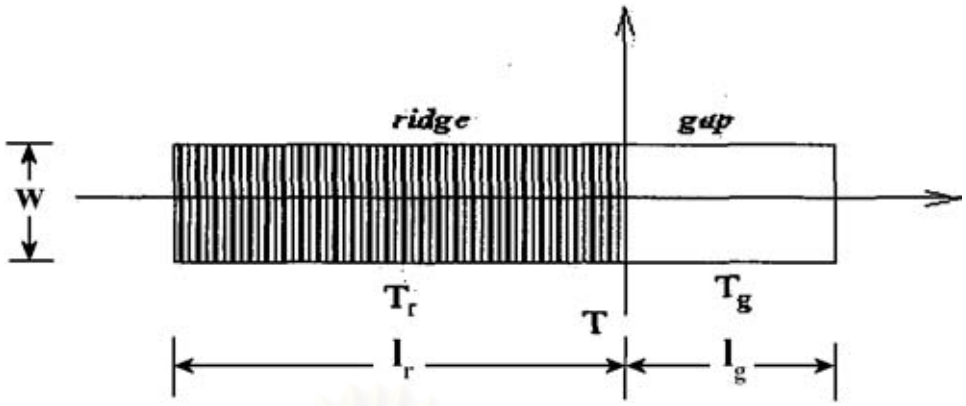
คือ ทำการคำนวณหาค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐาน (Standard deviation) ของระดับความเทา ภายในพื้นที่ขนาดเล็กรอบจุดสำคัญบนเส้นลายนิ้วมือที่พิจารณา โดยกำหนดให้เป็น μ และ σ และกำหนดให้ $v_{i,j}$ เป็นระดับความเทาของจุดที่ตั้งอยู่ที่ตำแหน่ง (i, j) ถ้า $v_{i,j} < \mu - k\sigma,$ แล้ว จะกำหนดให้จุดนี้เป็นจุดเชื่อมต่อของเส้นลายนิ้วมือ ในทางกลับกัน ถ้า $v_{i,j} > \mu + k\sigma,$ แล้ว จะกำหนดให้จุดนี้เป็นจุดเชื่อมต่อของร่อง โดยใช้ขนาดพื้นที่ = 4×4 และ $k = 1$ ในการพิจารณา

3. **ทำการค้นหาจุดสำคัญบนเส้นลายนิ้วมือ** (Minutiae) **โดยใช้วิธี** Logical-Template-Based

วิธีการใช้ Template-matching จะพิจารณาถึงตัวแปร 3 สิ่ง ของเส้นลายนิ้วมือ (ridge) ดังนี้

1. ความกว้างของเส้น (Ridge width)
2. ตำแหน่งทิศทางของเส้น
3. มุมระหว่างเส้นลายนิ้วมือที่แยกออกจากกัน (เป็นกรณีที่เส้น 1 เส้นแยกออกเป็น 2 เส้น)

การขึ้นอยู่กับความกว้างของเส้นจะถูกกำจัดออกไปโดยการทำลายเส้นให้บาง (Thinned ridge) ของภาพสองระดับ และการขึ้นอยู่กับมุมระหว่างเส้นที่แยกจากกันจะถูกกำจัดโดยการตรวจสอบการแยกของเส้น ซึ่งใช้การดูที่จุดสิ้นสุดของภาพร่อง ดังนั้นจึงมีเพียงตำแหน่งทิศทางของเส้นที่ต้องพิจารณา



รูปที่ 2.26 Logical template

จากรูปที่ 2.26 กำหนดให้ Logical template เป็น T และมีรูปร่างเป็นสี่เหลี่ยม ภายในประกอบไปด้วยสี่เหลี่ยมย่อย 2 อัน คือ T_r และ T_g ซึ่งใช้ในการตรวจจับเส้นลายนิ้วมือ (หรือร่อง) และช่องว่างที่ต่อมา โดยที่ความยาวของ T_r และ T_g ถูกกำหนดเป็น l_r และ l_g ซึ่งเป็นไปตามความยาวที่สั้นที่สุดของเส้นลายนิ้วมือ และความยาวที่สั้นที่สุดของช่องว่างที่อยู่ที่จุดสิ้นสุดของเส้นลายนิ้วมือ ดังนั้นขนาดของ T จะเท่ากับ $w \times (l_r + l_g)$ โดยที่ w คือ ความกว้าง ซึ่งขึ้นอยู่กับปัจจัยต่างๆ เช่น ความผิดเพี้ยนของข้อมูล (data distortion) และระยะทางระหว่างเส้น (inter-ridge distance) ซึ่งการทดลองภายในบทความ [9] ได้กำหนดให้ l_r = 6, l_g = 3 และ w = 3

จากตรรกะของ Logical template ข้างต้น สามารถอธิบายได้ว่า จะต้องได้ค่าเป็นจริง เมื่อ Logical template ย่อยทั้ง 2 มีค่าเป็นจริง เท่านั้น

$$E = E_r \,\&\, E_g$$

โดยที่ E , E_r และ E_g คือ Logical expression แทน T , T_r และ T_g

E_r จะให้ค่าเป็นจริงเมื่อคอลัมน์ในสี่เหลี่ยมย่อย มีอย่างน้อย 1 พิกเซล เป็นเส้นลายนิ้วมือ (หรือร่อง)

E_g จะให้ค่าเป็นจริงเมื่อไม่มีพิกเซลของเส้นลายนิ้วมือ (หรือร่อง) อยู่ในสี่เหลี่ยมย่อย T_g

จากสิ่งที่กล่าวมาข้างต้น สามารถเขียนเป็นสมการได้ ดังนี้

$$E_r = \left(N(T_r) = l_r\right), \text{ และ } E_g = \left(N(T_g) = 0\right),$$

โดยที่ $N(A)$ คือ ฟังก์ชันที่จะให้ค่าออกมาเป็นจำนวนของคอลัมน์ที่ไม่เป็น 0 ใน Binary matrix A

นอกจากนี้เพื่อให้รองรับความผิดเพี้ยน (Distortion) และทำให้ง่ายต่อการนำไปประยุกต์ใช้ จึงปรับสมการเป็นดังนี้

$$E = \left(w_r M(T_r) + w_g M(T_g)\right) \geq \Delta,$$

โดยที่ $M(A)$ คือ ฟังก์ชันที่จะให้ค่าออกมาเป็นจำนวนของหนึ่งใน Binary matrix A, w_r และ w_g คือค่าน้ำหนักซึ่งจะสอดคล้องกับเส้นลายนิ้วมือ และส่วนที่เป็นช่องว่างใน Logical expression, Δ คือค่าขีดแบ่ง (Threshold)

ในการนำขั้นตอนค้นหาจุดสำคัญบนเส้นลายนิ้วมือไปใช้งานจริง จะมี 2 ขั้นตอนดังนี้

1. เพื่อทำการปรับปรุงอัลกอริทึมให้มีประสิทธิภาพสูงขึ้น Logical template จะถูกนำไปใช้เฉพาะเซตย่อยของพิกเซลเส้นลายนิ้วมือ (หรือร่อง) ที่ดูเหมือนจะเป็นส่วนที่เส้นลายนิ้วมือ (หรือร่อง) สิ้นสุด

2. Logical template จะถูกนำไปใช้กับแต่ละพิกเซลของเส้นลายนิ้วมือ (หรือร่อง) ที่ถูกเลือกในขั้นตอนที่ 1 โดยใช้ตำแหน่งทิศทางของเส้นลายนิ้วมือ

(หรือร่อง) ในบริเวณนั้นพิจารณาตำแหน่งของ Local template โดยถ้า θ คือ ค่าตำแหน่งทิศทางของบริเวณนั้นแล้ว Template จะถูกนำไปใช้ 2 ครั้ง คือ ในตำแหน่งทิศทาง θ และ $\theta + \P$

4. **การประมวลผลภายหลัง** (Postprocessing)

เนื่องจากในกรณีที่ภาพลายนิ้วมือที่รับเข้ามามีคุณภาพต่ำ จะทำให้เกิดจุดสำคัญบนเส้นลายนิ้วมือปลอม (False Minutiae) ซึ่งจุดสำคัญบนเส้นลายนิ้วมือส่วนเกินเหล่านี้จะถูกกำจัดออกได้ โดยการประมวลผลภายหลัง ซึ่งในการทดลองนี้ได้ใช้วิธีการอย่างง่าย โดยกำหนดพื้นที่ย่อยขนาด 4×4 ซึ่งมีจุดศูนย์กลางอยู่ตรงจุดที่มีความเป็นไปได้ว่าเป็นจุดสำคัญบนเส้นลายนิ้วมือ

โดยถ้า $\mu_l + k_1\sigma_l < \mu_g + k_2\sigma_g$ แล้วจะไม่สนใจจุดสำคัญบนเส้นลายนิ้วมือ (Minutiae) นั้น

เมื่อ μ_l คือ ค่าเฉลี่ยเฉพาะส่วน (Local mean)

μ_g คือ ค่าเฉลี่ยรวม (Global mean)

σ_l คือ ค่าเบี่ยงเบนมาตรฐานเฉพาะส่วน (Local standard deviation)

σ_g คือ ค่าเบี่ยงเบนมาตรฐานรวม (Global standard deviation)

$K_1 = K_2 = 1$

2.2.4 การประมวลลายพิมพ์นิ้วมือเบื้องต้นสำหรับระบบตรวจพิสูจน์ลายนิ้วมืออัตโนมัติ [10]

ในงานวิทยานิพนธ์ [10] ได้นำเสนอ การปรับปรุงขั้นตอนการประมวลผลภาพเบื้องต้น (Preprocessing) เพื่อให้มีประสิทธิภาพและเพิ่มความเป็นอัตโนมัติมากขึ้น โดย

การประมวลผลภาพเบื้องต้นเป็นการปรับปรุงคุณภาพของภาพลายนิ้วมือที่รับเข้ามาให้มีคุณภาพดียิ่งขึ้นและลดข้อมูลให้มีขนาดน้อยลงเหลือไว้เฉพาะข้อมูลที่จำเป็น ซึ่งประกอบไปด้วยขั้นตอนต่างๆ ดังนี้

1. การปรับความสว่าง (Brightness)
2. การปรับความแตกต่างแสง (Contrast Normalization)
3. การกำจัดสัญญาณรบกวน (Noise Reduction)
4. การแปลงภาพเป็นภาพสองระดับ (Binarization)
5. การทำให้วัตถุในภาพบาง (Thinning)

ส่วนที่น่าสนใจในงานวิทยานิพนธ์ [10] มีดังนี้

1. การทำภาพให้เรียบและลดสัญญาณรบกวน (Smoothing & Noise Reduction)

   โดยทั่วไปจะใช้วิธีการเฉลี่ยค่ารอบย่าน (Average Filtering) ซึ่งมีผลข้างเคียงคือ ภาพจะเบลอและรายละเอียดสัญญาณรบกวนชัดเจนขึ้น ซึ่งสามารถแก้ไขโดยใช้ฟิลเตอร์แบบมัธยฐาน (Median Filtering) ซึ่งเป็นฟิลเตอร์ชนิดความถี่ต่ำผ่าน โดยเลือกใช้กรอบขนาด 3×3 ครอบลงไปทุกๆ จุดในภาพ จากนั้นหาค่ามัธยฐานของชุดข้อมูลตั้งแต่ X_0 ถึง X_8 แล้วแทนในตำแหน่ง X_0 ดังแสดงในรูปที่ 2.27

X_3	X_2	X_1
X_4	X_0	X_8
X_5	X_6	X_7

รูปที่ 2.27 ฟิลเตอร์แบบมัธยฐาน ขนาด 3×3

2. การปรับปรุงการแปลงภาพเป็นแบบสองระดับ

<u>วิธีเบื้องต้น</u> :

$$g(x,y)=\begin{cases}1 & \text{ถ้า} \quad f(x,y)>T \\ 0 & \text{ถ้า} \quad f(x,y)\le T\end{cases}$$

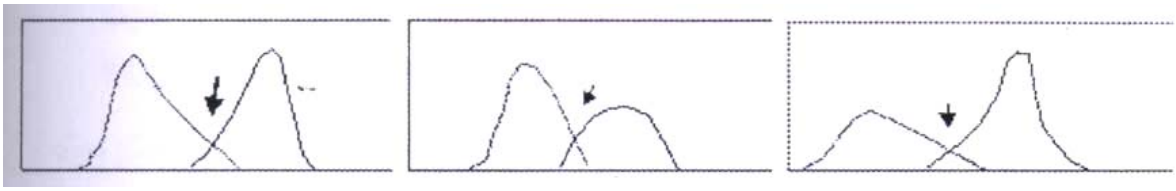
โดย $f(x,y)$ คือค่าสีที่ได้จากการอ่านค่าภาพเริ่มต้น, $g(x,y)$ คือค่าสีใหม่ที่แทนกลับลงไปในภาพ และ T คือ ค่าขีดแบ่ง (เป็นค่าที่ใช้ในการตัดสินในการแปลงจากค่าระดับเทาที่รับเข้ามาเป็นค่า 1 หรือ 0 โดยหากค่าระดับเทาที่รับเข้ามามีค่าน้อยกว่าค่าขีดแบ่งจะถูกกำหนดค่าเป็น 0 หากค่าระดับเทาที่รับเข้ามามีค่ามากกว่าค่าขีดแบ่งจะถูกกำหนดเป็น 1)

<u>วิธีทั่วไป</u> :

1. ผู้ใช้จะเป็นคนกำหนดค่าขีดแบ่งที่เหมาะสม โดยนำภาพลายนิ้วมือมาเขียนฮีสโตแกรมระดับเทา และดูจากจุดแบ่งแยกค่าการกระจายของพื้นหลังและค่าการกระจายของวัตถุ

2. ทำการเลือกค่าขีดแบ่งที่เหมาะสม โดยพิจารณาจากฮีสโตแกรมของภาพลายนิ้วมือ จะพบว่าฮีสโตแกรมแบ่งออกเป็น 2 กลุ่มอย่างชัดเจน ซึ่งค่าตรงกลางระหว่าง 2 กลุ่มจะเป็นค่าขีดแบ่งที่เหมาะสม

3. นำเอาข้อมูลความถี่ระดับเทาของภาพลายนิ้วมือมาสร้างเส้นโค้งความถี่ เนื่องจากลักษณะที่แยกเป็นสองของเส้นโค้ง ทำให้ในหนึ่งภาพลายนิ้วมือสามารถปรับเป็นเส้นโค้งเรียบ 2 รูปได้



รูปที่ 2.28 จุดแบ่งของค่าขีดแบ่งที่เหมาะสมเมื่อพิจารณาจากเส้นโค้งความถี่

[10]

เพื่อให้สามารถคำนวณหาค่าขีดแบ่งได้โดยอัตโนมัติ จึงทำการหาค่าขีดแบ่งด้วยข้อมูลทางสถิติ โดยวิเคราะห์ข้อมูลจากการวัดแนวโน้มสู่ส่วนกลางและการกระจาย

เนื่องจากภาพลายนิ้วมือจะประกอบไปด้วย 2 ส่วนเท่ากัน คือ เส้นสันหรือวัตถุ และเส้นร่องหรือพื้นหลัง ค่าขีดแบ่งจึงควรอยู่ตรงกลางของข้อมูลการกระจายจุดภาพ โดยมีวิธีทางคณิตศาสตร์อยู่หลายวิธี ซึ่งวิธีการที่เหมาะสม คือ ใช้ค่ามัธยฐานหรือค่าเฉลี่ย เนื่องจากถ้าใช้ฐานนิยมเป็นค่าขีดแบ่งจะเกิดปัญหา เพราะว่าค่าขีดแบ่งอาจจะอยู่ในพื้นหลัง (เส้นร่อง) หรือวัตถุ (เส้นสัน) ซึ่งไม่ถูกต้อง

2.2.5 Adaptive image normalisation based on block processing for enhancement of fingerprint image [11]

ในบทความนี้ [11] ได้นำเสนอ วิธีการการปรับปรุงคุณภาพของภาพลายนิ้วมือในส่วนก่อนการค้นหาจุดลักษณะสำคัญบนเส้นลายนิ้วมือ (Image preprocessing) โดยได้ออกแบบให้มีการทำ Normalisation ชนิดที่มีที่การปรับปรุงให้เหมาะสมกับระบบการทำงานที่มีการแบ่งภาพลายนิ้วมือออกเป็นส่วนๆ ในการประมวลผล (Block processing) สำหรับใช้งานในระบบวิเคราะห์ภาพลายนิ้วมือแบบอัตโนมัติ

ขั้นตอนการปรับปรุงคุณภาพของภาพลายนิ้วมือที่รับเข้ามาจากเครื่องอ่านลายนิ้วมือ สามารถแบ่งได้ออกเป็น 2 ขั้นตอนหลักๆ ดังต่อไปนี้

1. **การนำภาพที่รับเข้ามาแบ่งออกเป็นส่วนย่อย ๆ**

ภาพลายนิ้วมือที่ได้รับเข้ามาจะถูกแบ่งออกเป็นส่วนย่อยๆ ขนาด $K \times L$ และเริ่มต้นเข้าสู่ขั้นตอนการเลือกส่วนที่สนใจในการประมวลผลออกมา

2. **ทำการคำนวณหาค่าตัวแปรต่าง ๆ ที่จำเป็นสำหรับการประมวลผล**

ค่าตัวแปรต่างๆ สำหรับการทำ Normalisation ของภาพลายนิ้วมือจะถูกกำหนดค่าตามข้อมูลทางสถิติ เช่น ค่าเฉลี่ยโดยประมาณ และค่าความแปรปรวนตามแต่ละส่วนย่อยๆ

สำหรับภาพลายนิ้วมือ I ที่ได้รับมาซึ่งถูกกำหนดให้อยู่ในรูปของเมตริกซ์ขนาด $N \times M$ โดย $I(i, j)$ แสดงถึงค่าความเข้มของพิกเซล ในแถวที่ i และคอลัมน์ที่ j , โดย Hong และ Jain ได้แสดงขั้นตอนการทำ Normalisation ดังนี้ [12]

$$G(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{(VAR_0 (I(i,j) - \hat{M})^2}{\hat{VAR}}} & I(i,j) > \hat{M} \\ M_0 - \sqrt{\dfrac{(VAR_0 (I(i,j) - \hat{M})^2}{\hat{VAR}}} & otherwise \end{cases}$$

โดย

M_0 คือ ค่าเฉลี่ยที่ต้องการ

VAR_0 คือ ค่าความแปรปรวนที่ต้องการ

$\hat{M}$ คือ ค่าเฉลี่ยที่คำนวณได้จากภาพที่รับเข้ามาประมวลผล

$\hat{VAR}$ คือ ค่าความแปรปรวนที่คำนวณได้จากภาพที่รับเข้ามาประมวลผล

เนื่องจากค่าตัวแปรทางสถิติต่างๆ ภายในภาพ ซึ่งได้แก่ ค่าเฉลี่ยที่ต้องการและค่าความแปรปรวนที่ต้องการ สำหรับภาพทั่วไปจะปรับค่าเหล่านั้นตามคุณสมบัติ

ของภาพที่รับเข้ามาประมวลผล ซึ่งจะใช้ค่าเหล่านั้นเป็นค่าคงที่เท่ากันหมดทั่วทั้งภาพ แต่ในกรณีของภาพลายนิ้วมือที่รับเข้ามาประมวลผล บางครั้งภาพลายนิ้วมือที่รับเข้ามาอาจจะไม่สมบูรณ์หรือมีคุณภาพต่ำ เนื่องมาจากกรณีที่ใช้เครื่องอ่านลายนิ้วมือแบบอิเล็คทรอนิคส์ ผู้ใช้อาจจะออกแรงกดหรือสัมผัสที่หน้าสัมผัสของเครื่องอ่านลายนิ้วมือไม่สม่ำเสมอ หรือในกรณีที่ใช้หมึกพิมพ์ลายนิ้วมือลงบนกระดาษแล้วเก็บข้อมูลเข้าสู่ระบบโดยใช้ Scanner การกระจายความเข้มของน้ำหมึกที่ใช้พิมพ์ภาพลายนิ้วมืออาจไม่สม่ำเสมอ ในการแก้ปัญหาดังกล่าว ในบทความนี้ [11] ได้นำเสนอวิธีการทำ Normalisation แบบใหม่ โดยออกแบบค่า M_0 และ VAR_0 ให้สามารถปรับเปลี่ยนได้เหมาะสมสำหรับแต่ละส่วนย่อยๆ เฉพาะบริเวณหนึ่งๆ ของภาพลายนิ้วมือที่รับเข้ามาประมวลผล ซึ่งประกอบไปด้วยขั้นตอน ดังนี้

- Histogram equalization

  เป็นการจับคู่ระหว่างค่าระดับความเทา p เข้ากับระดับความเทา q เพื่อให้การกระจายค่าของระดับความเทา q มีความสม่ำเสมอ [13]

- **การเลือกส่วนของภาพที่สนใจในการประมวลผล** (ROI : Region Of Interest)

  เนื่องจากภาพลายนิ้วมือที่รับเข้ามาอาจจะมีพื้นหลังของภาพที่มีสัญญาณรบกวน ซึ่งอาจจะทำให้อัลกอริทึมประมวลผลนอกภาพลายนิ้วมือได้ โดยจะส่งผลให้เกิดความผิดพลาดขึ้น และอาจจะส่งผลรบกวนการประมวลผลในลำดับถัดไปได้ ทำเกิดผลลัพธ์ที่ผิดพลาดขึ้น

  ดังนั้นพื้นที่ของภาพลายนิ้วมือภายในภาพที่รับเข้ามาทำการประมวลผลนั้นควรจะมีการเลือกส่วนที่สนใจในการประมวลผลไว้

ล่วงหน้าก่อน โดยใช้วิธีการคือ ทำการแบ่งภาพที่รับเข้ามาออกเป็นส่วนๆ ที่ไม่ซ้อนทับกันขนาด $K \times L$, ในบทความนี้ได้ใช้ขนาด 16×16 จากนั้นจะทำการพิจารณาแต่ละส่วนย่อยๆ โดยดูจากค่าความแปรปรวนของค่าระดับความเทา ส่วนที่มีค่าความแปรปรวนของค่าระดับความเทาสูงกว่าที่กำหนดจะถูกเลือกเป็นส่วนที่จะถูกประมวลผลในขั้นตอนต่อไป และส่วนที่มีค่าความแปรปรวนของค่าระดับความเทาต่ำกว่าที่กำหนดจะถูกกำหนดให้เป็นส่วนที่ไม่มีการประมวลผลต่อไป

กำหนดให้ v_i เป็นค่าความแปรปรวนของค่าระดับความเท่าสำหรับส่วนย่อยที่ i ขั้นตอนการเลือกส่วนย่อยที่สนใจในการประมวลผลสามารถแสดงเป็นสมการ ดังนี้

$$B_{ROI} = \begin{cases} B_{origin} & \text{ถ้า } v_i > v_T \\ O & \textbf{ในกรณีอื่นๆ} \end{cases}$$

โดย B_{ROI} คือ ส่วนของภาพที่สนใจในการประมวลผล

B_{origin} คือ ข้อมูลของภาพลายนิ้วมือดั้งเดิมที่รับเข้ามาประมวลผล

O คือ ส่วนที่ไม่สนใจในการประมวลผล

เนื่องจากส่วนที่มีลักษณะเป็นเนื้อเดียวกันของภาพลายนิ้วมือที่รับเข้ามายังอาจจะปรากฏอยู่ภายในภาพลายนิ้วมือได้ ดังนั้นจึงมีความจำเป็นต้องตรวจสอบข้อมูลภาพลายนิ้วมือก่อนการคัดเลือก โดยผ่านขั้นตอนการฟิลเตอร์

- Adaptive image normalisation based on local property

สำหรับส่วนที่สนใจในการประมวลผล ที่ได้รับการคัดเลือกมานั้น ค่าเริ่มต้นของค่าเฉลี่ยที่ต้องการ (M_0^d) และค่าความแปรปรวนที่ต้องการ (VAR_0^d) จะถูกกำหนดค่า โดยการประมาณค่าทางสถิติของ ROI ซึ่งค่าเหล่านี้จะทำหน้าที่เป็นค่าอ้างอิงในกระบวนการปรับค่าตัวแปร จากนั้นจะใช้อัลกอริทึมในการปรับค่าเริ่มต้นตามคุณสมบัติเฉพาะของแต่ละพื้นที่ย่อยๆ ในแต่ละส่วนโดยมีสมการดังต่อไปนี้

$$M_i^d = M_0^d - \alpha_1 \cdot (\hat{M}_i - M_0^d)$$

$$VAR_i^d = VAR_0^d - \alpha_2 \cdot (\hat{VAR}_i - VAR_0^d)$$

โดย α_1 และ α_2 คือ ค่าสัมประสิทธิ์ถ่วงน้ำหนักที่แสดงถึงระดับของการกระจายในภาพผลลัพธ์

M_i คือ ค่าเฉลี่ยที่คำนวณได้จากส่วนที่ i

VAR_i คือ ค่าความแปรปรวนที่คำนวณได้จากส่วนที่ i

M_i^d คือ ค่าเฉลี่ยเริ่มต้นที่ได้

VAR_i คือ ค่าความแปรปรวนเริ่มต้นที่ได้

M_0^d คือ ค่าเฉลี่ยของระดับเทาที่ต้องการ

VAR_i^d คือ ค่าความแปรปรวนที่ต้องการ

บทที่ 3
ระบบตรวจสอบลายนิ้วมือที่ได้พัฒนาขึ้นใหม่

จุดเด่นของการออกแบบให้หน่วยประมวลผลบนสมาร์ตคาร์ดสามารถทำการตรวจสอบลายนิ้วมือ คือ มีความปลอดภัยสูง เนื่องจากแม่แบบลายนิ้วมือของผู้ถือบัตรที่แท้จริงจะถูกเก็บไว้ภายในหน่วยความจำของสมาร์ตคาร์ด และตลอดการทำงานจะไม่มีการส่งแม่แบบลายนิ้วมือออกมาภายนอกสมาร์ตคาร์ด จึงทำให้ปลอดภัยจากการดักจับและปลอมแปลงข้อมูลแม่แบบลายนิ้วมือ

ปัญหาสำคัญของการนำระบบตรวจสอบลายนิ้วมือมาประมวลผลบนสมาร์ตคาร์ด คือ ความเร็วในการทำงานของระบบ, ข้อจำกัดต่างๆ ในการคำนวณทางคณิตศาสตร์บนหน่วยประมวลผลของสมาร์ตคาร์ด, ขนาดของหน่วยความจำชั่วคราว, ขนาดของหน่วยความจำโปรแกรมที่จะใช้ในการเก็บโปรแกรมการเปรียบเทียบลายนิ้วมือ, ขนาดของหน่วยความจำที่จะใช้เก็บแม่แบบลายนิ้วมือ และความเร็วในการส่งข้อมูลลายนิ้วมือที่ต้องการตรวจสอบไปยังสมาร์ตคาร์ด โดยในงานวิจัยนี้จะทำการออกแบบระบบตรวจสอบลายนิ้วมือบนสมาร์ตคาร์ด โดยคำนึงถึงข้อจำกัดต่างๆ ดังที่ได้กล่าวในข้างต้น

งานวิจัยนี้ได้เลือกใช้การตรวจสอบลายนิ้วมือแบบเปรียบเทียบ 1 ต่อ 1 ด้วยเหตุผลดังต่อไปนี้

1. มีรูปแบบการทำงาน โดยทำการเปรียบเทียบระหว่างภาพลายนิ้วมือที่รับเข้ามาจากเครื่องอ่านลายนิ้วมือ กับแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำของสมาร์ตคาร์ด ซึ่งเป็นการประมวลผลแบบ 1 ต่อ 1
2. ข้อจำกัดทางด้านหน่วยประมวลผลหลัก และหน่วยความจำชั่วคราวของสมาร์ตคาร์ด เนื่องจากโดยทั่วไปหน่วยประมวลผลหลักจะมีความเร็วในการประมวลผลต่ำ และหน่วยความจำชั่วคราวจะมีขนาดเล็ก จึงเหมาะสมสำหรับการตรวจสอบลายนิ้วมือแบบเปรียบเทียบลายนิ้วมือ 1 ต่อ 1 เนื่องจากมีขั้นตอนการทำงานและอัลกอริทึมที่ซับซ้อนน้อยกว่า และสามารถประมวลผลได้รวดเร็วกว่า

ขั้นตอนการทำงานของระบบตรวจสอบลายนิ้วมือที่นำมาใช้ในงานวิจัยนี้ สามารถแบ่งออกเป็น 3 ส่วนหลัก ดังนี้

3.1 **การประมวลผลภาพเบื้องต้น** (Image preprocessing)

เป็นขั้นตอนในการนำภาพลายนิ้วมือที่รับมาจากเครื่องอ่านลายนิ้วมือมาผ่านกระบวนการปรับปรุงคุณภาพของภาพ เพื่อให้ภาพลายนิ้วมือมีความเหมาะสมกับขั้นตอนการค้นหาลักษณะสำคัญ การประมวลผลภาพเบื้องต้นประกอบไปด้วยขั้นตอนย่อย ดังต่อไปนี้

3.1.1 **การทำให้เรียบและการลดสัญญาณรบกวน** (Smoothing & Noise reduction) [10]

เป็นการลดสัญญาณรบกวนในภาพ โดยใช้ฟิลเตอร์แบบมัธยฐาน (Median Filtering) ซึ่งเป็นฟิลเตอร์ชนิดความถี่ต่ำผ่าน (Low Pass Filter) โดยได้ใช้วิธีการจาก [10] ดังที่ได้อธิบายไปแล้วในบทที่ 2

3.1.2 **การปรับ** Normalisation **และความแปรปรวนของภาพ** (Variant) [11]

เป็นการปรับระดับความเทาของภาพลายนิ้วมือให้เหมาะสม โดยจะแบ่งการประมวลผลออกเป็นส่วนย่อยๆ ซึ่งทำให้ระดับความเทาของภาพระหว่างร่อง (Valley) และเส้นลายนิ้วมือ (Ridge) เปลี่ยนไปตามค่าคงที่ในแต่ละส่วน

เนื่องจากจะต้องเปลี่ยนค่าระดับความเทาของแต่ละส่วนย่อย ให้เป็นไปตามที่ต้องการ และค่าความแปรปรวนที่ได้จากการเปลี่ยนระดับความเทาที่ต้องการ ควรจะต้องมีค่าเฉลี่ยและค่าความแปรปรวนเท่าเดิม เพื่อไม่ทำให้ข้อมูลผิดเพี้ยนไป ดังนั้นค่าความแปรปรวนของทั้งหมดควรจะเท่ากับความแปรปรวนเมื่อคิดเทียบจากแต่ละส่วนย่อย โดยได้ใช้วิธีการจาก [11] ดังที่ได้อธิบายไปแล้วในบทที่ 2

3.1.3 **การเลือกส่วนของภาพที่ใช้ในการประมวลผล** (Select region of interest) [11]

เป็นการเลือกส่วนของภาพที่จะถูกนำไปใช้ในการประมวลผลลำดับถัดไป โดยพิจารณาจากความแปรปรวนของค่าระดับความเทาภายในบริเวณใกล้เคียง โดยทำการแบ่งภาพตั้งต้นเป็นส่วนย่อยๆ ซึ่งไม่ซ้อนทับกัน ขนาด 16×16 พิกเซล ในกรณีที่ค่าความแปรปรวนสูงกว่าค่าขีดแบ่งที่กำหนดไว้ก็จะเลือกส่วนย่อยนั้นให้เป็นส่วนที่สนใจในการประมวลผล หากน้อยกว่าก็จะกำหนดให้เป็นส่วนที่ไม่สนใจในการประมวลผลโดยกำหนดค่าระดับความเทาเป็น 0 คือ สีดำ และหากมีส่วนของภาพที่เดิมเป็นส่วนที่ไม่สนใจในการประมวลผลอยู่ท่ามกลางส่วนที่สนใจในการประมวลผล ก็จะเปลี่ยนส่วนนั้นให้เป็นส่วนที่สนใจในการประมวลผล โดยใช้วิธีการจาก [11] ดังที่ได้อธิบายไปแล้วในบทที่ 2

3.1.4 **การปรับค่าฮีสโตแกรมของภาพลายนิ้วมือ** (Histogram Equalization) [14]

เป็นการเพิ่มความชัดเจนของภาพโดยอาศัยการกระจายของค่าระดับความเทา ซึ่งปกติแล้วภาพลายนิ้วมือจะมีค่าระดับความเทาตั้งแต่ 0 ถึง 255 และภาพที่ดีควรจะมีการกระจายของค่าระดับความเทาโดยสม่ำเสมอ กล่าวคือ ส่วนที่เป็นเส้นลายนิ้วมือ (Ridge) ควรจะเป็นสีดำ และส่วนที่เป็นร่อง (Valley) ของลายนิ้วมือควรจะเป็นสีขาว

เนื่องจากการเก็บภาพลายนิ้วมือจากอาสาสมัคร ผ่านทางเครื่องอ่านลายนิ้วมือ ในบางครั้งภาพลายนิ้วมือที่บันทึกได้นั้น มีลักษณะไม่สม่ำเสมอ สาเหตุมาจากอาสาสมัครใช้แรงกดนิ้วมือไปยังหน้าสัมผัสของเครื่องอ่านลายนิ้วมือในแต่ละส่วนไม่เท่ากัน ซึ่งทำให้ภาพลายนิ้วมือที่ได้บางส่วนจะมืดมากเกินไป (เกิดจากออกแรงกดมากเกินไป) หรือสว่างมากเกินไป (เกิดจากออกแรงกดน้อยเกินไป) และความเข้มในแต่ละส่วนของภาพไม่สม่ำเสมอ

แนวทางแก้ไขปัญหาดังกล่าวสามารถทำได้โดยใช้การปรับค่าฮีสโตแกรมของภาพลายนิ้วมือ เพื่อให้ทุกส่วนของภาพมีความสม่ำเสมอกัน

สมการที่ใช้ในการเปลี่ยนค่าระดับความเทาของภาพขาเข้าไปยังภาพขาออก โดยพิจารณาจากภาพลายนิ้วมือที่ถูกแบ่งเป็นส่วนย่อยๆ ซึ่งใช้ขนาด 16×16 พิกเซล ดังแสดงในสมการด้านล่างนี้

กำหนดให้ค่าระดับความเทาของพิกเซลในภาพขาเข้าเป็น i และค่าระดับความเทาของพิกเซลในตำแหน่งเดียวกันของภาพขาออกเป็น I, ความถี่สะสมของฮีสโตแกรมจาก 0 ถึง i $(0 \le i \le 255,\ 0 \le k \le 255)$ สามารถหาได้ดังนี้

$$C(i) = \sum_{k=0}^{i} H(k)$$

โดย $H(k)$ คือ จำนวนพิกเซลที่มีค่าระดับความเทาเท่ากับ k

$C(i)$ คือ ความถี่สะสมของจำนวนพิกเซลที่มีระดับความเทาตั้งแต่ 0 จนถึง i

เมื่อคำนวณความถี่สะสมของแต่ละระดับความเทาได้แล้ว จะนำค่าที่ได้มาคำนวณหาค่าระดับความเทาใหม่ (I) โดยใช้สมการดังนี้

$$I = C(i) \times \frac{M}{N}$$

โดย M คือ ค่าระดับความเทาสูงสุดที่อนุญาตให้มี (255)

N คือ จำนวนพิกเซลทั้งหมดในส่วนย่อยที่พิจารณา (16×16)

หลังจากคำนวณหาค่าระดับความเทาใหม่ได้แล้ว ค่าระดับความเทาเดิม (i) จะเปลี่ยนเป็นค่าระดับความเทาใหม่ (I) ซึ่งทำให้มีค่าระดับความเทากระจายอยู่ทั่วทุกระดับความเข้ม ส่งผลให้ภาพลายนิ้วมือมีความชัดเจนเพิ่มมากขึ้น ทำให้ความแตกต่างระหว่างส่วนที่เป็นเส้นลายนิ้วมือกับส่วนร่องชัดเจนมากขึ้น

3.1.5 การแปลงเป็นภาพสองระดับ (Binarization) [11]

เป็นการปรับระดับความเทาของภาพให้เป็นสองระดับ คือ สีขาว (แทนด้วย 1) และสีดำ (แทนด้วย 0) โดยแบ่งภาพออกเป็นส่วนย่อยๆ ที่ไม่ซ้อนทับกันขนาด 16×16 พิกเซล และนำค่าเฉลี่ยของระดับความเทาในส่วนย่อยๆ นั้น มาใช้เป็นค่าในการแบ่งกลุ่มของระดับความเทาออกเป็น 2 กลุ่ม โดยปรับค่าพิกเซลเดิมที่มีระดับความเทามากกว่าหรือเท่ากับค่าเฉลี่ยให้เป็น 1 และปรับค่าของพิกเซลเดิมที่มีระดับความเทาน้อยกว่าค่าเฉลี่ยให้เป็น 0 โดยได้ใช้วิธีการจาก [11] ดังที่ได้อธิบายไปแล้วในบทที่ 2

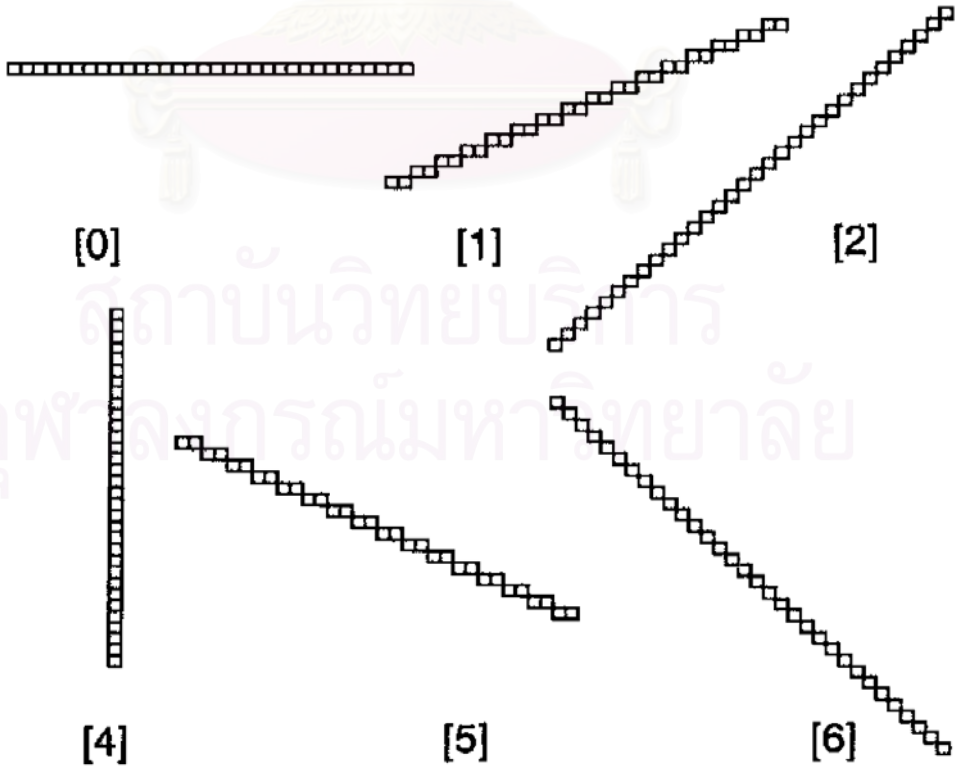
3.1.6 การหาทิศทางและการปรับแต่งเส้นลายนิ้วมือ

เนื่องจากธรรมชาติของลายนิ้วมือที่อยู่บนนิ้วมืออาจจะมีบาดแผลหรือรอยบาดเล็กๆ ส่งผลให้เส้นลายนิ้วมือขาดออกจากกัน ไม่ต่อเนื่อง ดังแสดงในรูปที่ 3.1 หรืออาจจะมีสัญญาณรบกวนเข้ามาภายในภาพ ซึ่งอาจจะเป็นสาเหตุให้เกิดจุดสำคัญบนเส้นลายนิ้วมือปลอม (false minutiae) ในขั้นตอนของการค้นหาจุดสำคัญบนเส้นลายนิ้วมือ

รูปที่ 3.1 ตัวอย่างภาพลายนิ้วมือที่มีรอยบาด

เพื่อที่จะแก้ไขปัญหา ดังที่กล่าวในข้างต้น จึงต้องมีการหาทิศทาง และปรับแต่งเส้นลายนิ้วมือ โดยหาทิศทางของเส้นลายนิ้วมือเพื่อพิจารณาว่าวางตัวอยู่ในรูปแบบใด ซึ่งได้ใช้วิธีการหลักจาก [14] แต่ได้ทำการเปลี่ยนขนาดของส่วนย่อยใน [14] จากเดิมมีขนาด 8×8 พิกเซล เป็นขนาดใหม่ 16×16 พิกเซล เพื่อให้สอดคล้องกับขนาดของส่วนย่อยในขั้นตอนก่อนหน้านี้ และได้ทำการเปลี่ยนขนาดของหน้าต่างทิศทาง จากเดิมใน [14] มีขนาด 16 พิกเซล เป็น 32 พิกเซล ซึ่งเปลี่ยนตามขนาดของส่วนย่อยที่เปลี่ยนไป

โดยมีวิธีการทำงาน คือ ทำการแบ่งภาพลายนิ้วมือออกเป็นส่วนย่อยๆ ขนาด 16×16 พิกเซล และทำการพิจารณาแนวการวางตัวของเส้นลายนิ้วมือสำหรับส่วนย่อยๆ แต่ละส่วน โดยใช้หน้าต่างของแต่ละทิศ จำนวน 8 ทิศ ได้แก่ 0 ถึง 7 ซึ่งแต่ละหน้าต่างมีความยาวเท่ากับ 32 พิกเซล ดังแสดงในรูปที่ 3.2 ในการที่จะหาทิศทางของเส้นลายนิ้วมือของแต่ละส่วนย่อย ทำได้โดยนำหน้าต่างมาเลื่อนผ่านส่วนย่อยที่ทำการแบ่งไว้ ทิศละ 16 ครั้ง เพื่อให้ครอบคลุมพื้นที่ของส่วนย่อยทั้งหมด ในแต่ละตำแหน่งที่หน้าต่างเลื่อนผ่านจะทำการคำนวณหาค่าเฉลี่ย $M(W_d)$ ของระดับความเทาในหน้าต่างส่วนนั้น จากนั้นพิจารณาค่าเฉลี่ย $M(W_d)$ ทั้งหมด โดยดูจากค่าเฉลี่ยการเลื่อนหน้าต่างว่าทิศทางใดให้ค่าเฉลี่ย $M(W_d)$ มากที่สุด ก็จะกำหนดให้ส่วนย่อยนั้นมีทิศทางตามหน้าต่างนั้น



รูปที่ 3.2 หน้าต่างทิศทาง จำนวน 8 ทิศ

เนื่องจากอาจจะมีสัญญาณรบกวนต่างๆ และรอยบาดแผลบนภาพลายนิ้วมือ ซึ่งอาจจะทำให้ข้อมูลทิศทางบางส่วนที่คำนวณออกมา มีค่าทิศทางที่ผิดพลาด ดังนั้น ค่าทิศทางของพื้นที่เหล่านั้นจำเป็นจะต้องมีการปรับค่าโดยอ้างอิงจากค่าทิศทางในพื้นที่ใกล้เคียง ซึ่งทำได้โดยคำนวณค่าฮีสโตแกรมของทิศทาง (directional histogram) $N(d)$ ของพื้นที่นั้นๆ และ 8 พื้นที่ข้างเคียงโดยรอบ โดย $N(d)$ คือ จำนวนของพื้นที่ที่มีทิศทางการวางตัวเท่ากับ d , ค่าที่มากที่สุดของ $N(d)$ จะถูกกำหนดเป็น D_1 และค่าที่มากที่สุดเป็นอันดับสองของ $N(d)$ จะถูกกำหนดเป็น D_2 , ค่า $D(x,y)$ คือค่าทิศทางที่ผ่านการปรับปรุงแล้วของพื้นที่ (x,y) เงื่อนไขในการปรับปรุงค่าทิศทาง มีดังต่อไปนี้

1. $D(x,y) = D_1, \quad \text{if } 5 \le N(D_1) \le 8$
2. $D(x,y) = \lfloor (D_1 + D_2)/2 \rfloor, \quad \text{if } 3 \le N(D_1) \le 5 \text{ and } 2 \le N(D_2) \le N(D_1) \text{ and } |D_1 - D_2| \le 2$
3. $D(x,y) = D(x,y) \text{ otherwise.}$

จากนั้นนำค่าทิศทางที่ได้ของแต่ละส่วนย่อยที่ได้รับการปรับปรุงแล้วกำหนดให้กับแต่ละพิกเซลภายในส่วนย่อยนั้น แล้วนำภาพลายนิ้วมือที่ผ่านการกำหนดทิศทางให้แต่ละพิกเซลมาทำการปรับแต่งเส้นลายนิ้วมือให้มีความต่อเนื่องมากขึ้น โดยมีขั้นตอนการทำงาน คือ ทำการพิจารณาแต่ละจุดของภาพลายนิ้วมือว่าเป็นสีขาว หรือสีดำ โดยในกรณีที่เป็นสีขาวให้ทำการนับช่องว่างที่เป็นสีขาวในแต่ละทิศทางเพื่อตรวจสอบว่ามีค่าต่ำกว่าค่าที่กำหนดหรือไม่ ถ้าค่าช่องว่างในทิศทางใดต่ำกว่าค่าที่กำหนดไว้ จะทำการนับต่อไปในทิศทางนั้นเพื่อตรวจสอบว่ามีจุดสีดำในทิศทางนั้นมากเพียงพอที่จะบอกถึงความต่อเนื่องในทิศทางนั้นหรือไม่ ถ้ามีจุดสีดำต่อไปในทิศทางดังกล่าวมากพอ จะทำการเติมสีดำให้กับจุดในช่องว่างที่เป็นสีขาวที่ได้นับไว้ในตอนต้น และสำหรับจุดที่เป็นสีดำก็นำมาพิจารณาเช่นเดียวกันแต่เปลี่ยนจุดช่องว่างเป็นจุดสีดำ และจุดที่บอกถึงความต่อเนื่องเป็นจุดสีขาว

3.1.7 การทำลายเส้นให้บาง

เป็นการทำให้เส้นลายนิ้วมือมีค่าความหนาเป็น 1 พิกเซล เพื่อให้ขั้นตอนการค้นหาจุดสำคัญบนเส้นลายนิ้วมือสามารถทำได้ง่ายขึ้น โดยมีหลักการทำงาน คือ ทำการลบพิกเซล ที่เมื่อลบแล้วไม่ทำให้เส้นลายนิ้วมือเสียความต่อเนื่องไป โดยจะทำงานวนซ้ำๆ กันจนกว่าทุกพิกเซลของภาพถูกพิจารณาหมด โดยมีขั้นตอนการประมวลผลดังนี้

1. เลือกตำแหน่งจุด (พิกเซล) ที่จะนำมาพิจารณาในรอบนั้นๆ โดยจุดที่ได้เลือกจะเป็นจุดที่เป็นขอบรอยต่อของเส้นลายพิมพ์นิ้วมือกับพื้นหลัง
2. พิจารณาการลบจุดที่เลือกพิจารณาทีละจุด ในกรณีที่เมื่อลบจุดนั้นๆ แล้วไม่ทำให้ลายนิ้วมือขาดความต่อเนื่อง โดยพิจารณาจากจำนวนของจุดรอบข้างที่เป็นส่วนของเส้นลายนิ้วมือ (สีดำ) ดังสมการด้านล่างนี้ และพิจารณาจากการเปลี่ยนแปลงของจุดรอบข้าง

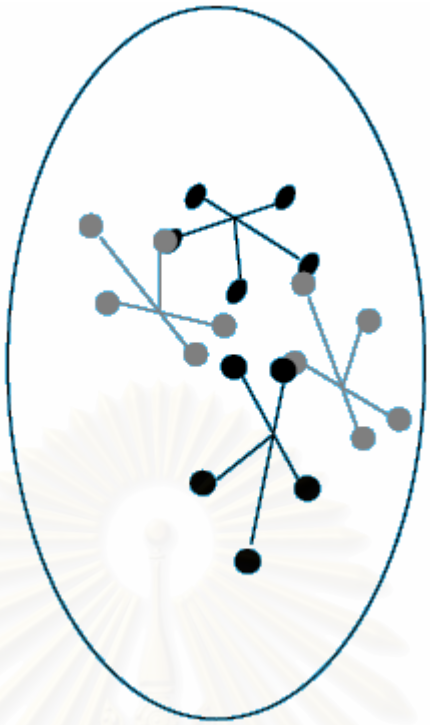
$$n(x, y) = \sum_{i=1}^{8} b(i)$$

3.2 การค้นหาลักษณะสำคัญ (Feature Extraction)

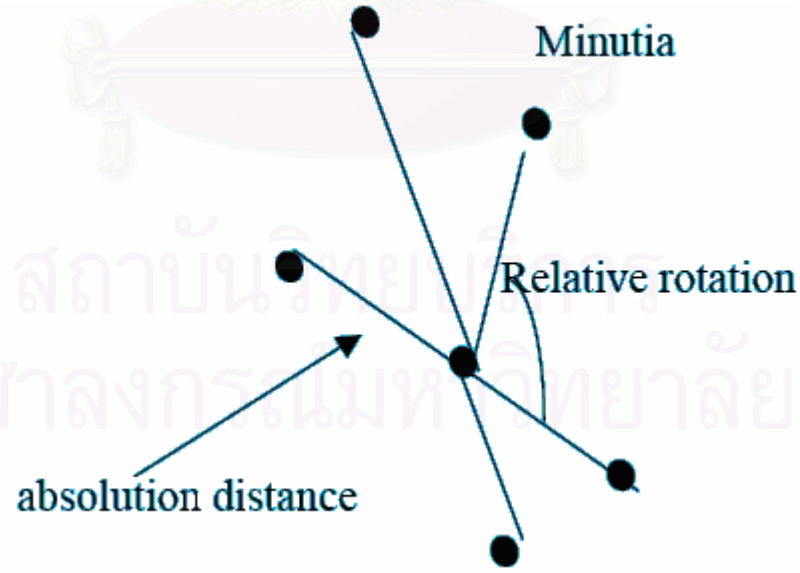
เป็นขั้นตอนค้นหาจุดสำคัญบนเส้นลายนิ้วมือ (Minutiae) โดยในขั้นตอนนี้ และในขั้นตอนการเปรียบเทียบลักษณะสำคัญ (อยู่ในหัวข้อที่ 3.3 ซึ่งจะได้กล่าวถัดไป) ได้ดัดแปลงวิธีการมาจาก [14] เนื่องจากได้ทำการทดลองใช้วิธีตามแบบใน [14] คือออกแบบให้มีการเก็บข้อมูลจุดสำคัญบนเส้นลายนิ้วมือหลักและจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงที่ใกล้ที่สุดจำนวน 5 จุดและทำการเปรียบเทียบแบบ Local Matching เพื่อกำจัดจุดสำคัญบนเส้นลายนิ้วมือปลอมออก โดยจุดที่ได้คะแนนจากการเปรียบเทียบเป็น 0 จะถือว่าเป็นจุดสำคัญบนเส้นลายนิ้วมือปลอมและจะถูกลบออกไป (จุดที่ได้คะแนนอย่างน้อยเท่ากับ 1 หรือมากกว่าจะถูกเลือกให้นำไปใช้ในขั้นตอนการค้นหาแบบ Global Matching ต่อไป) จากนั้นจึงนำข้อมูลที่ได้มาคำนวณใหม่ โดยทำการเก็บข้อมูลจุดสำคัญบนเส้นลายนิ้วมือหลักและจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงทั่วทั้งภาพจำนวน 50 จุด จากนั้นจึงทำการเปรียบเทียบแบบ Global

Matching และคำนวณคะแนนจากการเปรียบเทียบ โดยค่าคะแนนที่ได้จากการเปรียบเทียบของครั้งที่ได้คะแนนสูงที่สุดจะถูกนำมาใช้ในการตัดสินว่าภาพลายนิ้วมือที่นำมาตรวจสอบเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือหรือต่างบุคคลกัน โดยนำมาเปรียบเทียบกับค่าขีดแบ่ง ถ้าคะแนนที่ได้สูงกว่าค่าขีดแบ่ง ก็จะถือว่าเป็นบุคคลเดียวกัน หากคะแนนที่ได้ต่ำกว่าค่าขีดแบ่ง จะถือว่าเป็นต่างบุคคลกัน จากผลการทดลองพบว่าจำนวนจุดสำคัญบนเส้นลายนิ้วมือปลอมที่พบในขั้นตอนการทำ Local Matching มีจำนวนน้อยมาก เนื่องมาจากข้อมูลภาพลายนิ้วมือก่อนเข้าสู่ขั้นตอนนี้ ได้ผ่านขั้นตอนการหาทิศทางและปรับแต่งเส้นลายนิ้วมาแล้ว (ได้กล่าวไว้แล้วในหัวข้อที่ 3.1.6) ทำให้จุดสำคัญบนเส้นลายนิ้วมือปลอมส่วนใหญ่ได้ถูกกำจัดออกไปแล้ว ดังนั้นจึงทำการดัดแปลงวิธีการจาก [14] ให้มีการเก็บข้อมูลและทำการเปรียบเทียบแบบ Global Matching เพียงอย่างเดียว เพื่อลดความซับซ้อนในการประมวลผลบนสมาร์ตคาร์ด และลดเวลาที่ใช้ในการประมวลผลลง

ในขั้นตอนนี้จะทำการค้นหาจุดสำคัญบนเส้นลายนิ้วมือ (Minutiae) โดยหาจุดที่เส้นลายนิ้วมือสิ้นสุด และจุดที่เส้นลายนิ้วมือแยกออกจากกัน โดยจะเก็บข้อมูลตำแหน่งในแกน X, ตำแหน่งในแกน Y และชนิดของจุดนั้นๆ จากนั้นจะนำข้อมูลที่ได้มาคำนวณหาความสัมพันธ์ของจุดสำคัญบนเส้นลายนิ้วมืออื่นๆ ที่ใกล้เคียงทั่วทั้งภาพ เพื่อความรวดเร็วในการประมวลผลจึงกำหนดให้มีจำนวนจุดข้างเคียงทั้งหมดไม่เกิน 50 จุด โดยจะเก็บข้อมูลเป็นตำแหน่ง, ชนิดของจุดสำคัญบนเส้นลายนิ้วมือหลัก และตำแหน่ง, ชนิด, มุมของจุดสำคัญบนเส้นลายนิ้วมือที่ใกล้ที่เคียงมากที่สุด จำนวน 50 จุด



รูปที่ 3.3 ตัวอย่างโครงสร้างความสัมพันธ์ระหว่างจุดสำคัญบนเส้นลายนิ้วมือหลักกับจุดสำคัญบนเส้นลายนิ้วมือที่ใกล้เคียงมากที่สุด 5 จุด



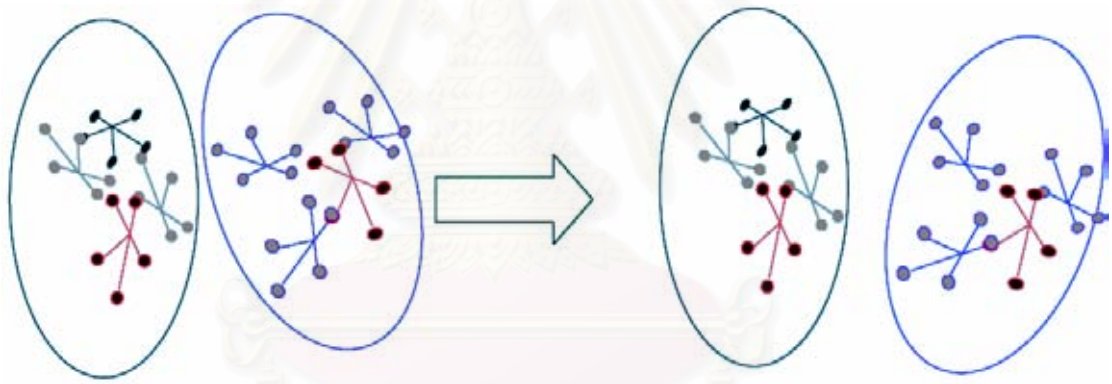
รูปที่ 3.4 ตัวอย่างรูปแบบในการเก็บข้อมูลระหว่างจุดสำคัญบนเส้นลายนิ้วมือหลักกับจุดสำคัญบนเส้นลายนิ้วมือรอบข้าง

โดยในรูปที่ 3.4 แสดงการเก็บข้อมูลเพื่อใช้ในการเปรียบเทียบ ซึ่งสามารถแบ่งชนิดของข้อมูลที่ทำการเก็บได้เป็น 2 ชนิดดังนี้

1. มุม ซึ่งเป็นการคำนวณจากมุมในทิศทางตามเข็มนาฬิการะหว่างเส้นตรงที่ลากจากจุดสำคัญบนเส้นลายนิ้วมือหลักไปยังจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงที่กำลังพิจารณา กับเส้นตรงที่ลากจากจุดสำคัญบนเส้นลายนิ้วมือหลักไปยังจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงอื่นๆที่เหลือ

2. ระยะทางจากจุดสำคัญบนเส้นลายนิ้วมือหลัก (x_1, y_1) กับจุดสำคัญบนเส้นลายนิ้วมือข้างเคียง (x_2, y_2) โดยคำนวณตามสูตร Euclidean distance

ระยะทาง = $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$



รูปที่ 3.5 ตัวอย่างการนำข้อมูลจุดสำคัญบนเส้นลายนิ้วมือจากข้อมูลภาพลายนิ้วมือสองรูปที่มีการเปลี่ยนตำแหน่งมาเปรียบเทียบ

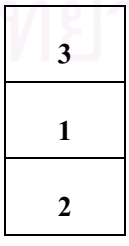
3.3 **การเปรียบเทียบลักษณะสำคัญ** (Feature Matching)

เป็นขั้นตอนการเปรียบเทียบลายนิ้วมือ ระหว่างลายนิ้วมือที่รับเข้ามากับแม่แบบลายนิ้วมือที่เก็บไว้ โดยในงานวิจัยชิ้นนี้ได้พัฒนาอัลกอริทึมในขั้นตอนนี้ขึ้นใหม่ เพื่อให้สามารถประมวลผลได้บนสมาร์ตคาร์ดที่มีหน่วยความจำชั่วคราวขนาดเล็ก

3.3.1 แนวคิดและหลักการทำงาน

เนื่องจากหน่วยประมวลผลบนสมาร์ตคาร์ดมีขนาดเล็กและมีความเร็วในการประมวลต่ำ จึงไม่เหมาะที่จะใช้ในการประมวลผลข้อมูลทางคณิตศาสตร์มากๆ ดังนั้นในงานวิจัยชิ้นนี้ได้ออกแบบให้ขั้นตอนการประมวลผลภาพเบื้องต้นและการค้นหาลักษณะสำคัญ จะถูกประมวลผลบนโฮสต์ เนื่องจากทั้งสองขั้นตอนนี้ส่วนใหญ่เป็นการประมวลผลทางด้านรูปภาพ (Image processing) ซึ่งต้องใช้พลังในการประมวลผลและหน่วยความจำสูง และต้องการความรวดเร็วในการประมวลผล โดยในขั้นตอนการเปรียบเทียบจุดสำคัญบนเส้นลายนิ้วมือจะกระทำภายในหน่วยประมวลของสมาร์ตคาร์ด ซึ่งทำให้แม่แบบลายนิ้วมือที่ถูกเก็บไว้ในสมาร์ตคาร์ดมีความปลอดภัยสูง เนื่องจากไม่มีการส่งแม่แบบลายนิ้วมือออกมานอกสมาร์ตคาร์ด และถูกปกป้องจากคุณสมบัติของสมาร์ตคาร์ดที่ออกแบบให้หน่วยความจำของสมาร์ตคาร์ด ไม่สามารถเข้าถึงได้โดยตรงจากภายนอก ในงานวิจัยนี้จะใช้แนวคิดในการมุ่งเน้นลดปริมาณการใช้งานหน่วยความจำชั่วคราวบนสมาร์ตคาร์ดในระหว่างการประมวลผลตรวจสอบลายนิ้วมือเพื่อให้สามารถประมวลผลบนสมาร์ตคาร์ดที่มีขนาดของหน่วยความจำชั่วคราวเล็กกว่าขนาดข้อมูลของลายนิ้วมือทั้งหมดได้ ซึ่งจะทำการเปรียบเทียบระหว่างข้อมูลจุดสำคัญบนลายนิ้วมือที่รับมาจากเครื่องอ่านลายนิ้วมือกับข้อมูลแม่แบบลายนิ้วมือ โดยจะใช้วิธีการแบ่งข้อมูลจุดสำคัญบนเส้นลายนิ้วมือที่ต้องการตรวจสอบที่ได้หลังจากผ่านกระบวนการค้นหาลักษณะสำคัญแล้วออกเป็น 3 ส่วน ดังแสดงในภาพที่ 3.6 เพื่อให้ขนาดของข้อมูลที่ได้เหมาะสมกับขนาดหน่วยความจำชั่วคราวบนสมาร์ตคาร์ด และการแบ่งออกเป็น 3 ส่วน ในกรณีส่วนใหญ่จะทำให้ส่วนตรงกลางเป็นจุดกึ่งกลางของภาพลายนิ้วมือ ซึ่งเป็นส่วนที่มักจะมีข้อมูลมากที่สุดและมีผลกระทบเนื่องจากความโค้งของนิ้วมือน้อยที่สุด

รูปที่ 3.6 ตัวอย่างข้อมูล
ลายนิ้วมือที่ถูกแบ่งเป็น 3 ส่วน



รูปที่ 3.7 ตำแหน่งข้อมูล
ลายนิ้วมือในแต่ละส่วน

ในขั้นตอนของการสร้างแม่แบบลายนิ้วมือ (Template Enrollment) ข้อมูลลายนิ้วมือที่ได้หลังจากขั้นตอนการค้นหาจุดสำคัญบนเส้นลายนิ้วมือทั้งหมดจะถูกบันทึกลงหน่วยความจำภายในสมาร์ตคาร์ด

ในขั้นตอนของการตรวจสอบลายนิ้วมือ หลังจากที่ภาพลายนิ้วมือที่ต้องการตรวจสอบผ่านขั้นตอนการค้นหาจุดสำคัญบนเส้นลายนิ้วมือเรียบร้อยแล้ว อัลกอริทึมจะทำการแบ่งข้อมูลจุดสำคัญบนเส้นลายนิ้วมือที่ได้จากภาพลายนิ้วมือที่ต้องการตรวจสอบออกเป็น 3 ส่วน ดังแสดงในรูปที่ 3.6 และทำการคำนวณหาจำนวนผลรวมของจุดสำคัญบนเส้นลายนิ้วมือ ในแต่ละส่วน จากนั้นจะนำผลรวมของแต่ละส่วนที่ได้มาพิจารณาเพื่อหาส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือมากที่สุด ซึ่งจะถูกกำหนดเป็นส่วนที่ตรวจสอบเปรียบเทียบเป็นส่วนแรก (Primary Matching) ส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือมากเป็นอันดับที่ 2 จะถูกกำหนดเป็นส่วนที่จะถูกตรวจสอบเปรียบเทียบเป็นลำดับที่สอง (Secondary Matching) และส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือน้อยที่สุดจะถูกกำหนดเป็นส่วนที่จะถูกตรวจสอบเปรียบเทียบเป็นลำดับที่สาม (Tertiary Matching) ในกรณีที่มีสองหรือสามส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือเท่ากัน อัลกอริทึมจะเลือกส่วนที่มีหมายเลขตำแหน่งน้อยที่สุดเรียงไปยังส่วนที่มีหมายเลขตำแหน่งมากที่สุด ตามรูปที่ 3.7 ซึ่งจะเห็นได้ว่าส่วนที่มีเลขน้อยที่สุด (1) จะเป็นส่วนกึ่งกลาง เนื่องจากโดยทั่วไปส่วนที่ 2 และ 3 จะเป็นขอบของนิ้วมือซึ่งมักจะมีส่วนที่ไม่ใช้ในการประมวลผลมากกว่าส่วนกึ่งกลาง เนื่องจากความโค้งของนิ้ว

ข้อมูลลายนิ้วมือแต่ละส่วนที่ส่งไปยังสมาร์ตคาร์ดจะถูกนำไปเปรียบเทียบกับข้อมูลลายนิ้วมือทั้งหมดที่อยู่บนสมาร์ตคาร์ด โดยสมาร์ตคาร์ดจะเป็นผู้ทำการเปรียบเทียบและนำค่าคะแนนที่ได้ไปเปรียบเทียบกับค่าขีดแบ่งต่างๆ ดังที่จะได้กล่าวในลำดับถัดไป เหตุผลที่ข้อมูลลายนิ้วมือที่รับเข้ามาเพียงหนึ่งส่วนจะต้องทำการเปรียบเทียบกับข้อมูลลายนิ้วมือทุกส่วนที่มีอยู่ในสมาร์ตคาร์ด เนื่องจากในการใช้งานจริง พบว่าในบางครั้งตำแหน่งและมุมของภาพลายนิ้วมือที่ต้องการตรวจสอบจะแตกต่างไปจากแม่แบบลายนิ้วมือเป็นอย่างมาก เช่น วางนิ้วมือกลับด้าน, เอียง หรือวางนิ้วมือผิดตำแหน่ง, เลื่อนไป ซึ่งทำให้ข้อมูลบางส่วนที่อยู่ในส่วนแรกของแม่แบบลายนิ้วมืออาจจะเปลี่ยนตำแหน่งไปอยู่ส่วนที่สองหรือส่วนที่สามของข้อมูลลายนิ้วมือที่ต้องการตรวจสอบได้ ดังนั้นการออกแบบให้เปรียบเทียบกับข้อมูลทุกส่วนที่เก็บไว้ในสมาร์ตคาร์ด จึงเป็นการเพิ่มความถูกต้องของผลลัพธ์ที่ได้ และ

เพิ่มความสามารถของอัลกอริทึม ในการรองรับการเปลี่ยนตำแหน่งหรือมุมของภาพลายนิ้วมือที่ต้องการตรวจสอบ

ในการตรวจสอบแต่ละครั้ง ค่าคะแนนที่ได้จากการเปรียบเทียบ (Matching Score) จะถูกนำไปเทียบกับค่าขีดแบ่ง โดยในงานวิจัยชิ้นนี้ ได้ออกแบบให้มีค่าขีดแบ่งย่อยๆ แตกต่างลงไปในการตรวจสอบแต่ละครั้ง และยังแบ่งออกเป็นค่าขีดแบ่งระดับบน (Upper Threshold) และค่าขีดแบ่งระดับล่าง (Lower Threshold) ซึ่งแตกต่างจากวิธีการทั่วไปที่มีค่าขีดแบ่งอยู่ค่าเดียว โดยแบ่งออกเป็น

1.ค่าขีดแบ่งที่ใช้การตรวจสอบครั้งแรก (ส่วนที่มีจุดสำคัญบนเส้นลายนิ้วมือมากที่สุด)

1.1. **ค่าขีดแบ่งระดับบน1**

เป็นตัวกำหนดระดับของค่าคะแนนที่ได้จากการเปรียบเทียบครั้งแรก ที่จะถือว่าเป็นลายนิ้วมือจากบุคคลคนเดียวกัน หากค่าคะแนนที่ได้จากการเปรียบเทียบในการตรวจสอบครั้งแรกมีค่าสูงกว่าค่าขีดแบ่งระดับบน1 จะแสดงว่าเป็นลายนิ้วมือจากบุคคลเดียวกัน และออกจากขั้นตอนการเปรียบเทียบลายนิ้วมือทันที โดยไม่ต้องตรวจสอบข้อมูลภาพลายนิ้วมือส่วนที่เหลือ

1.2. **ค่าขีดแบ่งระดับล่าง1**

เป็นตัวกำหนดระดับของค่าคะแนนที่ได้จากการเปรียบเทียบครั้งแรก ที่จะถือว่าเป็นลายนิ้วมือจากต่างบุคคลกัน ในกรณีที่ตรวจสอบแล้วพบว่าไม่มีจุดสำคัญบนเส้นลายนิ้วมือที่เหมือนกันเลย หรือมีในระดับที่น้อยมาก คือ มีค่าคะแนนที่ได้จากการเปรียบเทียบในการตรวจสอบครั้งแรกมีค่าต่ำกว่าค่าขีดแบ่งระดับล่าง1 จะแสดงว่าเป็นลายนิ้วมือจากต่างบุคคล และออกจากขั้นตอนการเปรียบเทียบลายนิ้วมือทันที โดยไม่ต้องตรวจสอบข้อมูลภาพลายนิ้วมือส่วนที่เหลือ

2.ค่าขีดแบ่งที่ใช้การตรวจสอบครั้งที่สอง (ส่วนที่มีจุดสำคัญบนเส้นลายนิ้วมือมากเป็นอันดับสอง)

2.1. ค่าขีดแบ่งระดับบน2

เป็นตัวกำหนดระดับของค่าคะแนนที่ได้จากการเปรียบเทียบครั้งที่สอง ที่จะถือว่าเป็นลายนิ้วมือจากบุคคลคนเดียวกัน หากค่าคะแนนที่ได้จากการเปรียบเทียบในการตรวจสอบครั้งที่สองมีค่าสูงกว่าค่าขีดแบ่งระดับบน2 จะแสดงว่าเป็นลายนิ้วมือจากบุคคลเดียวกัน และออกจากขั้นตอนการเปรียบเทียบลายนิ้วมือทันที โดยไม่ต้องตรวจสอบข้อมูลภาพลายนิ้วมือส่วนที่เหลือ

2.2. ค่าขีดแบ่งระดับล่าง2

เป็นตัวกำหนดระดับของค่าคะแนนที่ได้จากการเปรียบเทียบครั้งที่สอง ที่จะถือว่าเป็นลายนิ้วมือจากต่างบุคคลกัน ในกรณีที่ตรวจสอบแล้วพบว่าไม่มีจุดสำคัญบนเส้นลายนิ้วมือที่เหมือนกันเลย หรือมีในระดับที่น้อยมาก คือ มีค่าคะแนนที่ได้จากการเปรียบเทียบในการตรวจสอบครั้งที่สองมีค่าต่ำกว่าค่าขีดแบ่งระดับล่าง2 จะแสดงว่าเป็นลายนิ้วมือจากต่างบุคคล และออกจากขั้นตอนการเปรียบเทียบลายนิ้วมือทันที โดยไม่ต้องตรวจสอบข้อมูลภาพลายนิ้วมือส่วนที่เหลือ

ค่าขีดแบ่งระดับบนจะช่วยลดเวลาในกรณีของภาพของลายนิ้วมือที่เข้ามาเป็นของบุคคลเดียวกันในบางกรณี (ส่วนใหญ่เป็นกรณีข้อมูลภาพลายนิ้วมือที่รับเข้ามาไม่มีการเปลี่ยนแปลงตำแหน่งและขนาด หรือมีการเปลี่ยนแปลงเพียงเล็กน้อย และไม่มีสัญญาณรบกวน เมื่อเปรียบเทียบกับแม่แบบลายนิ้วมือ) ส่วนค่าขีดแบ่งระดับล่างจะช่วยลดเวลาในกรณีของภาพของลายนิ้วมือที่เข้ามาเป็นของต่างบุคคลกัน โดยมีตำแหน่งและชนิดของจุดสำคัญบนเส้นลายนิ้วมือที่แตกต่างกันระหว่างภาพลายนิ้วมือที่รับเข้ามากับแม่แบบลายนิ้วมือ

3.ค่าขีดแบ่งที่ใช้การตรวจสอบครั้งที่สาม (ส่วนที่มีจุดสำคัญบนเส้นลายนิ้วมือน้อยที่สุด)

3.1. ค่าขีดแบ่ง3

ใช้เป็นตัวกำหนดระดับของค่าคะแนนที่ได้จากการเปรียบเทียบครั้งที่สาม ที่จะถือว่าเป็นลายนิ้วมือจากบุคคลเดียวกันหรือต่างบุคคลกัน หากค่าคะแนนที่ได้จากการเปรียบเทียบ ในการตรวจสอบครั้งที่สามมีค่าสูงกว่าค่าขีดแบ่ง3 จะแสดงว่าเป็นลายนิ้วมือจากบุคคลเดียวกัน หากค่าต่ำกว่าแสดงว่าเป็นลายนิ้วมือจากต่างบุคคลกัน

3.3.2 วิธีการที่ใช้ในการเปรียบเทียบข้อมูลจุดสำคัญบนเส้นลายนิ้วมือของแต่ละส่วนย่อย

อัลกอริทึมที่ใช้ในการเปรียบเทียบข้อมูลจุดสำคัญบนเส้นลายนิ้วมือในงานวิจัยชิ้นนี้ได้ดัดแปลงมาจาก [14] โดยมีหลักการทำงาน คือ จะทำการนำข้อมูลจุดสำคัญบนเส้นลายนิ้วมือจากข้อมูลลายนิ้วมือส่วนย่อยที่ต้องการตรวจสอบมาทำการเปรียบเทียบกับข้อมูลจุดสำคัญบนเส้นลายนิ้วมือของแม่แบบลายนิ้วมือที่เก็บไว้ภายในสมาร์ตคาร์ด โดยข้อมูลจุดสำคัญบนเส้นลายนิ้วมือของส่วนย่อยที่ต้องการตรวจสอบแต่ละจุด (ซึ่งประกอบไปด้วยจุดสำคัญบนเส้นลายนิ้วมือที่เป็นจุดศูนย์กลางอยู่ 1 จุด และจุดข้างเคียงจำนวน 50 จุด) จะถูกนำมาตรวจสอบกับจุดสำคัญบนเส้นลายนิ้วมือของแม่แบบลายนิ้วมือที่เก็บไว้ภายในสมาร์ตคาร์ดที่มีชนิดของจุดสำคัญบนเส้นลายนิ้วมือศูนย์กลางเหมือนกัน ทุกๆ จุด (จุดที่เส้นลายนิ้วมือสิ้นสุด หรือจุดที่เส้นลายนิ้วมือ 1 เส้น มีการแยกเป็น 2 เส้นหรือมากกว่า) เพื่อให้สามารถรองรับการเปลี่ยนแปลงตำแหน่ง, การเปลี่ยนมุม และการเปลี่ยนแปลงของขนาด (ระยะทาง) เนื่องมาจากสภาพความยืดหยุ่นของผิวได้ โดยผลลัพธ์ที่ได้จากการเปรียบเทียบในแต่ละจุดนั้นจะเป็นคะแนนความคล้ายคลึงกันของจำนวนจุดสำคัญบนเส้นลายนิ้วมือข้างเคียง ซึ่งจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงที่มีความคล้ายคลึงกัน (ระหว่างจุดสำคัญบนเส้นลายนิ้วมือที่ต้องการตรวจสอบกับจุดสำคัญบนเส้นลายนิ้วมือของแม่แบบลายนิ้วมือที่เก็บไว้ภายในสมาร์ตคาร์ด) จำนวน 1 จุด จะได้เป็น 1 คะแนน เนื่องจากได้กำหนดให้จำนวนจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงมีได้ไม่เกิน 50 จุด ดังนั้น คะแนนมากที่สุดที่เป็นไปได้ คือ 50 คะแนน

โดยขั้นตอนการพิจารณาความคล้ายคลึงของจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงแต่ละจุดที่อ้างอิงไปยังจุดสำคัญบนเส้นลายนิ้วมือศูนย์กลางเดียวกัน จะประกอบไปด้วยขั้นตอนดังต่อไปนี้

1. ทำการพิจารณาชนิดจุดสำคัญบนเส้นลายนิ้วมือ หากเป็นชนิดเดียวกันจะเข้าสู่การพิจารณาลำดับถัดไป หากเป็นต่างชนิดกัน จะให้คะแนนเป็น 0 ทันที
2. ทำการพิจารณาค่าความแตกต่างของมุม โดยนำค่ามุมจากจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงของส่วนย่อยที่ต้องการตรวจสอบมาลบกับค่ามุมจากจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงของแม่แบบลายนิ้วมือที่เก็บไว้ภายในสมาร์ตคาร์ด หากค่าผลต่างที่ได้มีค่าน้อยกว่าค่าความแตกต่างมากที่สุดที่ยอมรับได้ จะเข้าสู่การพิจารณาลำดับถัดไป หากมีค่ามากกว่าจะให้คะแนนเป็น 0 ทันที
3. ทำการพิจารณาค่าความแตกต่างของระยะทางจากจุดสำคัญบนเส้นลายนิ้วมือศูนย์กลางมายังจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงที่กำลังพิจารณานั้นๆ โดยนำค่าระยะทางจากจุดสำคัญบนเส้นลายนิ้วมือศูนย์กลางไปยังจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงของส่วนย่อยที่ต้องการตรวจสอบมาลบกับค่าระยะทางจากจุดสำคัญบนเส้นลายนิ้วมือจุดศูนย์กลางไปยังจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงของแม่แบบลายนิ้วมือที่เก็บไว้ภายในสมาร์ตคาร์ด หากค่าผลต่างที่ได้มีค่าน้อยกว่าค่าความแตกต่างมากที่สุดที่ยอมรับได้ จะได้คะแนนเป็น 1 หากมีค่ามากกว่าจะให้คะแนนเป็น 0

จากนั้นจะนำค่าคะแนนที่ได้จากการเปรียบเทียบจุดสำคัญบนเส้นลายนิ้วมือข้างเคียงแต่ละจุดที่อ้างอิงไปยังจุดสำคัญบนเส้นลายนิ้วมือศูนย์กลางเดียวกันมาทำการรวมกัน ผลคะแนนรวมได้คือค่าคะแนนความคล้ายคลึงของจุดสำคัญบนเส้นลายนิ้วมือศูนย์กลางนั้นๆ

ทำการเปลี่ยนจุดสำคัญบนเส้นลายนิ้วมือศูนย์กลางเป็นจุดอื่นๆ และคำนวณตามขั้นตอนข้างต้นจนครบทุกจุด จากนั้นนำค่าคะแนนทั้งหมดที่ได้มาทำการหาคะแนนการเปรียบเทียบครั้งที่ได้คะแนนสูงที่สุด (ซึ่งคือการเปรียบเทียบครั้งที่มีความเหมือนกันมากที่สุด) คะแนนที่ได้ คือ คะแนนความคล้ายคลึงระหว่างลายนิ้วมือที่ต้องการตรวจสอบ

กับแม่แบบลายนิ้วมือ ซึ่งเป็นคะแนนที่จะนำไปใช้ในการเปรียบเทียบกับค่าขีดแบ่งต่างๆ ดังที่ได้กล่าวมาแล้วในหัวข้อ 3.3.1

3.3.3 ขั้นตอนการเปรียบเทียบลายนิ้วมือระหว่างโฮสต์กับสมาร์ตคาร์ด

ประกอบไปด้วยขั้นตอนดังต่อไปนี้

1. โฮสต์ติดต่อไปยังสมาร์ตคาร์ดเพื่อร้องขอเริ่มต้นการเปรียบเทียบลายนิ้วมือ

2. สมาร์ตคาร์ดส่งสัญญาณตอบกลับ เพื่อแสดงว่าพร้อมที่จะเริ่มต้นการตรวจสอบ

3. โฮสต์ส่งส่วนย่อยของข้อมูลจุดสำคัญบนเส้นลายนิ้วมือไปยังสมาร์ตคาร์ด (ส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือมากที่สุด)

4. สมาร์ตคาร์ดนำส่วนย่อยของข้อมูลจุดสำคัญบนเส้นลายนิ้วมือที่รับเข้ามาเข้าสู่กระบวนการตรวจสอบครั้งที่ 1 ซึ่งมีขั้นตอนดังต่อไปนี้

   4.1 สมาร์ตคาร์ดนำข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนแรกที่รับมาจากโฮสต์ไปตรวจสอบกับแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำของสมาร์ตคาร์ด จากนั้นจะคำนวณหาคะแนนที่ได้จากการเปรียบเทียบ และนำไปเปรียบเทียบกับค่าขีดแบ่งระดับบน1 และค่าขีดแบ่งระดับล่าง1

   4.2 หากคะแนนที่ได้จากการเปรียบเทียบสูงกว่าค่าขีดแบ่งระดับบน1 แสดงว่าเป็นลายนิ้วมือของบุคคลเดียวกัน สมาร์ตคาร์ดส่งคำตอบไปยังโฮสต์ และสิ้นสุดการเปรียบเทียบ

   4.3 หากค่าคะแนนที่ได้จากการเปรียบเทียบต่ำกว่าค่าขีดแบ่งระดับบน1 และต่ำกว่าค่าขีดแบ่งระดับล่าง1 แสดงว่าไม่ใช่ลายนิ้วมือของบุคคลเดียวกัน สมาร์ตคาร์ดส่งคำตอบไปยังโฮสต์ และสิ้นสุดการเปรียบเทียบ

4.4 หากค่าคะแนนที่ได้จากการเปรียบเทียบต่ำกว่าค่าขีดแบ่งระดับบน1 และสูงกว่าค่าขีดแบ่งระดับล่าง1 จะถือว่ายังสรุปผลลัพธ์ไม่ได้ จะต้องนำข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนอื่นมาตรวจสอบเพิ่มเติม โดยจะเข้าสู่กระบวนการตรวจสอบครั้งที่ 2

5. สมาร์ตคาร์ดติดต่อไปยังโฮสต์เพื่อร้องข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนที่สองมาทำการเปรียบเทียบ

6. โฮสต์ส่งส่วนย่อยของข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนที่ 2 ไปยังสมาร์ตคาร์ด (ส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือมากที่สุดเป็นอันดับที่สอง)

7. สมาร์ตคาร์ดนำส่วนย่อยของข้อมูลจุดสำคัญบนเส้นลายนิ้วมือที่รับเข้ามา เข้าสู่กระบวนการตรวจสอบครั้งที่ 2 ซึ่งมีขั้นตอนดังต่อไปนี้

7.1 สมาร์ตคาร์ดนำข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนที่ 2 ที่รับมาจากโฮสต์ไปตรวจสอบกับแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำของสมาร์ตคาร์ด จากนั้นจะคำนวณหาคะแนนที่ได้จากการเปรียบเทียบและนำไปเปรียบเทียบกับค่าขีดแบ่งระดับบน2 และค่าขีดแบ่งระดับล่าง2

7.2 หากคะแนนที่ได้จากการเปรียบเทียบสูงกว่าค่าขีดแบ่งระดับบน2 แสดงว่าเป็นลายนิ้วมือของบุคคลเดียวกัน สมาร์ตคาร์ดส่งคำตอบไปยังโฮสต์ และสิ้นสุดการเปรียบเทียบ

7.3 หากค่าคะแนนที่ได้จากการเปรียบเทียบต่ำกว่าค่าขีดแบ่งระดับบน2 และต่ำกว่าค่าขีดแบ่งระดับล่าง2 แสดงว่าไม่ใช่ลายนิ้วมือของบุคคลเดียวกัน สมาร์ตคาร์ดส่งคำตอบไปยังโฮสต์ และสิ้นสุดการเปรียบเทียบ

7.4 หากค่าคะแนนที่ได้จากการเปรียบเทียบต่ำกว่าค่าขีดแบ่งระดับบน2 และสูงกว่าค่าขีดแบ่งระดับล่าง2 จะถือว่ายังสรุปผลลัพธ์ไม่ได้ จะต้องนำข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนสุดท้ายมาตรวจสอบเพิ่มเติม โดยจะเข้าสู่กระบวนการตรวจสอบครั้งที่ 3

8. สมาร์ตคาร์ดติดต่อไปยังโฮสต์เพื่อร้องขอข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนสุดท้ายเพื่อทำการเปรียบเทียบ

9. โฮสต์ส่งส่วนย่อยของข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนสุดท้ายไปยังสมาร์ตคาร์ด (ส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือน้อยที่สุด)

10. สมาร์ตคาร์ดนำส่วนย่อยของข้อมูลจุดสำคัญบนเส้นลายนิ้วมือที่รับเข้ามา เข้าสู่กระบวนการตรวจสอบครั้งที่ 3 ซึ่งมีขั้นตอนดังต่อไปนี้

    10.1 สมาร์ตคาร์ดนำส่วนย่อยของข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนสุดท้ายที่รับเข้ามาไปตรวจสอบกับแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำของสมาร์ตคาร์ด จากนั้นจะคำนวณหาค่าคะแนนที่ได้จากการเปรียบเทียบ และนำไปเปรียบเทียบกับค่าขีดแบ่ง3

    10.2 หากค่าคะแนนที่ได้จากการเปรียบเทียบสูงกว่าค่าขีดแบ่ง3 แสดงว่าเป็นลายนิ้วมือของบุคคลเดียวกัน สมาร์ตคาร์ดส่งคำตอบไปยังโฮสต์ และสิ้นสุดการเปรียบเทียบ

    10.3 หากค่าคะแนนที่ได้จากการเปรียบเทียบต่ำกว่าค่าขีดแบ่ง3 แสดงว่าเป็นลายนิ้วมือต่างบุคคลกัน สมาร์ตคาร์ดส่งคำตอบไปยังโฮสต์ และสิ้นสุดการเปรียบเทียบ

3.3.4 ขั้นตอนการทำงานของระบบตรวจสอบลายนิ้วมือ

ในหัวข้อนี้ได้กล่าวถึงขั้นตอนการทำงานของระบบตรวจสอบลายนิ้วมือทั้งหมด โดยสามารถแบ่งออกได้เป็น 2 กรณี หลักดังต่อไปนี้

1. **กรณีลงทะเบียนลายนิ้วมือ** (ยังไม่มีแม่แบบลายนิ้วมือบนสมาร์ตคาร์ด) สามารถแบ่งออกเป็นขั้นตอนการทำงานย่อย 6 ขั้นตอนดังต่อไปนี้

   1.1 ผู้ใช้งานนำนิ้วมือที่ต้องการลงทะเบียนสัมผัสกับเครื่องอ่านลายนิ้วมือ

   1.2 เครื่องอ่านลายนิ้วมือทำการแปลงข้อมูลลายนิ้วมือที่อ่านได้จาก Analog เป็น Digital และทำการส่งข้อมูลไปยังเครื่องคอมพิวเตอร์

   1.3 เครื่องคอมพิวเตอร์นำข้อมูลภาพลายนิ้วมือที่ได้รับจากเครื่องอ่านลายนิ้วมือ เข้าสู่ขั้นตอนการประมวลผลภาพเบื้องบน และการค้นหาลักษณะสำคัญบนเส้นลายนิ้วมือ (ดังที่ได้กล่าวไว้แล้วในหัวข้อ 3.1 และ 3.2 ก่อนหน้านี้)

   1.4 เครื่องคอมพิวเตอร์ส่งข้อมูลจุดสำคัญบนเส้นลายนิ้วมือทั้งหมดไปยังสมาร์ตคาร์ดโดยผ่านทางเครื่องอ่าน/เขียนสมาร์ตคาร์ด (รายละเอียดของเครื่องอ่าน/เขียนสมาร์ตคาร์ดจะได้กล่าวไว้โดยละเอียด ในบทที่ 4)

   1.5 สมาร์ตคาร์ดทำการรับข้อมูลจุดสำคัญบนเส้นลายนิ้วมือและนำข้อมูลทั้งหมดบันทึกลงหน่วยความจำของสมาร์ตคาร์ด

   1.6 สมาร์ตคาร์ดส่งผลลัพธ์ของการบันทึกกลับไปยังเครื่องคอมพิวเตอร์ (โดยผ่านทางเครื่องอ่าน/เขียนสมาร์ตคาร์ด)

รูปที่ 3.8 ขั้นตอนการทำงานของระบบตรวจสอบลายนิ้วมือ กรณีต้องการลงทะเบียนลายนิ้วมือ

2. **กรณีเปรียบเทียบลายนิ้วมือ** (ทำการรับภาพลายนิ้วมือที่ต้องการตรวจสอบไปเปรียบเทียบกับแม่แบบลายนิ้วมือที่อยู่ภายในสมาร์ตคาร์ด)

2.1. ผู้ใช้งานนำนิ้วมือที่ต้องการตรวจสอบสัมผัสกับเครื่องอ่านลายนิ้วมือ

2.2. เครื่องอ่านลายนิ้วมือทำการแปลงข้อมูลลายนิ้วมือที่อ่านได้จาก Analog เป็น Digital และทำการส่งข้อมูลไปยังเครื่องคอมพิวเตอร์

2.3. เครื่องคอมพิวเตอร์นำข้อมูลภาพลายนิ้วมือที่ได้รับจากเครื่องอ่านลายนิ้วมือเข้าสู่ขั้นตอนการประมวลผลภาพเบื้องบนและการค้นหาลักษณะสำคัญบนเส้นลายนิ้วมือ (ดังที่ได้กล่าวไว้แล้วในหัวข้อ 3.1 และ 3.2 ก่อนหน้านี้) จากนั้นเครื่องคอมพิวเตอร์ทำการแบ่งข้อมูลจุดสำคัญบนเส้นลายนิ้วมือที่คำนวณได้ออกเป็น 3 ส่วน

2.4. เครื่องคอมพิวเตอร์ทำการส่งข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนย่อยแรกซึ่งมีจำนวนจุดสำคัญบนเส้นลายนิ้วมือมากที่สุดสำหรับการตรวจสอบครั้งแรกไปยังสมาร์ตคาร์ด ผ่านทางเครื่องอ่าน/เขียนสมาร์ตคาร์ด

2.5. สมาร์ตคาร์ดทำการรับข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนย่อยแรกมาตรวจสอบเปรียบเทียบกับแม่แบบลายนิ้วมือบนสมาร์ตคาร์ด และนำค่าคะแนนที่ได้จากการเปรียบเทียบไปตรวจสอบกับค่าขีดแบ่งระดับบน1 และค่าขีดแบ่งระดับล่าง1 เพื่อพิจารณาว่าต้องการส่วนอื่นมาประมวลผลต่อหรือสามารถหาผลลัพธ์ได้ทันที จากนั้นทำการส่งข้อมูลจากการเปรียบกับค่าขีดแบ่งกลับไปยังเครื่องคอมพิวเตอร์ ผ่านทางเครื่องอ่าน/เขียนสมาร์ตคาร์ด

เครื่องคอมพิวเตอร์รอรับผลการตรวจสอบกลับมาจากสมาร์ตคาร์ด ถ้าหากสมาร์ตคาร์ดส่งผลลัพธ์ของการตรวจสอบกลับมาก็จะนำผลลัพธ์นั้นไปประยุกต์ใช้ตามความต้องการของแต่ละโปรแกรม แต่ถ้าสมาร์ตคาร์ดต้องการข้อมูลลายนิ้วมือส่วนอื่นมาประมวลผลต่อ ก็จะทำการส่งข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนย่อยที่สอง ซึ่งมีจำนวนจุดสำคัญบนเส้นลายนิ้วมือมากเป็นลำดับสองไปยังสมาร์ตคาร์ด โดยผ่านทางเครื่องอ่าน/เขียนสมาร์ตคาร์ด

สมาร์ตคาร์ดทำการรับข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนย่อยที่สองมาตรวจสอบเปรียบเทียบกับแม่แบบลายนิ้วมือบนสมาร์ตคาร์ด และนำค่าคะแนนที่ได้จากการเปรียบเทียบไปตรวจสอบกับค่าขีดแบ่งระดับบน 2 และค่าขีดแบ่งระดับล่าง 2 เพื่อพิจารณาว่าต้องการส่วนอื่นมาประมวลผลต่อหรือสามารถหาผลลัพธ์ได้ทันที จากนั้นทำการส่งข้อมูลจากการเปรียบกับค่าขีดแบ่งกลับไปยังเครื่องคอมพิวเตอร์ ผ่านทางเครื่องอ่าน/เขียนสมาร์ตคาร์ด

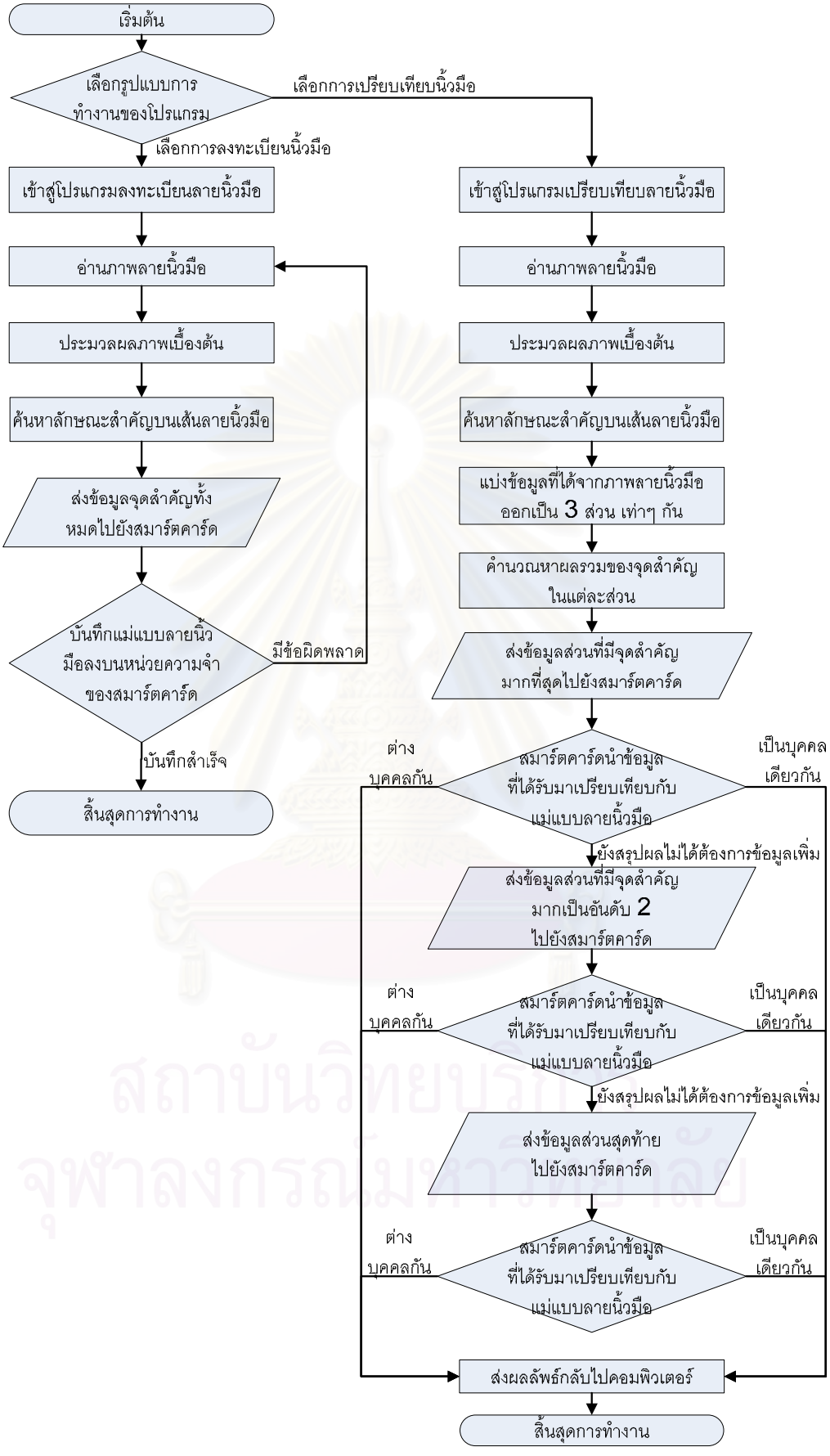
เครื่องคอมพิวเตอร์รอรับผลการตรวจสอบกลับมาจากสมาร์ตคาร์ด ถ้าหากสมาร์ตคาร์ดส่งผลลัพธ์ของการตรวจสอบกลับมาก็จะนำผลลัพธ์นั้นไป

ประยุกต์ใช้ตามความต้องการของแต่ละโปรแกรม แต่ถ้าสมาร์ตคาร์ดต้องการข้อมูลลายนิ้วมือส่วนอื่นมาประมวลผลต่อ ก็จะทำการส่งข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนย่อยที่สาม ซึ่งมีจำนวนจุดสำคัญบนเส้นลายนิ้วมือน้อยที่สุดไปยังสมาร์ตคาร์ด โดยผ่านทางเครื่องอ่าน/เขียนสมาร์ตคาร์ด

สมาร์ตคาร์ดทำการรับข้อมูลจุดสำคัญบนเส้นลายนิ้วมือส่วนย่อยที่สามมาตรวจสอบเปรียบเทียบกับแม่แบบลายนิ้วมือบนสมาร์ตคาร์ด และนำค่าคะแนนที่ได้จากการเปรียบเทียบไปตรวจสอบกับค่าขีดแบ่งระดับ3 เพื่อทำการหาผลลัพธ์ และส่งผลลัพธ์กลับไปยังเครื่องคอมพิวเตอร์ (โดยผ่านทางเครื่องอ่าน/เขียนสมาร์ตคาร์ด)

2.6. เครื่องคอมพิวเตอร์นำผลลัพธ์ที่ได้ไปประยุกต์ใช้ตามความต้องการ

รูปที่ 3.9 ขั้นตอนการทำงานของระบบตรวจสอบลายนิ้วมือ กรณีต้องการเปรียบเทียบลายนิ้วมือ



รูปที่ 3.10 Flowchart การทำงานของระบบทั้งหมด

3.4 การเพิ่มความปลอดภัยของการเก็บแม่แบบลายนิ้วมือบนสมาร์ตคาร์ด

การออกแบบให้แม่แบบลายนิ้วมือถูกเก็บไว้ในหน่วยความจำ EEPROM บนสมาร์ตคาร์ดจะมีความปลอดภัยในระดับสูง เนื่องจากหน่วยความจำ EEPROM ของสมาร์ตคาร์ดจะถูกปกป้องจากคุณสมบัติของสมาร์ตคาร์ดที่ออกแบบให้หน่วยความจำ EEPROM ไม่มีการติดต่อกับภายนอกโดยตรง การติดต่อกับหน่วยความจำ EEPROM จะต้องกระทำผ่านหน่วยประมวลของสมาร์ตคาร์ดเท่านั้น

อย่างไรก็ตาม หากหน่วยความจำส่วนที่ใช้ในการเก็บข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ดนั้นไม่ได้เป็นแบบเขียนได้ครั้งเดียว (ROM: Read Only Memory) แต่เป็นแบบเขียนได้หลายครั้ง (Flash Memory) และหน่วยความจำ EEPROM แยกออกเป็นต่างชิ้นส่วนจากหน่วยประมวลผล ดังเช่น สมาร์ตคาร์ดที่นำมาใช้ในงานวิจัยชิ้นนี้ จะมีความเป็นไปได้ที่ข้อมูลแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำ EEPROM จะถูกอ่านออกมาได้ ในกรณีที่ผู้โจรกรรมข้อมูลรู้ชนิดของหน่วยประมวลผลที่ใช้, ชนิดของหน่วยความจำ EEPROM, รูปแบบคำสั่งในการเขียนโปรแกรม, วิธีการเขียนข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ด, โครงสร้างการเชื่อมต่อระหว่างหน่วยประมวลกับหน้าสัมผัสของสมาร์ตคาร์ดและหน่วยความจำ EEPROM เนื่องจากผู้โจรกรรมอาจจะทำการเขียนข้อมูลโปรแกรมลงบนสมาร์ตคาร์ดใหม่ เพื่อทำการสั่งงานให้หน่วยประมวลผลของสมาร์ตคาร์ดทำการอ่านข้อมูลจากหน่วยความจำ EEPROM แล้วส่งออกมาภายนอกได้ ซึ่งการแก้ไขปัญหาดังกล่าว โดยทั่วไปจะทำได้โดยทำการเข้ารหัสข้อมูลแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำ EEPROM ทำให้เมื่อผู้โจรกรรมได้ข้อมูลจาก EEPROM ไปก็ไม่สามารถนำไปใช้ได้ เนื่องจากถูกเข้ารหัสไว้

เนื่องจากการเข้ารหัสข้อมูลแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำ EEPROM เมื่อต้องการตรวจสอบลายนิ้วมือ ข้อมูลแม่แบบลายนิ้วมือที่ทำการเข้ารหัสไว้จะต้องทำการถอดรหัสโดยใช้หน่วยประมวลผลบนสมาร์ตคาร์ดในการถอดรหัส หลังจากนั้นจึงจะสามารถนำข้อมูลแม่แบบลายนิ้วมือที่ผ่านการถอดรหัสแล้วไปทำการเปรียบกับข้อมูลลายนิ้วมือที่ต้องการตรวจสอบโดยหน่วยประมวลผลบนสมาร์ตคาร์ด แต่เนื่องจากหน่วยประมวลผลบนสมาร์ตคาร์ดบางชนิดจะมีข้อจำกัดต่างๆ ในการประมวลผล อาทิ มีความเร็วในการประมวลผลต่ำ และในกรณีของสมาร์ตคาร์ดที่มีหน่วยประมวลผลขนาด 8 บิต เช่น สมาร์ตคาร์ดที่นำมาใช้ในงานวิจัยชิ้นนี้

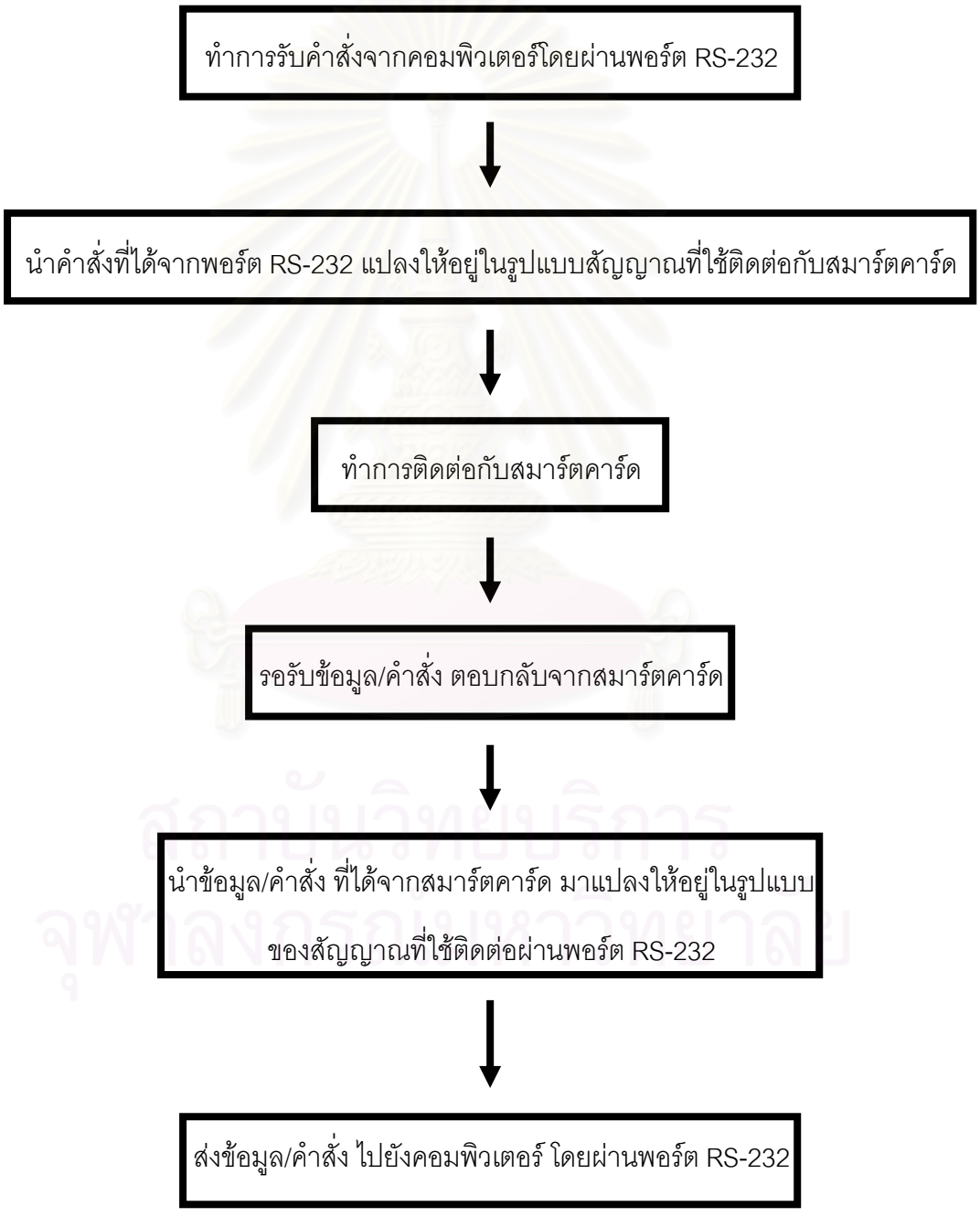
จะสามารถทำการประมวลผลข้อมูลได้ครั้งละ 8 บิตเท่านั้น ซึ่งการนำมาใช้ในการเข้ารหัสและถอดรหัสข้อมูลแม่แบบลายนิ้วมือบนสมาร์ตคาร์ด กรณีที่ต้องการความปลอดภัยสูง อัลกอริทึมที่ใช้ในการเข้ารหัสและถอดรหัสจะมีความซับซ้อนมาก ส่งผลให้หน่วยประมวลผลของสมาร์ตคาร์ดต้องใช้ระยะเวลานานในการเข้ารหัสและถอดรหัสข้อมูลในแต่ละครั้ง

เพื่อเป็นการลดระยะเวลาที่ผู้ใช้งานต้องรอผลลัพธ์จากการประมวลผลการตรวจสอบข้อมูลลายนิ้วมือของสมาร์ตคาร์ด ในงานวิจัยชิ้นนี้ จึงได้นำเสนอแนวคิด ในการออกแบบให้ข้อมูลแม่แบบลายนิ้วมือถูกเก็บไว้ในหน่วยความจำส่วนที่ในการเก็บข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ด แทนที่จะเก็บไว้ในหน่วยจำ EEPROM ในวิธีการทั่วไป และข้อมูลแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำส่วนที่ใช้ในการเก็บข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ดจะไม่มีการเข้ารหัสข้อมูล จึงทำให้สามารถตัดขั้นตอนการทำงานในการเข้ารหัสและถอดรหัสออกไปได้ ทำให้ได้ผลลัพธ์จากการตรวจสอบลายนิ้วมือเร็วขึ้น

การออกแบบให้เก็บข้อมูลแม่แบบลายนิ้วมือไว้ในหน่วยความจำส่วนที่ใช้ในการเก็บข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ดจะทำให้ข้อมูลแม่แบบลายนิ้วมือปลอดภัยจากวิธีการโจรกรรมที่ได้กล่าวมาในข้างต้น เนื่องจากหน่วยความจำส่วนที่ใช้ในการเก็บข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ดจะถูกปกป้องโดยคุณสมบัติ Code protection ซึ่งจะป้องกันไม่ให้มีการอ่านข้อมูลโปรแกรมออกมา ดังนั้นหากมีการโจรกรรมโดยทำการเขียนข้อมูลโปรแกรมลงไปใหม่ ตามวิธีการที่ได้กล่าวในข้างต้น ข้อมูลแม่แบบลายนิ้วมือที่อยู่ในหน่วยความจำส่วนที่ใช้ในการเก็บข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ดก็จะถูกเขียนทับไปด้วย ทำให้ผู้โจรกรรมไม่สามารถอ่านข้อมูลแม่แบบลายนิ้วมือได้ ดังนั้นข้อมูลแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำส่วนที่ใช้ในการเก็บข้อมูลโปรแกรมสำหรับหน่วยประมวลผลของสมาร์ตคาร์ดจึงไม่มีความจำเป็นต้องทำการเข้ารหัสข้อมูล

บทที่ 4
การออกแบบเครื่องอ่าน/เขียนสมาร์ตคาร์ด (Smartcard Reader/Writer)

เครื่องอ่าน/เขียนสมาร์ตคาร์ด ได้ถูกออกแบบให้สามารถใช้งานได้กับสมาร์ตคาร์ดแบบมีหน่วยประมวลผลในตัว (Processor Card) ตามมาตรฐาน ISO 7816 [3] ส่วนใหญ่ได้



รูปที่ 4.1 แนวคิดการทำงานของ เครื่องอ่าน/เขียนสมาร์ตคาร์ด

4.1 รูปแบบการเชื่อมต่อระหว่างเครื่องอ่าน/เขียนสมาร์ตคาร์ด กับเครื่องคอมพิวเตอร์

เครื่องอ่าน/เขียนสมาร์ตคาร์ดที่ได้ทำการสร้างขึ้นเพื่อใช้ในการทดลองในงานวิจัยนี้ ได้ออกแบบให้ติดต่อกับคอมพิวเตอร์โดยผ่านทาง พอร์ตแบบอนุกรม RS-232 แบบ DB9 เนื่องจากรูปแบบสัญญาณของพอร์ตแบบอนุกรม RS-232 แบบ DB9 กับรูปแบบสัญญาณที่ใช้กับขาข้อมูลของสมาร์ตคาร์ดมีความใกล้เคียงกันมาก จะแตกต่างกันก็เพียงระดับลอจิกของสัญญาณเท่านั้น ดังนั้นจึงเลือกใช้ไอซี เบอร์ MAX232 เพื่อใช้เป็นไดรฟ์เวอร์ ในการแปลงสัญญาณที่ได้จากพอร์ตอนุกรม RS-232 ให้อยู่ในรูปแบบที่สอดคล้องกับระดับสัญญาณที่ขาข้อมูลของสมาร์ตคาร์ด โดยไอซีที่นำมาใช้เป็นของ MAXIM เบอร์ MAX232 โดยเลือกใช้แบบ 16 PIN PDIP (Plastic-Dual-In-Line Package)

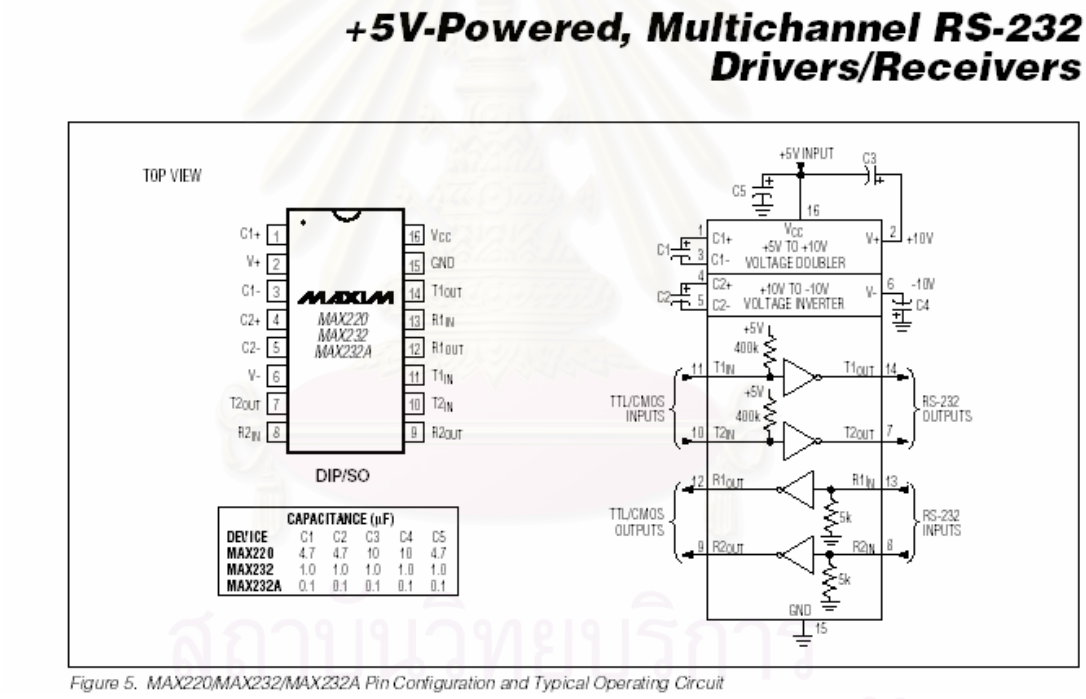
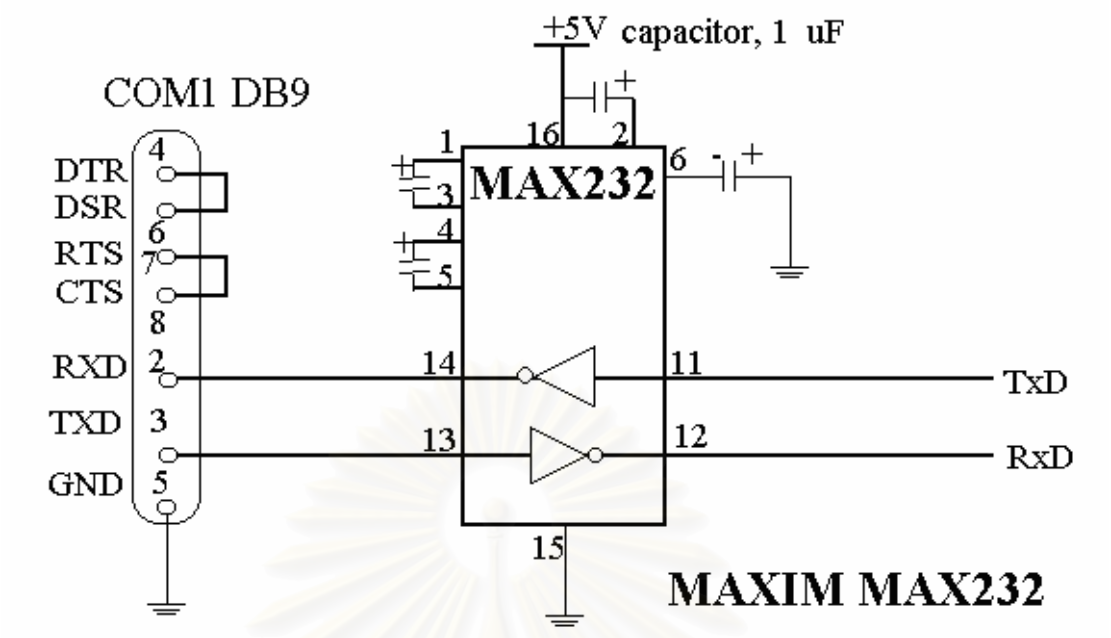


Figure 5. MAX220/MAX232/MAX232A Pin Configuration and Typical Operating Circuit

รูปที่ 4.2 ขาสัญญาณต่างๆ ของไอซี MAX232 และวงจรในการใช้งานทั่วไป

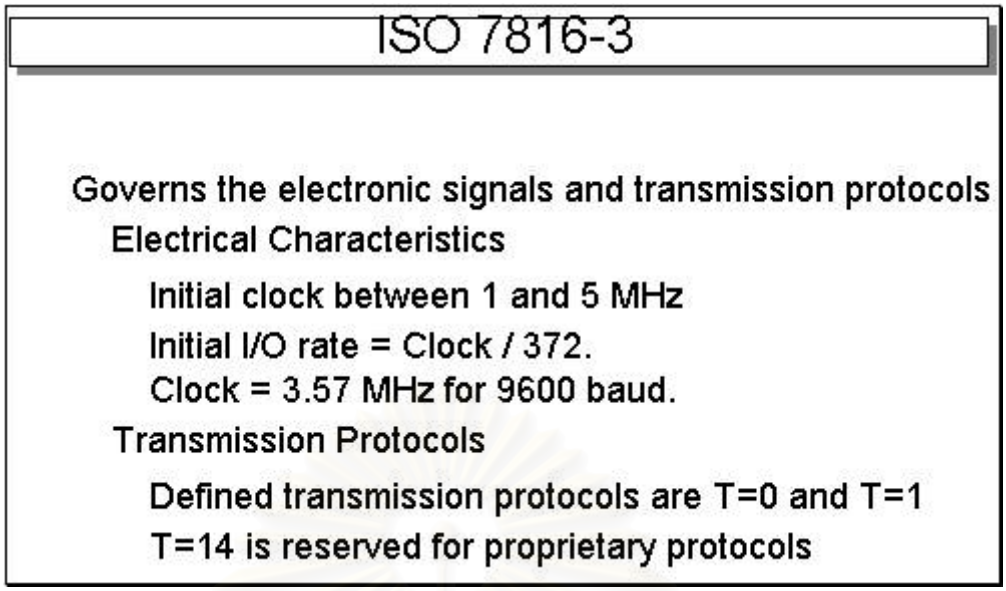
จากรูปที่ 4.2 จะเห็นได้ว่าในการนำไอซีเบอร์ MAX232 มาใช้งาน จำเป็นจะต้องมีการต่อตัวเก็บประจุ (Capacitor) ภายนอก 4 ตัว ซึ่งก็คือ C1-C4 โดยในวงจรของเครื่องอ่าน/เขียนสมาร์ตคาร์ด ซึ่งได้ออกแบบให้ใช้ ตัวเก็บประจุทั้ง 4 ตัวนี้เป็นชนิดแทนทาลัม สำหรับค่าของตัวเก็บประจุนั้นได้ใช้ตามที่โรงงานผู้ผลิตกำหนด ดังรูปที่ 4.2 คือ 1.0 uF



รูปที่ 4.3 การต่อไอซี MAX232 กับพอร์ต RS-232 ชนิด DB9

4.2 ความถี่สัญญาณนาฬิกาที่ใช้กับเครื่องอ่าน/เขียนสมาร์ตคาร์ด

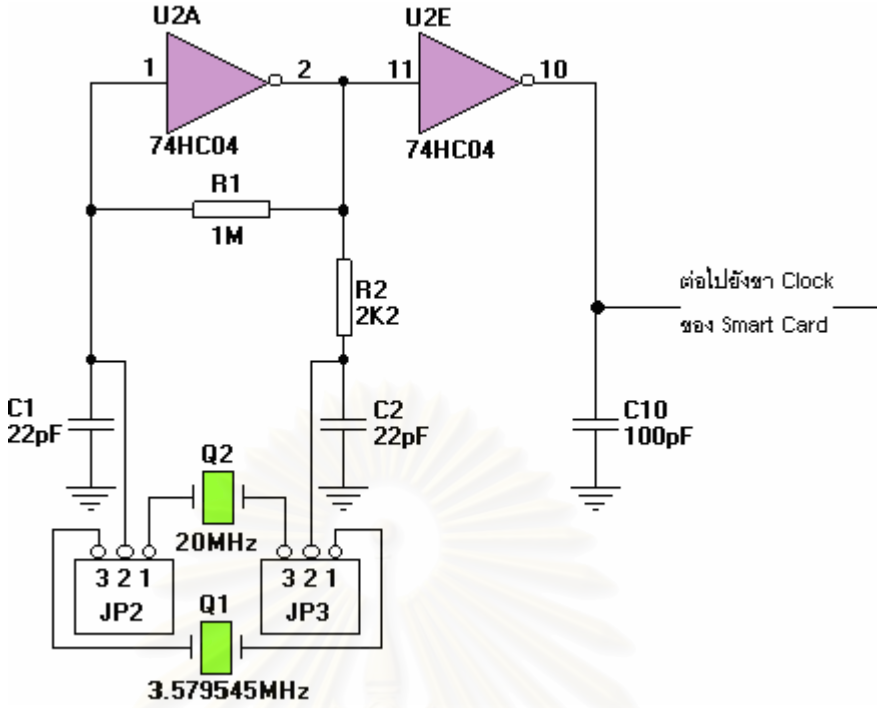
ในส่วนนี้ได้ออกแบบให้สามารถเลือกความถี่สัญญาณนาฬิกาที่จ่ายให้กับสมาร์ตคาร์ดได้ 2 ความถี่ โดยความถี่แรกคือ 3.57 MHz ตามมาตรฐาน ISO 7816 [3] ซึ่งเมื่อใช้ความถี่สัญญาณนาฬิกาเท่ากับ 3.57 MHz จะทำให้อัตราความเร็วของการรับส่งข้อมูลที่ติดต่อระหว่างสมาร์ตคาร์ดกับตัวเครื่องอ่าน/เขียนสมาร์ตคาร์ดมีค่าเท่ากับ 9600 baud ตามรูปที่ 4.4



รูปที่ 4.4 คุณสมบัติบางประการของมาตรฐาน ISO 7816-3 [3]

โดยตัวคริสตอลจริงที่ได้ติดตั้งในเครื่องอ่าน/เขียนสมาร์ตคาร์ดจะใช้ค่า 3.579545 MHz (เหตุผลที่ใช้คริสตอลค่า 3.579545 MHz เนื่องจากเป็นค่าที่ใกล้เคียงที่สุดที่หาได้ในท้องตลาดเมื่อเทียบกับ 3.57 MHz) เป็นตัวกำเนิดความถี่สัญญาณนาฬิกาให้กับตัวสมาร์ตคาร์ด

ส่วนความถี่ที่สองคือ 20 MHz ซึ่งเป็นความถี่สัญญาณนาฬิกาสูงสุดสำหรับสมาร์ตคาร์ดที่เลือกใช้ในงานวิจัยชิ้นนี้สามารถรองรับได้ ซึ่งเมื่อสมาร์ตคาร์ดทำงานที่ความถี่ดังกล่าว จะส่งผลให้สามารถประมวลผลได้เร็วกว่า เมื่อใช้ความถี่สัญญาณนาฬิกาที่ 3.57 MHz มากกว่า 460%

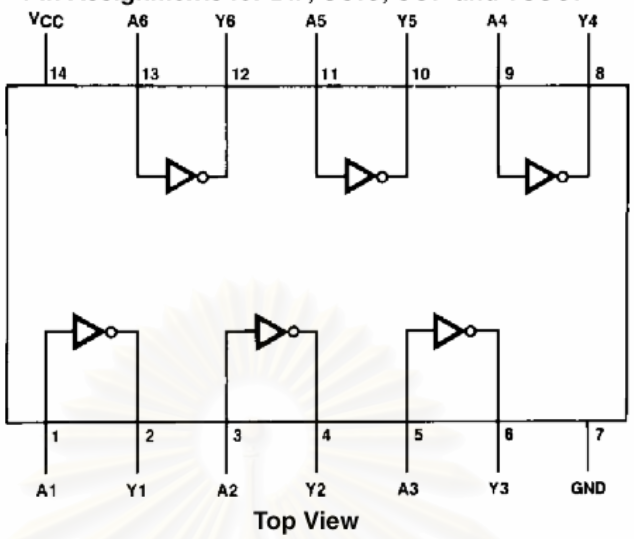


รูปที่ 4.5 วงจรในส่วนของตัวกำเนิดความถี่สัญญาณนาฬิกาให้กับสมาร์ตคาร์ด

โดยจากวงจรในรูปที่ 4.5 ได้ใช้ตัวเก็บประจุ 2 ตัวในการต่อกับคริสตอล ซึ่งในการออกแบบได้ใช้ตัวเก็บประจุแบบแทนทาลัม ซึ่งค่าที่ใช้คือ 22 pF (ฟิโคฟารัด) จากนั้นในวงจรจะใช้อินเวอร์เตอร์เกต 2 ตัว เพื่อให้เกิดเป็นความถี่สัญญาณนาฬิกา โดยอินเวอร์เตอร์เกตจะใช้จากไอซีเบอร์ 74HC04 ซึ่งภายในไอซีเบอร์ 74HC04 จะมีตัวอินเวอร์เตอร์เกตอยู่ 6 ตัว ดังแสดงในรูปที่ 4.6

Connection Diagram

Pin Assignments for DIP, SOIC, SOP and TSSOP



Top View

รูปที่ 4.6 ตำแหน่งของตัวอินเวอร์เตอร์ภายในไอซี 74HC04 ทั้ง 6 ตัว และตำแหน่งขาที่ต่อกับภายนอกของอินเวอร์เตอร์แต่ละตัว

Absolute Maximum Ratings(Note 1)

(Note 2)

Supply Voltage (V_{CC})	−0.5 to +7.0V
DC Input Voltage (V_{IN})	−1.5 to V_{CC} +1.5V
DC Output Voltage (V_{OUT})	−0.5 to V_{CC} +0.5V
Clamp Diode Current (I_{IK}, I_{OK})	±20 mA
DC Output Current, per pin (I_{OUT})	±25 mA
DC V_{CC} or GND Current, per pin (I_{CC})	±50 mA
Storage Temperature Range (T_{STG})	−65°C to +150°C
Power Dissipation (P_D)	
(Note 3)	600 mW
S.O. Package only	500 mW
Lead Temperature (T_L)	
(Soldering 10 seconds)	260°C

Recommended Operating Conditions

	Min	Max	Units
Supply Voltage (V_{CC})	2	6	V
DC Input or Output Voltage (V_{IN}, V_{OUT})	0	V_{CC}	V
Operating Temperature Range (T_A)	−40	+85	°C
Input Rise or Fall Times			
(t_r, t_f) V_{CC} = 2.0V		1000	ns
V_{CC} = 4.5V		500	ns
V_{CC} = 6.0V		400	ns

Note 1: Absolute Maximum Ratings are those values beyond which damage to the device may occur.

Note 2: Unless otherwise specified all voltages are referenced to ground.

Note 3: Power Dissipation temperature derating — plastic "N" package: −12 mW/°C from 65°C to 85°C.

รูปที่ 4.7 คุณสมบัติบางส่วนของไอซี 74HC04

จากรูปที่ 4.7 จะพบว่าระดับแรงดันไฟ (Vcc) ที่ไอซีเบอร์ 74HC04 ใช้งานจะอยู่ในช่วงระหว่าง 2 โวลต์ ถึง 6 โวลต์ ดังนั้นในวงจรนี้ได้ออกแบบให้ไอซีเบอร์ 74HC04 ใช้ระดับแรงดันไฟ (Vcc) ที่มีค่าเท่ากับ 5 V เพื่อเป็นการลดความซับซ้อนในวงจร และง่ายต่อการออกแบบเนื่องจากในไอซีเบอร์ MAX232 และสมาร์ตคาร์ด ก็สามารถใช้งานได้กับระดับแรงดันไฟ เท่ากับ 5 V ได้เช่นกัน โดยไอซีเบอร์ 74HC04 ที่นำมาใช้ในวงจร ได้เลือกใช้แพ็คเก็จแบบ PDIP

4.3 IC Voltage Regulator ที่ใช้ในเครื่องอ่าน/เขียนสมาร์ตคาร์ด

เนื่องจากตัวสมาร์ตคาร์ด และตัวอุปกรณ์ต่างๆ ในวงจรเครื่องอ่าน/เขียนสมาร์ตคาร์ด ใช้ระดับแรงดันไฟ (Vcc) = 5V เป็นส่วนใหญ่ ดังนั้นในการออกแบบวงจรจึงเลือกใช้ไอซี Voltage Regulator แบบ 5V โดยได้เลือกใช้เบอร์ MC78L05ACP ซึ่งมีเหตุผลที่เลือกใช้งาน ดังนี้

1. มีช่วงของการรับระดับแรงดันขาเข้า (Voltage Input) ได้กว้าง ซึ่งทำให้เครื่องอ่าน/เขียนสมาร์ตคาร์ด ที่ออกแบบสามารถใช้ได้ตั้งแต่ในช่วง 5 โวลต์ ถึง 15 โวลต์ ทำให้มีความยืดหยุ่นในการติดตั้งและใช้งาน โดยสามารถใช้ไฟ 12 โวลต์ จากแหล่งจ่ายไฟของเครื่องคอมพิวเตอร์โดยตรง หรือสามารถใช้ถ่านแบบก้อนสี่เหลี่ยม 9 V เป็นต้น
2. ระดับแรงดันขาออก (Output Voltage) มีค่าคงที่ = 5 โวลต์ และมีค่าความคลาดเคลื่อนไม่เกิน 5%
3. มีการจำกัดกระแสของ Internal Short Circuit
4. มีการป้องกัน Internal Thermal Overload
5. มีขนาดที่เล็ก ทำให้ประหยัดเนื้อที่ และง่ายต่อการออกแบบจัดวางอุปกรณ์

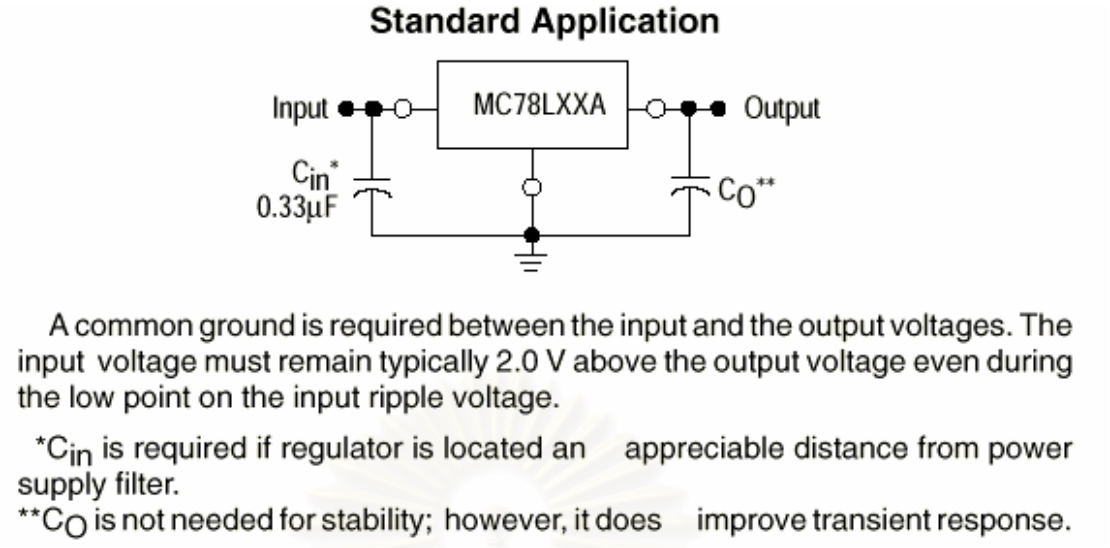
Pin: 1. Output
2. Ground
3. Input

1. **ขาของไฟออก**
2. **ขาของ** Ground
3. **ขาของไฟเข้า**

รูปที่ 4.8 ลักษณะรูปร่างของไอซี MC78L05ACP

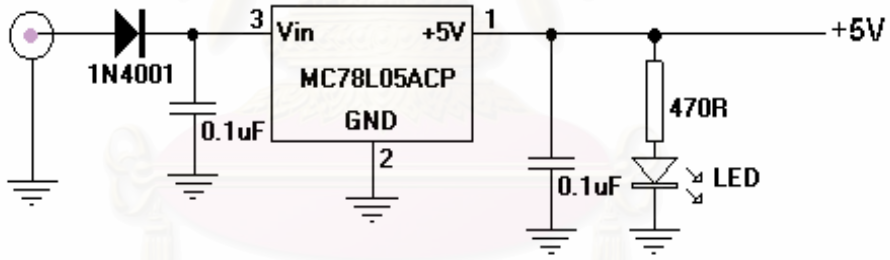
และรายละเอียดของขาที่ติดต่อกับภายนอก

ซึ่งจากรูปที่ 4.8 จะเห็นได้ว่าไอซีเบอร์ MC78L05ACP มีรูปแบบการใช้งานที่ง่าย โดยมีขาเชื่อมต่อ เพียง 3 ขาเท่านั้น



รูปที่ 4.9 การนำไอซี MC78L05ACP ไปใช้งานมาตรฐานทั่วไป

โดยในวงจรเครื่องอ่าน/เขียนสมาร์ตคาร์ด มีรูปแบบการใช้งานไอซีเบอร์ MC78L05ACP และการเชื่อมต่อตามรูปที่ 4.9 โดยใช้ค่าของ C_{in} เท่ากับ 0.1 uF และค่าของ C_O เท่ากับ 0.1 uF



รูปที่ 4.10 วงจรที่ใช้งานจริงของเครื่องอ่าน/เขียนสมาร์ตคาร์ดในส่วนของภาคจ่ายไฟ

จากรูปที่ 4.10 จะเห็นว่า จากตรงขาที่ต่อไฟเข้าได้นำเอาไดโอดเบอร์ IN4001 มาต่อคั่นกลางกับไอซีเบอร์ MC78L05ACP เพื่อให้ตัวไดโอดเบอร์ IN4001 ทำหน้าที่กรองกระแสไฟ เพื่อป้องกันในกรณีที่ไฟที่เข้ามาเป็นไฟกระแสสลับ (AC : Alternating Current) ซึ่งอาจทำให้เกิดความเสียหายขึ้นกับวงจรได้และในตอนท้ายของภาพที่ 4.10 จะเห็นว่าได้ออกแบบให้ติดตั้ง LED (Light Emitting Diode) ไว้เพื่อเป็นการตรวจสอบกระแสไฟที่เข้าวงจรและตรวจสอบการทำงานของตัวไอซี MC78L05ACP ซึ่ง LED จะถูกต่อมาจากขา Output ของไอซี MC78L05ACP โดยมีตัวต้านทานขนาด 1/8 วัตต์ ค่า 470 Ω ต่อคั่นกลางระหว่างไอซี MC78L05ACP กับ LED เนื่องจากระดับแรงดันที่ออกมาจากขา Output (5 V) ของไอซี MC78L05ACP มีค่าสูงเกินไปสำหรับ LED

จึงต้องทำการออกแบบให้มีตัวต้านทานคั่นกลางเพื่อให้มีแรงดันตกคร่อมบนตัวต้านทาน เพื่อควบคุมระดับแรงดันที่จ่ายไปยัง LED โดยทั่วไปแล้วแรงดันตกคร่อมตัว LED ควรจะมีค่าเท่ากับ 2 โวลต์ ดังนั้นต้องมีแรงดันตกคร่อมตัวต้านทานเท่ากับ 5-2 = 3 โวลต์

ค่ากระแสที่เหมาะสมกับ LED ควรมีค่าประมาณ 0.0063 A

โดยสามารถคำนวณ หาค่าความต้านทานที่ต้องการได้ดังนี้

จากสูตร V = IR

ทราบค่า V ซึ่งมีค่าเท่ากับ 3 โวลต์

ทราบค่า I เนื่องจากการต่ออนุกรมกระแสจะเท่ากันทั้งวงจร ดังนั้นกระแสที่ไหลผ่านตัว LED จะต้องมีค่าเท่ากับกระแสที่ไหลผ่านตัวต้านทาน ซึ่งมีค่าเท่ากับ 0.0063 A

ดังนั้นเมื่อนำค่าเข้าไปแทนในสูตร จะสามารถหาค่าความต้านทาน ได้ดังนี้

จากสูตร V = IR

3 = 0.0063 X R

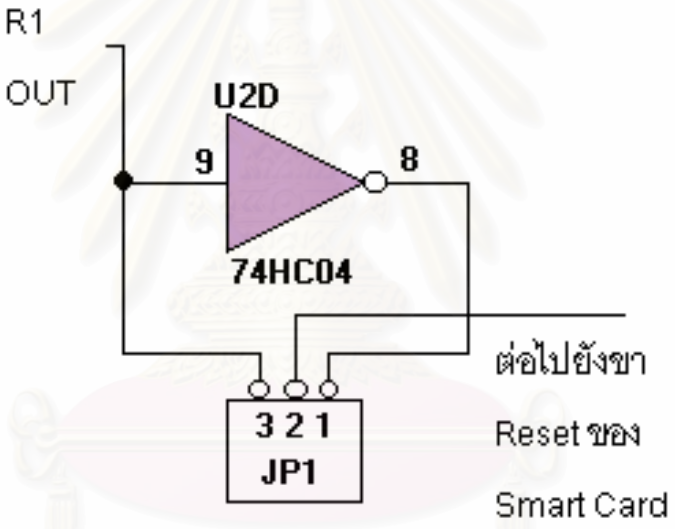
R = 3/0.0063

R = 476.190476190476190476190476190476

ซึ่งค่าของตัวต้านทานที่ใกล้เคียงที่สุดที่หาได้ตามท้องตลาดคือ 470 Ω ดังนั้น จึงใช้ค่าความต้านทาน 470 Ω ต่อคั่นกลางระหว่างไอซีเบอร์ MC78L05ACP กับ LED

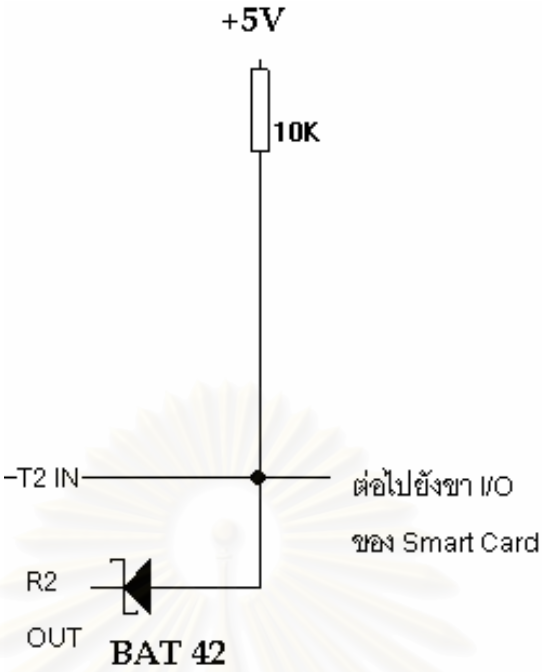
4.4 การออกแบบวงจรเชื่อมต่อระหว่างไอซี MAX232 กับสมาร์ตคาร์ด

โดยในการออกแบบนี้ ขั้นแรกจากคุณสมบัติที่ได้กำหนดไว้ให้ตัวเครื่องอ่าน/เขียนสมาร์ตคาร์ดนี้ ได้กำหนดให้สามารถใช้งานได้กับสมาร์ตคาร์ด ตามมาตรฐาน ISO 7816 ที่เป็นแบบ Asynchronous (Processor Card) เพื่อให้เครื่องอ่าน/เขียนสมาร์ตคาร์ด สามารถรองรับสมาร์ตคาร์ดได้ทั้งแบบที่ขารีเซตจะทำงานเมื่อมีลอจิกต่ำ (Active Low) และแบบที่ขารีเซตจะทำงานเมื่อมีลอจิกสูง (Active High) ดังนั้นในการออกแบบในส่วนที่ติดต่อกับขารีเซตของสมาร์ตคาร์ด จึงต้องทำการออกแบบให้มีจัมเปอร์ ในการเลือกว่าจะต่อผ่านตัวอินเวอร์เตอร์หรือไม่ โดยตัวอินเวอร์เตอร์ ที่นำมาใช้นี้จะมาจากไอซีเบอร์ 74HC04 ตัวเดียวกับที่ได้ใช้ในส่วนของการสร้างความถี่สัญญาณนาฬิกาให้กับสมาร์ตคาร์ด โดยได้กล่าวไปแล้วในหัวข้อที่ 4.2



รูปที่ 4.11 ภาพขยายวงจรส่วนของจัมเปอร์และอินเวอร์เตอร์

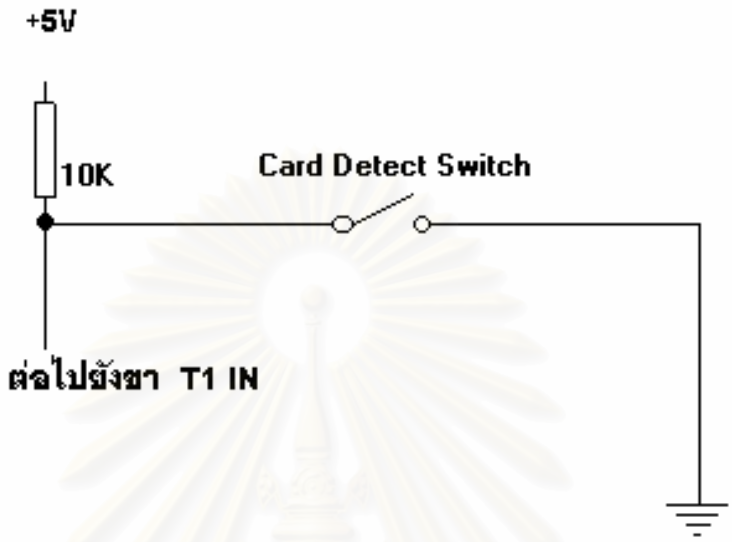
ในส่วนของการติดต่อกับขาข้อมูล (I/O) ของสมาร์ตคาร์ดนั้นได้ทำต่อจาก T2 IN กับ R2 OUT ไปยังขา I/O ของ สมาร์ตคาร์ด



รูปที่ 4.12 ภาพขยายวงจรในส่วนของการติดต่อกับขาข้อมูล (I/O) ของสมาร์ตคาร์ด

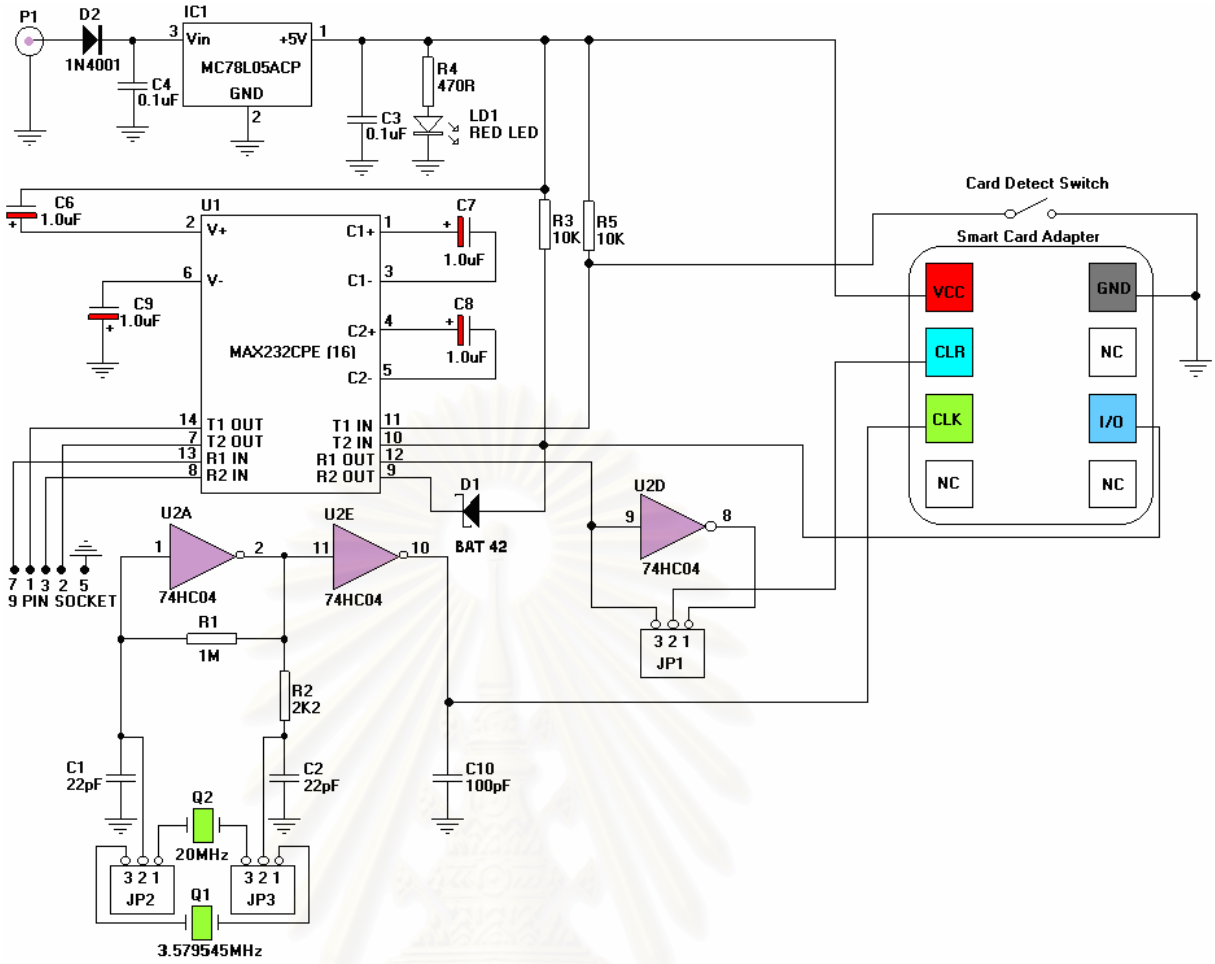
จากรูปที่ 4.12 จะพบว่าส่วนที่ต่อกับขา R2 ของไอซี MAX232 นั้น มีไดโอด (Diode) แบบ Small Signal Schottky เบอร์ BAT42 ต่อไว้เพื่อทำหน้าที่เป็นตัวควบคุมทิศทางข้อมูลของขา Data โดยข้อมูลที่จะส่งไปยังเครื่องคอมพิวเตอร์จะถูกส่งผ่านขา T2 IN ของไอซี MAX232 และในกรณีที่รับข้อมูลจากเครื่องคอมพิวเตอร์จะรับผ่านทางขา R2 OUT ของไอซี MAX232

4.5 วงจรตรวจสอบว่ามีสมาร์ตคาร์ดเสียบเข้ากับเครื่องอ่าน/เขียนสมาร์ตคาร์ดหรือไม่ (Card Detect Switch)



รูปที่ 4.13 วงจรตรวจสอบว่ามีสมาร์ตคาร์ดเสียบเข้ากับเครื่องอ่าน/เขียนสมาร์ตคาร์ดหรือไม่

ในการที่ตรวจสอบว่าได้มีสมาร์ตคาร์ดเสียบเข้าเครื่องอ่าน/เขียนสมาร์ตคาร์ดแล้วหรือยัง จะใช้ตัว Card Detect Switch ที่อยู่ในช่องเสียบสมาร์ตคาร์ด (Smart Card Connector) ซึ่งเป็นแบบที่จะเชื่อมต่อวงจรเมื่อไม่มีสมาร์ตคาร์ดเสียบอยู่ และจะเปิดวงจรเมื่อมีสมาร์ตคาร์ดเสียบเข้ามา (Normal Close) โดยในสถานะที่ไม่มีสมาร์ตคาร์ดในช่องเสียบสมาร์ตคาร์ด ตัววงจรจะถูกเชื่อมต่อกับ Ground ส่งผลให้กระแสไฟที่ไหลจากตัวต้านทานที่ Pull up ไว้ จะไหลลง Ground หมด ซึ่งจะทำให้ไม่มีกระแสไหลไปยังขา T1 IN ของไอซีเบอร์ MAX232 ส่งผลให้ลอจิกที่ขา T1 มีค่าเป็น 0 ในส่วนของกรณีที่มีสมาร์ตคาร์ดอยู่ในช่องเสียบสมาร์ตคาร์ด ตัวสวิชต์จะอยู่ในสถานะเปิดวงจรทำให้วงจรไม่ต่อกับ Ground ส่งผลให้กระแสจากตัวต้านทานไหลไปยังขา T1 IN ของตัวไอซี MAX232 ทำให้ลอจิกที่ขา T1 มีค่าเป็น 1 ซึ่งตัวไอซี MAX232 จะทำการแปลงค่าลอจิกนี้ส่งออกไปยังเครื่องคอมพิวเตอร์ผ่านทางพอร์ต RS-232



รูปที่ 4.14 วงจรที่สมบูรณ์ โดยรวมทุกส่วนของวงจรที่ได้กล่าวไว้ข้างต้น

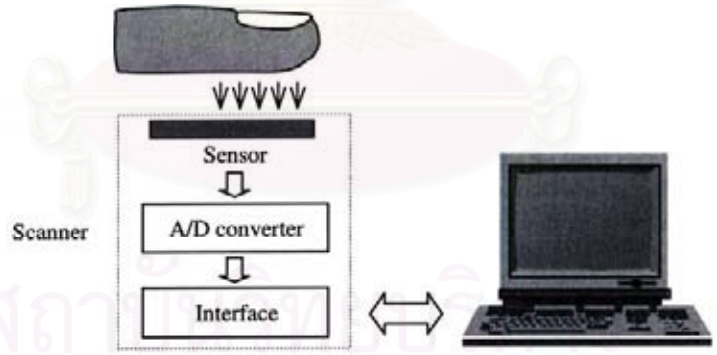
รูปที่ 4.15 เครื่องอ่าน/เขียนสมาร์ตคาร์ด ที่ประกอบเสร็จเรียบร้อย

บทที่ 5
การทดลอง

ในบทนี้ จะได้กล่าวถึงการทดลองและผลที่ได้จากการทดลองของการทดสอบโปรแกรมตรวจสอบลายนิ้วมือกับภาพลายนิ้วมือที่คัดเลือกจากฐานข้อมูลภาพลายนิ้วมือที่ได้เก็บข้อมูลจากอาสาสมัคร จำนวน 70 คน และภาพลายนิ้วมือบางส่วนจากฐานข้อมูล FVC2002

5.1 หลักการทำงานของเครื่องอ่านลายนิ้วมือแบบใช้แสงชนิด Frustrated Total Internal Reflection (FTIR) [6]

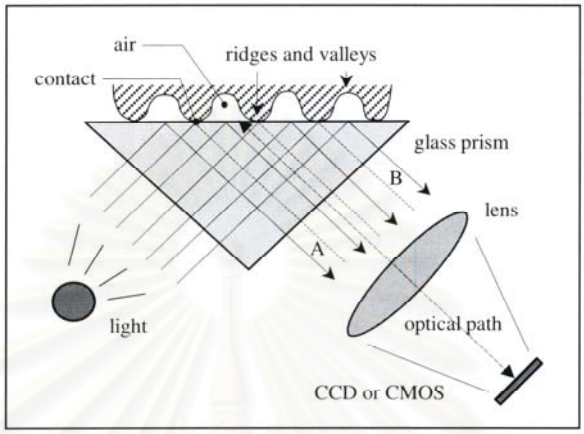
หลักการทำงานของเครื่องอ่านลายนิ้วมือโดยทั่วไป จะทำการอ่านพื้นผิวลายนิ้วมือที่สัมผัสกับหน้าสัมผัสของเครื่องอ่านลายนิ้วมือและแปลงข้อมูลที่ได้จาก Analog เป็น Digital จากนั้นจะส่งข้อมูลไปยังอุปกรณ์ภายนอก เช่น เครื่องคอมพิวเตอร์ ดังที่ได้แสดงในรูปที่ 5.1



รูปที่ 5.1 ขั้นตอนการทำงานของเครื่องอ่านลายนิ้วมือ ที่มา: [6]

เครื่องอ่านลายนิ้วมือที่ใช้ในวิทยานิพนธ์ฉบับนี้ เป็นแบบ FTIR (Frustrated Total Internal Reflection) มีหลักการทำงาน คือ เมื่อมีนิ้วมือสัมผัสที่ด้านของแก้ว (หรือพลาสติก) ที่ทำหน้าที่เป็นปริซึม ส่วนที่เป็นเส้นลายนิ้วมือจะสัมผัสกับปริซึมโดยตรง แต่ส่วนที่เป็นร่องของลายนิ้วมือจะอยู่ห่างจากปริซึมในระยะหนึ่ง (ดูรูปที่ 5.2 ด้านล่างประกอบ) ที่ด้านซ้ายจะมีแหล่งกำเนิดแสง ซึ่งเมื่อแสงผ่านเข้าไปยังปริซึม ส่วนที่อยู่บริเวณร่องของลายนิ้วมือก็จะสะท้อนแสงออกมาไปยังส่วนรับ

ภาพที่อยู่ด้านขวามือกลายเป็นส่วนสีขาวในภาพลายนิ้วมือ ในขณะเดียวกันส่วนที่เป็นเส้นลายนิ้วมือจะก็จะดูดซับแสงที่มาจากแหล่งกำเนิดแสงด้านซ้าย เป็นส่วนใหญ่ไว้ ส่งผลให้ไม่มีแสงไปยังส่วนรับภาพด้านขวา (หรือมีน้อย) จึงเกิดเป็นเส้นลายนิ้วมือสีดำหรือเทาในภาพลายนิ้วมือ



รูปที่ 5.2 หลักการทำงานที่ใช้ในเครื่องอ่านลายนิ้วมือแบบ FTIR ที่มา: [6]

เนื่องจากรูปแบบการทำงานดังแสดงในรูปที่ 5.2 รูปทรงของภาพที่ได้จะมีความผิดเพี้ยนเนื่องมาจากระนาบที่วางลายนิ้วมือไม่ได้ขนานกับตัวรับภาพจึงทำให้แสง A และ B ดังแสดงในภาพที่ 5.2 เดินทางในระยะที่ต่างกัน ซึ่งทำให้เกิดผลลัพธ์ คือ ภาพบางส่วนจะมีการถูกขยายหรือย่อส่วนลง การแก้ไขข้อผิดพลาดดังกล่าว สามารถทำได้หลายวิธี เช่น การปรับแต่งทางด้านโปรแกรมที่ใช้รับภาพจากเครื่องอ่านลายนิ้วมือ หรือการปรับแต่งทางด้านการรับแสงโดยใช้เลนส์รับแสงแบบพลาสติกที่ออกแบบเป็นพิเศษเพื่อแก้ปัญหานี้ เป็นต้น

ในบางครั้งเมื่อนิ้วมือแห้งมากๆ จะทำให้นิ้วมือไม่สัมผัสกับหน้าสัมผัสของเครื่องอ่านลายนิ้วมือได้อย่างปกติ ส่งผลให้ภาพลายนิ้วมือที่อ่านได้จะจางมาก การปรับปรุงให้เครื่องอ่านลายนิ้วมือสามารถอ่านลายนิ้วมือที่แห้งมากๆ ได้ดีขึ้น สามารถทำได้โดยเคลือบซิลิโคนไว้ที่ส่วนหน้าสัมผัสของเครื่องอ่านลายนิ้วมือ ซึ่งจะช่วยให้นิ้วสัมผัสกับหน้าสัมผัสของเครื่องอ่านลายนิ้วมือได้ดียิ่งขึ้น

5.2 เครื่องอ่านลายนิ้วมือที่ใช้ในการเก็บข้อมูล

ในส่วนการเก็บภาพลายนิ้วมือจากอาสาสมัคร ได้ทำการเก็บภาพลายนิ้วมือจากอาสาสมัคร จำนวน 70 คน โดยเก็บภาพลายนิ้วมือผ่านทางเครื่องอ่านลายนิ้วมือ จำนวน 2 รุ่น ดังนี้

5.2.1 เครื่องอ่านลายนิ้วมือแบบแสง ชนิด FTIR รุ่น U.are.U 2000

เป็นผลิตภัณฑ์จากบริษัท Digital Persona ผลิตในประเทศไทย ให้ความละเอียดของภาพสูงสุดขนาด 358x286 พิกเซล ภาพที่ได้เป็นภาพระดับเทา 8 บิต โดยที่เครื่องไม่มีการติดตั้งตัวจำกัดขอบเขตนิ้วมือไว้ (Finger guide) การเชื่อมต่อกับเครื่องคอมพิวเตอร์เป็นแบบ USB (Universal Serial Bus)

รูปที่ 5.3 เครื่องอ่านลายนิ้วมือแบบแสง รุ่น U.are.U 2000

รูปที่ 5.4 ภาพลายนิ้วมือที่อ่านได้จากเครื่องอ่านลายนิ้วมือรุ่น U.are.U 2000

5.2.2 เครื่องอ่านลายนิ้วมือแบบแสง ชนิด FTIR รุ่น U.are.U 4000B

เป็นผลิตภัณฑ์จากบริษัท Digital Persona ผลิตในประเทศจีน ให้ความละเอียดของภาพสูงสุดขนาด 462x522 พิกเซล ภาพที่ได้เป็นภาพระดับเทา 8 บิต โดยที่เครื่องอ่านลายนิ้วมือมีการติดตั้งตัวจำกัดขอบเขตนิ้วมือไว้ การเชื่อมต่อกับเครื่องคอมพิวเตอร์เป็นแบบ USB

รูปที่ 5.5 เครื่องอ่านลายนิ้วมือแบบแสง รุ่น U.are.U 4000B

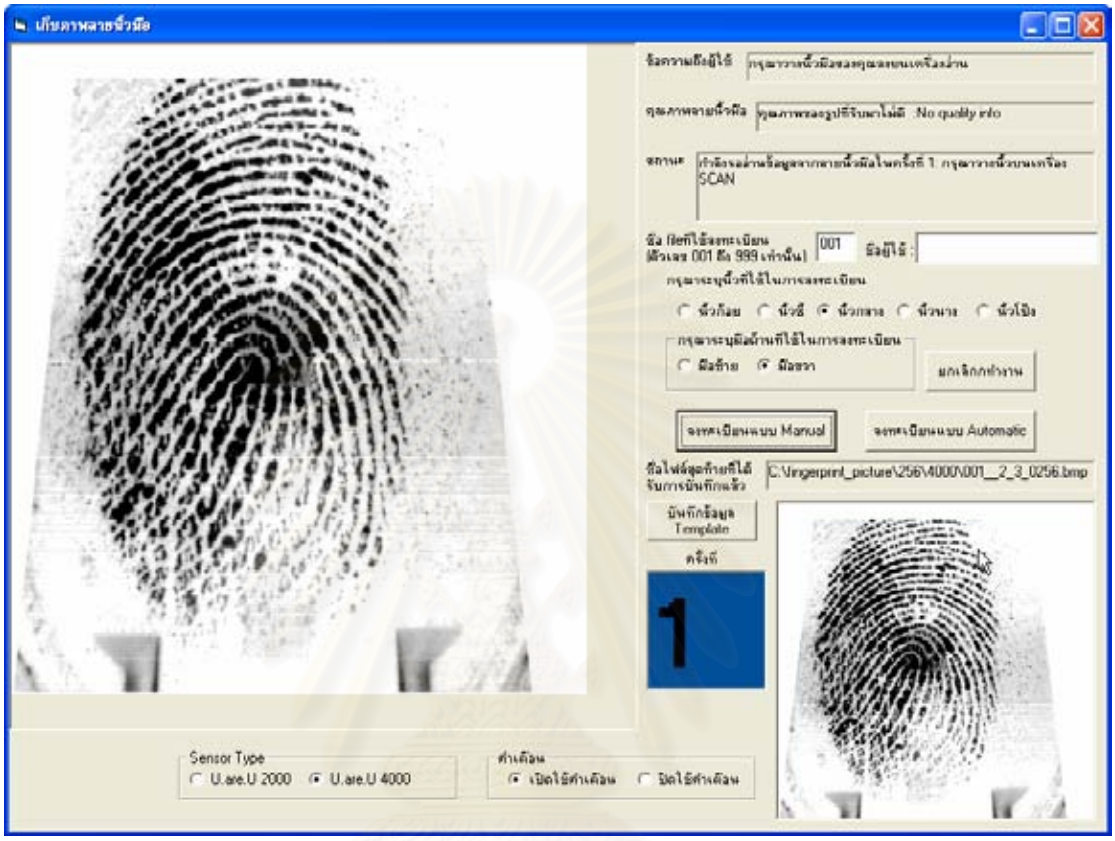
รูปที่ 5.6 ภาพลายนิ้วมือที่อ่านได้จากเครื่องอ่านลายนิ้วมือรุ่น U.are.U 4000B

5.3 การเก็บภาพลายนิ้วมือจากอาสาสมัคร

ในการเก็บลายนิ้วมือจากอาสาสมัคร ได้กำหนดให้เก็บภาพลายนิ้วมือ จากนิ้วนาง, นิ้วกลาง, นิ้วชี้ และนิ้วโป้ง จากมือทั้งสองด้าน (สาเหตุที่ไม่ใช้นิ้วก้อยในการเก็บข้อมูลเนื่องจากมีขนาดเล็กเกินไป และในบางกรณีที่นิ้วก้อยของอาสาสมัครมีขนาดเล็กมากจะมีจำนวนจุดสำคัญบนเส้นลายนิ้วมือที่อ่านได้ไม่เพียงพอ) โดยจะเก็บภาพลายนิ้วมือ จำนวน 12 ครั้งต่อหนึ่งนิ้วและต่อ 1 เครื่องอ่านลายนิ้วมือ

ได้ทำการเขียนโปรแกรมเพื่อทำการติดต่อกับเครื่องอ่านลายนิ้วมือทั้งสองรุ่นและบันทึกภาพลายนิ้วมือลงบน Hard disk โดยภาพที่ได้จากเครื่องอ่านลายนิ้วมือจะถูกเก็บในรูปแบบ

.bmp (Bitmap) โดยที่ชื่อไฟล์จะระบุลำดับจำนวนคนที่เก็บ, นิ้วที่เก็บ, จำนวนครั้งที่เก็บภาพของนิ้วนั้นๆ



รูปที่ 5.7 โปรแกรมที่ใช้ในการเก็บข้อมูลภาพลายนิ้วมือจากอาสาสมัคร

5.3.1 ปัญหาที่พบจากเก็บข้อมูลภาพลายนิ้วมือจากอาสาสมัคร

1. พื้นที่รับภาพของเครื่องอ่านลายนิ้วมือรุ่น U.are.U 2000 มีขนาดเล็กกว่านิ้วมือของบุคคลส่วนใหญ่ และเนื่องจากการรับภาพในแต่ละครั้งอาจจะมีการเปลี่ยนแปลงมุมและตำแหน่งของนิ้วมือที่กดลงบนหน้าสัมผัสของเครื่องอ่านลายนิ้วมือ จึงทำให้ภาพลายนิ้วมือที่รับเข้ามาในบางครั้งมีบางส่วนของลายนิ้วมือที่ขาดหายไป โดยเฉพาะอย่างยิ่งส่วนด้านขอบ จึงทำให้มีเฉพาะบางส่วนของลายนิ้วมือเท่านั้นที่จะคงอยู่เหมือนกันในทุกภาพที่รับเข้ามา

2. ภาพที่ได้จากเครื่องอ่านลายนิ้วมือรุ่น U.are.U 4000B จะมีรูปสี่เหลี่ยมอยู่กึ่งกลางภาพเกือบทุกภาพ ในระดับโทนสีเทาจนถึงดำสนิท ซึ่งกว่า 30% ของภาพที่ทำการเก็บข้อมูลรูปสี่เหลี่ยมดังกล่าวจะค่อนข้างเข้มมาก ทำให้การค้นหาจุดสำคัญของภาพลายนิ้วมือในบริเวณดังกล่าวเกิดข้อผิดพลาด

3. ในบางครั้งนิ้วมือของอาสาสมัครแห้งเกินไปหรือออกแรงกดน้อยเกินไป ทำให้ภาพที่รับมาได้จากเครื่องอ่านลายนิ้วมือ จะจางมาก ซึ่งเมื่อผ่านขั้นตอนการปรับคุณภาพของภาพก่อนการค้นหาจุดสำคัญบนเส้นลายนิ้วมือ (Image preprocessing) แล้วทำให้เกิดเส้นลายนิ้วมือขาดเป็นจำนวนมาก แก้ไขโดยให้อาสาสมัครทำการนำมือทั้งสองมาถูกันเพื่อให้มือมีความชื้นมากขึ้น หรือให้ออกแรงกดเพิ่มมากขึ้น

รูปที่ 5.8 ตัวอย่างภาพลายนิ้วมือจากนิ้วที่แห้งเกินไป

4. ในบางครั้งนิ้วมือของอาสาสมัครเปียกมากเกินไปหรือออกแรงมากเกินไป ทำให้ภาพที่รับมาได้จากเครื่องอ่านลายนิ้วมือ จะดำไปทั้งภาพ ซึ่งทำให้ไม่สามารถแยกแยะระหว่างเส้นนูนกับเส้นร่องได้ แก้ไขโดยทำการเช็ดมือให้แห้งขึ้น หรือลดระดับแรงกดให้น้อยลง

รูปที่ 5.9 ตัวอย่างภาพลายนิ้วมือจากนิ้วที่เปียกเกินไป

5.4 สมาร์ตคาร์ดที่ใช้ในงานวิจัย

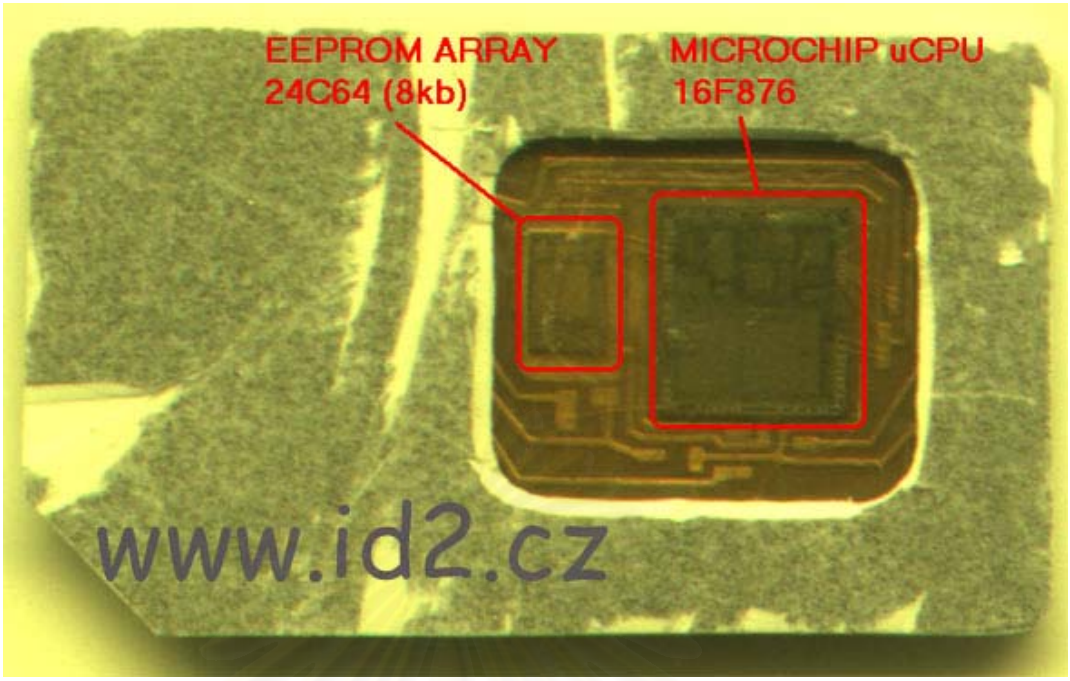
สมาร์ตคาร์ดที่ได้คัดเลือกนำมาใช้ในงานวิจัยชิ้นนี้ ภายในประกอบไปด้วยไมโครคอนโทรลเลอร์ ขนาด 8 บิต จากบริษัท Microchip เบอร์ PIC16F876 และหน่วยความจำข้อมูล EEPROM อนุกรม แบบ I^2C (Inter-IC Communication) ขนาดความจุ 64 กิโลบิต เบอร์ 24LC64 โดยการเชื่อมต่อภายในเป็นดังรูปที่ 5.11

5.4.1 คุณสมบัติหลักของไมโครคอนโทรลเลอร์ PIC16F876

1. หน่วยประมวลผลเป็นแบบ RISC (Reduced Instruction-Set Computer) มีคำสั่งการทำงานเพียง 35 คำสั่ง
2. รองรับความถี่สัญญาณนาฬิกาสูงสุดถึง 20 MHz
3. มีขนาดหน่วยความจำโปรแกรม 8 กิโลเวิร์ด
4. มีขนาดหน่วยความจำชั่วคราว 368 ไบต์
5. มีหน่วยความจำข้อมูล EEPROM ภายใน 256 ไบต์
6. มีสแต็ก 8 ระดับ

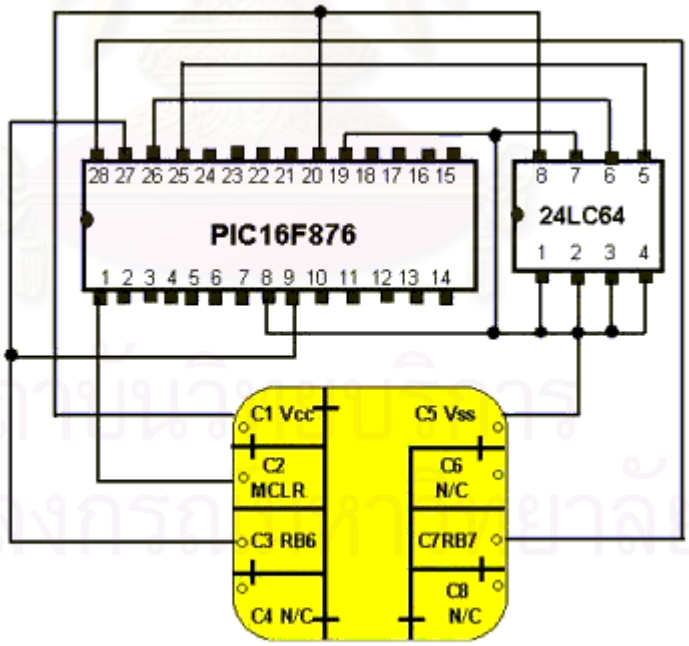
5.4.2 การโปรแกรมข้อมูลของโปรแกรมเปรียบเทียบลายนิ้วมือลงบนสมาร์ตคาร์ด

หลังจากที่ได้เขียนโปรแกรมระบบปฏิบัติการสมาร์ตคาร์ด (Smartcard OS) และทำการแปลงโปรแกรมเป็น .Hex แล้ว จากนั้นจะนำข้อมูลโปรแกรม .Hex ที่ได้ไปเขียนลงหน่วยความจำโปรแกรมส่วนที่เป็น Flash Memory ของสมาร์ตคาร์ด ผ่านทางเครื่องโปรแกรมไอซี (IC Programmer) โดยทำการต่อสายสัญญาณจากเครื่องโปรแกรมไอซีไปยังหน้าสัมผัสของสมาร์ตคาร์ด จำนวน 5 เส้น ผ่านทางช่องเสียบสมาร์ตคาร์ด ซึ่งประกอบไปด้วย ขา GND, ขา VCC, ขา MCLR, ขา RB6 และ ขา RB7



รูปที่ 5.10 ภายในของสมาร์ตคาร์ด PIC16F876 + 24C64

ที่มา : http://www.id2.cz/silvercard.htm



รูปที่ 5.11 การเชื่อมต่อภายในสมาร์ตคาร์ด PIC16F876 + 24LC64

รูปที่ 5.12 ด้านที่มีขาสัญญาณของสมาร์ตคาร์ด PIC16F876 + 24C64

รูปที่ 5.13 ด้านที่ไม่มีขาสัญญาณของสมาร์ตคาร์ด PIC16F876 + 24C64

5.5 การเพิ่มความเร็วในการประมวลผลของสมาร์ตคาร์ดโดยเพิ่มความถี่สัญญาณนาฬิกา

ในหัวข้อนี้จะกล่าวถึงวิธีการเพิ่มความเร็วในการประมวลผลของสมาร์ตคาร์ด ที่นอกเหนือจากการปรับปรุงทางด้านโปรแกรมที่ใช้ในการตรวจสอบลายนิ้วมือบนสมาร์ตคาร์ด โดยจุดประสงค์ของการเพิ่มความเร็วในการประมวลผลของสมาร์ตคาร์ด เพื่อลดเวลาที่ผู้ใช้งานจะต้องรอผลลัพธ์ของการตรวจสอบลายนิ้วมือจากสมาร์ตคาร์ดให้สั้นลง

โดยทั่วไปแล้วสมาร์ตคาร์ดชนิดที่มีหน่วยประมวลผลภายในตัว ส่วนใหญ่จะทำงานที่ความถี่สัญญาณนาฬิกาประมาณ 3.57 MHz ตามมาตรฐาน ISO 7816 [3] ซึ่งโดยทั่วไปแล้วความถี่สัญญาณนาฬิกาดังกล่าวจะใช้ในการจ่ายเป็นสัญญาณนาฬิกาหลักให้กับหน่วย

ประมวลผลหลักในสมาร์ตคาร์ด ดังนั้นถ้าเพิ่มความถี่สัญญาณนาฬิกาที่จ่ายให้กับสมาร์ตคาร์ดที่ขาสัญญาณ CLK ให้สูงขึ้น ก็จะเป็นการเพิ่มความเร็วในการประมวลผลของสมาร์ตคาร์ดให้สูงขึ้นด้วย จากการศึกษากับสมาร์ตคาร์ดจำนวน 4 ใบ ที่ใช้ชนิดของหน่วยประมวลแตกต่างกัน พบว่าความถี่สัญญาณนาฬิกาสูงสุดที่สมาร์ตคาร์ดสามารถรองรับได้นั้น จะขึ้นอยู่กับความถี่สัญญาณนาฬิกาสูงสุดที่หน่วยประมวลผลหลักของสมาร์ตคาร์ดรองรับได้ สำหรับสมาร์ตคาร์ดที่ไม่ทราบรายละเอียดของหน่วยประมวลผลหลักภายใน สามารถทำการทดลองเพื่อหาความเร็วสูงสุดที่สมาร์ตคาร์ดนั้นสามารถทำงานได้ โดยทำการเพิ่มความถี่สัญญาณนาฬิกาจาก 3.57 MHz เพิ่มไปทีละน้อย จนกระทั้งสมาร์ตคาร์ดไม่สามารถตอบ ATR (Answer To Reset) ออกมาได้อย่างถูกต้อง ความถี่สัญญาณนาฬิกาสูงสุดที่สมาร์ตคาร์ดยังคงสามารถตอบ ATR มาได้อย่างถูกต้องจะเป็นความถี่สัญญาณนาฬิกาสูงสุดที่สมาร์ตคาร์ดสามารถรองรับได้

โดยสมาร์ตคาร์ดที่นำมาใช้ในงานวิจัยนี้ ได้ใช้หน่วยประมวลผลหลักเป็นไมโครคอนโทรลเลอร์ จากบริษัท Microchip เบอร์ PIC16F876 ซึ่งรองรับความถี่สัญญาณนาฬิกาสูงสุดได้ที่ 20 MHz ดังนั้นผลการทดลองทั้งหมดที่นำเสนอในงานวิจัยนี้จะอ้างอิงจากความถี่สัญญาณนาฬิกาที่จ่ายให้กับสมาร์ตคาร์ด ที่ความถี่ 20 MHz ซึ่งเมื่อสมาร์ตคาร์ดทำงานที่ความถี่นี้จะส่งผลให้สามารถประมวลผลได้เร็วกว่า เมื่อใช้ความถี่สัญญาณนาฬิกาที่ 3.57 MHz มากกว่า 460%

5.6 ผลการทดลอง

ในการทดลองระบบตรวจสอบลายนิ้วมือที่พัฒนาขึ้นมาใหม่นี้ ได้ทำการทดสอบกับภาพลายนิ้วมือที่ได้ทำการคัดเลือกมาจากฐานข้อมูล FVC2002 [4] ซึ่งภาพลายนิ้วมือใน FVC2002 [4] จะเก็บในรูปแบบ .tif และภาพลายนิ้วมือที่ได้คัดเลือกมาจากภาพลายนิ้วมือที่ได้บันทึกจากอาสาสมัคร 70 คน ซึ่งเก็บในรูปแบบ .bmp โดยได้ทำการทดสอบกับเครื่องคอมพิวเตอร์ AMD Athlon64 3200+ ที่ความเร็ว 2700 MHz

รูปที่ 5.14 ตัวอย่างภาพลายนิ้วมือจากฐานข้อมูล FVC2002 [4]

รูปที่ 5.15 ภาพลายนิ้วมือที่ผ่านขั้นตอนการเลือกส่วนของภาพที่ใช้ประมวลผล

รูปที่ 5.16 ภาพลายนิ้วมือที่ผ่านการปรับค่าฮีสโตแกรม

รูปที่ 5.17 ภาพลายนิ้วมือที่ผ่านการแปลงภาพเป็นสองระดับ

รูปที่ 5.18 ภาพลายนิ้วมือที่ผ่านการหาทิศทางและปรับแต่งเส้นลายนิ้วมือ

รูปที่ 5.19 ภาพลายนิ้วมือที่ผ่านการทำลายเส้นให้บาง

รูปที่ 5.14 ถึง รูปที่ 5.19 แสดงภาพลายนิ้วมือจากฐานข้อมูล FVC2002 ที่ผ่านขั้นตอนการประมวลผลต่างๆ

รูปที่ 5.20 ตัวอย่างภาพลายนิ้วมือจากอาสาสมัคร จากเครื่องอ่าน U.are.U 2000

รูปที่ 5.21 ภาพลายนิ้วมือที่ผ่านขั้นตอนการเลือกส่วนของภาพที่ใช้ประมวลผล

รูปที่ 5.22 ภาพลายนิ้วมือที่ผ่านการปรับค่าฮีสโตแกรม

รูปที่ 5.23 ภาพลายนิ้วมือที่ผ่านการแปลงภาพเป็นสองระดับ

รูปที่ 5.24 ภาพลายนิ้วมือที่ผ่านการหาทิศทางและปรับแต่งเส้นลายนิ้วมือ

รูปที่ 5.25 ภาพลายนิ้วมือที่ผ่านการทำลายเส้นให้บาง

รูปที่ 5.20 ถึง รูปที่ 5.25 แสดงภาพลายนิ้วมือจากอาสาสมัครที่ทำการบันทึกภาพโดยใช้เครื่องอ่านลายนิ้วมือรุ่น U.are.U 2000 ที่ผ่านขั้นตอนการประมวลผลต่างๆ จากรูปจะพบว่าพื้นที่รับภาพลายนิ้วมือของเครื่องอ่านลายนิ้วมือรุ่น U.are.U 2000 มีขนาดเล็กกว่าขนาดลายนิ้วมืออาสาสมัคร ทำให้ข้อมูลภาพลายนิ้วมือบางส่วนขาดหายไป

รูปที่ 5.26 ตัวอย่างภาพลายนิ้วมือจาก
อาสาสมัคร จากเครื่องอ่าน U.are.U 4000B

รูปที่ 5.27 ภาพลายนิ้วมือที่ผ่านขั้นตอนการ
เลือกส่วนของภาพที่ใช้ประมวลผล

รูปที่ 5.28 ภาพลายนิ้วมือที่ผ่านการปรับค่า
ฮีสโตแกรม

รูปที่ 5.29 ภาพลายนิ้วมือที่ผ่านการแปลงภาพ
เป็นสองระดับ

รูปที่ 5.30 ภาพลายนิ้วมือที่ผ่านการหาทิศทางและปรับแต่งเส้นลายนิ้วมือ

รูปที่ 5.31 ภาพลายนิ้วมือที่ผ่านการทำลายเส้นให้บาง

รูปที่ 5.26 ถึง รูปที่ 5.31 แสดงภาพลายนิ้วมือจากอาสาสมัครที่ทำการบันทึกภาพโดยใช้เครื่องอ่านลายนิ้วมือรุ่น U.are.U 4000B ที่ผ่านขั้นตอนการประมวลผลต่างๆ จากรูปจะพบว่ามีรูปสี่เหลี่ยมสีเทา อยู่กึ่งกลางของภาพลายนิ้วมือ ส่งผลให้เส้นลายนิ้วมือบริเวณดังกล่าวเกิดการประมวลผลผิดพลาดบางส่วน

ในตารางที่ 5.1 แสดงตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากฐานข้อมูลภาพลายนิ้วมือที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือ รุ่น U.are.U 2000 โดยใช้ค่าขีดแบ่งระดับบน1 เท่ากับ 15, ค่าขีดแบ่งระดับล่าง1 เท่ากับ 10, ค่าขีดแบ่งระดับบน2 เท่ากับ 12, ค่าขีดแบ่งระดับล่าง2 เท่ากับ 8 และ ค่าขีดแบ่ง3 เท่ากับ 11

โดยชื่อไฟล์จะประกอบไปด้วย คนลำดับที่__มือ__นิ้ว_จำนวนครั้งที่บันทึกข้อมูลของนิ้วนั้นๆ โดยในส่วนของมือ เลข 1 หมายถึง มือซ้าย และเลข 2 หมายถึง มือขวา, ในส่วนของนิ้วเลข 1 หมายถึง นิ้วก้อย, เลข 2 หมายถึง นิ้วนาง, เลข 3 หมายถึง นิ้วกลาง, เลข 4 หมายถึง นิ้วชี้, เลข 5 หมายถึง นิ้วโป้ง เนื่องจากไม่มีการเก็บภาพลายนิ้วมือของนิ้วก้อยจากอาสาสมัคร ดังนั้นจึงจะไม่มี

กรณีที่หมายเลขนิ้ว = 1 ตัวอย่าง เช่น 16__2_4_3 จะหมายถึง คนลำดับที่ 16, มือขวา, นิ้วชี้, ทำการบันทึกเป็นครั้งที่ 3

ในการทดสอบโปรแกรม การแสดงผลการตรวจสอบของลายนิ้วมือที่มาจากบุคคลเดียวกันแต่มาจากต่างนิ้ว หรือลายนิ้วมือจากบุคคลเดียวกันที่เป็นนิ้วเดียวกันแต่มาจากมือคนละข้างจะถือว่าเป็นลายนิ้วมือที่มาจากต่างบุคคล เนื่องจากลายนิ้วมือจากต่างนิ้วหรือต่างมือกันจะมีจุดสำคัญบนเส้นลายนิ้วมือแตกต่างกันออกไป

ลำดับ	ชื่อไฟล์แม่แบบ	ชื่อไฟล์เปรียบเทียบ	ผลลัพธ์จากโปรแกรม	ความถูกต้องของผลลัพธ์	ได้ผลลัพธ์ในขั้นตอนที่
1	16__2_4_3	16__2_4_2	บุคคลเดียวกัน	ถูกต้อง	1
2	16__2_4_4	16__2_4_2	บุคคลเดียวกัน	ถูกต้อง	1
3	17__2_3_1	16__2_4_2	ต่างบุคคลกัน	ถูกต้อง	1
4	21__2_4_3	21__1_5_12	ต่างบุคคลกัน	ถูกต้อง	3
5	21__2_4_3	21__2_4_2	บุคคลเดียวกัน	ถูกต้อง	2
6	21__2_4_5	17__2_3_3	ต่างบุคคลกัน	ถูกต้อง	1
7	7__1_2_10	21__2_4_5	บุคคลเดียวกัน	ผิดพลาด	2
8	7__1_2_10	21__2_4_6	ต่างบุคคลกัน	ถูกต้อง	3
9	7__2_2_12	16__2_4_5	ต่างบุคคลกัน	ถูกต้อง	1
10	8__1_4_3	19__1_4_2	ต่างบุคคลกัน	ถูกต้อง	1
11	8__1_4_4	16__2_4_5	ต่างบุคคลกัน	ถูกต้อง	1
12	8__1_4_5	8__1_4_4	บุคคลเดียวกัน	ถูกต้อง	1
13	8__1_4_5	8__1_4_1	ต่างบุคคลกัน	ผิดพลาด	1
14	6__2_4_2	21__1_2_8	บุคคลเดียวกัน	ผิดพลาด	3
15	6__2_4_2	19__1_3_3	ต่างบุคคลกัน	ถูกต้อง	1

ลำดับ	ชื่อไฟล์แม่แบบ	ชื่อไฟล์เปรียบเทียบ	ผลลัพธ์จากโปรแกรม	ความถูกต้องของผลลัพธ์	ได้ผลลัพธ์ในขั้นตอนที่
16	6__2_4_2	17__2_3_4	ต่างบุคคลกัน	ถูกต้อง	1
17	7__2_5_10	19__2_4_2	ต่างบุคคลกัน	ถูกต้อง	3
18	7__2_5_10	19__1_4_8	ต่างบุคคลกัน	ถูกต้อง	1
19	7__2_5_10	21__1_5_12	ต่างบุคคลกัน	ถูกต้อง	3
20	7__2_5_10	21__2_4_6	ต่างบุคคลกัน	ถูกต้อง	1
21	7__2_5_10	7__1_2_10	ต่างบุคคลกัน	ถูกต้อง	1
22	16__2_4_4	16__2_4_3	บุคคลเดียวกัน	ถูกต้อง	1
23	17__2_3_3	17__2_3_1	บุคคลเดียวกัน	ถูกต้อง	1
24	17__2_3_3	17__2_3_2	บุคคลเดียวกัน	ถูกต้อง	1
25	17__2_3_4	16__2_4_5	ต่างบุคคลกัน	ถูกต้อง	1
26	17__2_3_4	17__2_3_1	บุคคลเดียวกัน	ถูกต้อง	1
27	18__2_4_5	16__2_4_4	ต่างบุคคลกัน	ถูกต้อง	1
28	18__2_4_5	17__2_3_2	ต่างบุคคลกัน	ถูกต้อง	1
29	18__2_4_5	18__2_4_4	บุคคลเดียวกัน	ถูกต้อง	1
30	18__2_4_6	18__2_4_4	บุคคลเดียวกัน	ถูกต้อง	1

ตารางที่ 5.1 ตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากภาพลายนิ้วมือที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือรุ่น U.are.U 2000

จากผลการทดลองการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากฐานข้อมูลภาพลายนิ้วมือที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือ รุ่น U.are.U 2000 จำนวน 1,236 ครั้ง ได้ค่าความถูกต้องกรณีบุคคลที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือ เท่ากับ 87.2% และค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นต่างบุคคล (อัตราความผิดพลาดที่เกิดจากระบบไม่ยอมรับบุคคลที่เป็น

ผู้เดียวกับที่ได้ลงทะเบียนไว้, FRR: False Rejection Rate) = 12.8%, ค่าความถูกต้องกรณีที่บุคคลที่รับเข้ามาเป็นต่างบุคคลกัน = 87.47%, และค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นต่างบุคคลกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นบุคคลเดียวกัน (อัตราความผิดพลาดที่เกิดจากการยอมรับลายนิ้วมือที่มิใช่บุคคลเดียวกับที่ลงทะเบียนไว้, FAR: False Acceptance Rate) = 12.53%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือเพียงส่วนเดียวในการตรวจสอบแล้วได้ผลลัพธ์ = 61.63%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสองส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 25.58%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสามส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 12.79%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือเพียงส่วนเดียวในการตรวจสอบแล้วได้ผลลัพธ์ = 51.88%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสองส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 20.89%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสามส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 27.23%

ในตารางที่ 5.2 แสดงตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากฐานข้อมูลภาพลายนิ้วมือที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือ รุ่น U.are.U 4000B โดยใช้ค่าขีดแบ่งระดับบน1 เท่ากับ 13, ค่าขีดแบ่งระดับล่าง1 เท่ากับ 8, ค่าขีดแบ่งระดับบน 2 เท่ากับ 12, ค่าขีดแบ่งระดับล่าง2 เท่ากับ 9 และ ค่าขีดแบ่ง3 เท่ากับ 12 โดยรูปแบบของชื่อไฟล์จะเหมือนกับภาพลายนิ้วมือจากเครื่องอ่าน U.are.U 2000 ดังที่ได้อธิบายไว้ก่อนหน้านี้แล้ว

ลำดับ	ชื่อไฟล์แม่แบบ	ชื่อไฟล์เปรียบเทียบ	ผลลัพธ์จากโปรแกรม	ความถูกต้องของผลลัพธ์	ได้ผลลัพธ์ในขั้นตอนที่
1	10__2_5_5	10__2_5_2	บุคคลเดียวกัน	ถูกต้อง	2
2	10__2_5_6	10__2_5_4	บุคคลเดียวกัน	ถูกต้อง	1
3	11__2_5_7	11__2_5_10	บุคคลเดียวกัน	ถูกต้อง	1
4	13__1_5_8	13__1_5_10	บุคคลเดียวกัน	ถูกต้อง	1
5	13__2_5_5	13__2_5_4	บุคคลเดียวกัน	ถูกต้อง	1
6	16__1_4_6	16__1_4_5	บุคคลเดียวกัน	ถูกต้อง	2
7	17__2_5_5	17__2_5_4	บุคคลเดียวกัน	ถูกต้อง	1
8	18__1_4_4	18__1_4_2	บุคคลเดียวกัน	ถูกต้อง	1
9	19__2_4_13	19__2_4_11	บุคคลเดียวกัน	ถูกต้อง	3
10	1__1_2_12	1__1_2_11	บุคคลเดียวกัน	ถูกต้อง	1
11	1__1_3_4	1__1_3_2	บุคคลเดียวกัน	ถูกต้อง	1
12	1__1_4_5	1__1_2_11	บุคคลเดียวกัน	ผิดพลาด	1
13	1__1_4_5	1__1_4_2	บุคคลเดียวกัน	ถูกต้อง	1
14	1__1_5_10	10_2_5_2	บุคคลเดียวกัน	ผิดพลาด	1
15	1__1_5_10	13_1_5_10	ต่างบุคคลกัน	ถูกต้อง	3
16	1__2_2_10	19__2_4_9	ต่างบุคคลกัน	ถูกต้อง	2
17	1__2_2_5	16__1_5_8	ต่างบุคคลกัน	ถูกต้อง	2
18	1__2_2_5	1__2_2_10	บุคคลเดียวกัน	ถูกต้อง	1
19	1__2_2_8	10__2_5_5	ต่างบุคคลกัน	ถูกต้อง	3
20	1__2_2_8	11__2_5_10	บุคคลเดียวกัน	ผิดพลาด	2
21	2__2_3_3	1__1_5_8	ต่างบุคคลกัน	ถูกต้อง	3
22	2__2_3_3	2__2_3_2	บุคคลเดียวกัน	ถูกต้อง	1

ลำดับ	ชื่อไฟล์แม่แบบ	ชื่อไฟล์เปรียบเทียบ	ผลลัพธ์จากโปรแกรม	ความถูกต้องของผลลัพธ์	ได้ผลลัพธ์ในขั้นตอนที่
23	2__2_3_4	18__1_4_3	ต่างบุคคลกัน	ถูกต้อง	3
24	2__2_3_4	1__1_2_12	บุคคลเดียวกัน	ผิดพลาด	3
25	2__2_3_4	1__2_2_5	บุคคลเดียวกัน	ผิดพลาด	2
26	4__2_5_2	1__1_2_8	บุคคลเดียวกัน	ผิดพลาด	1
27	7__1_3_13	4__2_5_3	ต่างบุคคลกัน	ถูกต้อง	3
28	7__2_3_2	16__1_5_12	ต่างบุคคลกัน	ถูกต้อง	3
29	7__2_3_6	7__2_3_2	บุคคลเดียวกัน	ถูกต้อง	1
30	7__2_3_6	7__2_3_4	บุคคลเดียวกัน	ถูกต้อง	1

ตารางที่ 5.2 ตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากภาพลายนิ้วมือที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือรุ่น U.are.U 4000B

จากผลการทดลองการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากฐานข้อมูลภาพลายนิ้วมือที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือ รุ่น U.are.U 4000B จำนวน 4,395 ครั้ง ได้ค่าความถูกต้องกรณีบุคคลที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือ เท่ากับ 98.06% และค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นต่างบุคคล (อัตราความผิดพลาดที่เกิดจากระบบไม่ยอมรับบุคคลที่เป็นผู้เดียวกับที่ได้ลงทะเบียนไว้, FRR: False Rejection Rate) = 1.94%, ค่าความถูกต้องกรณีที่บุคคลที่รับเข้ามาเป็นต่างบุคคลกัน = 62.5% และค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นต่างบุคคลกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นบุคคลเดียวกัน (อัตราความผิดพลาดที่เกิดจากการยอมรับลายนิ้วมือที่มิใช่บุคคลเดียวกับที่ลงทะเบียนไว้, FAR: False Acceptance Rate) = 37.5%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือเพียงส่วนเดียวในการตรวจสอบแล้วได้ผลลัพธ์ = 85.81%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสองส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 11.61%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสามส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 2.58%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือเพียงส่วนเดียวในการตรวจสอบแล้วได้ผลลัพธ์ = 28.94%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสองส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 40.64%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสามส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 30.42%

ในตารางที่ 5.3 แสดงตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากฐานข้อมูล FVC2002 DB1 [4] โดยใช้ค่าขีดแบ่งระดับบน1 เท่ากับ 12, ค่าขีดแบ่งระดับล่าง1 เท่ากับ 9, ค่าขีดแบ่งระดับบน2 เท่ากับ 13, ค่าขีดแบ่งระดับล่าง2 เท่ากับ 10 และค่าขีดแบ่ง3 เท่ากับ 11

โดยชื่อไฟล์จะประกอบไปด้วย ลำดับที่_จำนวนครั้งที่บันทึกข้อมูลของนิ้วเดียวกัน

ลำดับ	ชื่อไฟล์แม่แบบ	ชื่อไฟล์เปรียบเทียบ	ผลลัพธ์จากโปรแกรม	ความถูกต้องของผลลัพธ์	ได้ผลลัพธ์ในขั้นตอนที่
1	101_2	101_1	บุคคลเดียวกัน	ถูกต้อง	1
2	104_2	101_4	ต่างบุคคลกัน	ถูกต้อง	1
3	104_2	101_5	ต่างบุคคลกัน	ถูกต้อง	1
4	104_3	101_1	ต่างบุคคลกัน	ถูกต้อง	1
5	104_4	104_1	บุคคลเดียวกัน	ถูกต้อง	1
6	104_3	101_3	ต่างบุคคลกัน	ถูกต้อง	1

ลำดับ	ชื่อไฟล์แม่แบบ	ชื่อไฟล์เปรียบเทียบ	ผลลัพธ์จากโปรแกรม	ความถูกต้องของผลลัพธ์	ได้ผลลัพธ์ในขั้นตอนที่
7	104_2	103_6	บุคคลเดียวกัน	ผิดพลาด	1
8	104_3	102_2	ต่างบุคคลกัน	ถูกต้อง	2
9	104_3	102_3	ต่างบุคคลกัน	ถูกต้อง	3
10	104_4	104_2	บุคคลเดียวกัน	ถูกต้อง	1
11	104_5	101_1	ต่างบุคคลกัน	ถูกต้อง	1
12	104_5	102_4	บุคคลเดียวกัน	ผิดพลาด	1
13	104_2	104_1	ต่างบุคคลกัน	ผิดพลาด	2
14	104_5	104_3	บุคคลเดียวกัน	ถูกต้อง	3
15	104_5	103_2	ต่างบุคคลกัน	ถูกต้อง	1
16	104_6	101_1	ต่างบุคคลกัน	ถูกต้อง	1
17	104_6	101_3	ต่างบุคคลกัน	ถูกต้อง	1
18	104_6	102_3	บุคคลเดียวกัน	ผิดพลาด	1
19	104_6	103_4	ต่างบุคคลกัน	ถูกต้อง	1
20	104_7	101_7	ต่างบุคคลกัน	ถูกต้อง	1
21	104_7	101_2	ต่างบุคคลกัน	ถูกต้อง	1
22	104_6	104_4	บุคคลเดียวกัน	ถูกต้อง	1
23	105_3	105_1	บุคคลเดียวกัน	ถูกต้อง	1
24	105_3	105_2	บุคคลเดียวกัน	ถูกต้อง	1
25	104_7	103_4	ต่างบุคคลกัน	ถูกต้อง	1
26	105_3	102_4	ต่างบุคคลกัน	ถูกต้อง	1
27	104_7	103_5	ต่างบุคคลกัน	ถูกต้อง	3
28	104_8	101_4	ต่างบุคคลกัน	ถูกต้อง	3

ลำดับ	ชื่อไฟล์แม่แบบ	ชื่อไฟล์เปรียบเทียบ	ผลลัพธ์จากโปรแกรม	ความถูกต้องของผลลัพธ์	ได้ผลลัพธ์ในขั้นตอนที่
29	104_8	104_4	บุคคลเดียวกัน	ถูกต้อง	1
30	105_1	103_5	ต่างบุคคลกัน	ถูกต้อง	3

ตารางที่ 5.3 ตัวอย่างผลการทดลองบางส่วนของการเปรียบเทียบภาพลายนิ้วมือที่ได้รับการคัดเลือกจากฐานข้อมูล FVC2002 DB1 [4]

จากผลการทดลองกับภาพลายนิ้วมือที่ได้รับการคัดเลือกจากฐานข้อมูล FVC2002 DB1 [4] จำนวน 1,743 ครั้ง ได้ค่าความถูกต้องกรณีบุคคลที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือ เท่ากับ 83.54% และค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วแต่ระบบให้ผลลัพธ์เป็นต่างบุคคล (อัตราความผิดพลาดที่เกิดจากระบบไม่ยอมรับบุคคลที่เป็นผู้เดียวกับที่ได้ลงทะเบียนไว้, FRR: False Rejection Rate) = 16.46%, ค่าความถูกต้องกรณีที่บุคคลที่รับเข้ามาเป็นต่างบุคคลกัน = 71.07%, และค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นต่างบุคคลกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นบุคคลเดียวกัน (อัตราความผิดพลาดที่เกิดจากการยอมรับลายนิ้วมือที่มิใช่บุคคลเดียวกับที่ลงทะเบียนไว้, FAR: False Acceptance Rate) = 28.93%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือเพียงส่วนเดียวในการตรวจสอบแล้วได้ผลลัพธ์ = 79.42%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสองส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 14.81%

จำนวนเปอร์เซ็นต์กรณีบุคคลเดียวกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสามส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 5.77%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือเพียงส่วนเดียวในการตรวจสอบแล้วได้ผลลัพธ์ = 72.07%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสองส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 16.07%

จำนวนเปอร์เซ็นต์กรณีต่างบุคคลกันใช้ชิ้นส่วนข้อมูลลายนิ้วมือสามส่วนในการตรวจสอบแล้วได้ผลลัพธ์ = 11.86%

ในตารางที่ 5.4 แสดงตัวอย่างผลการทดลองบางส่วนของการทดลองเปลี่ยนค่าขีดแบ่งทั้ง 5 ค่าเป็นค่าต่างๆ (โดยค่าขีดแบ่งระดับบน1 แทนด้วยตัวอักษร “UT1” ทำการเปลี่ยนค่าในช่วงระหว่าง 10 ถึง 15, ค่าขีดแบ่งระดับล่าง1 แทนด้วยตัวอักษร “LT1” ทำการเปลี่ยนค่าในช่วงระหว่าง 5 ถึง 10, ค่าขีดแบ่งระดับบน2 แทนด้วยตัวอักษร “UT2” ทำการเปลี่ยนค่าในช่วงระหว่าง 9 ถึง 14, ค่าขีดแบ่งระดับล่าง2 แทนด้วยตัวอักษร “LT2” ทำการเปลี่ยนค่าในช่วงระหว่าง 4 ถึง 9, ค่าขีดแบ่ง3 แทนด้วยตัวอักษร “T3” ทำการเปลี่ยนค่าในช่วงระหว่าง 7 ถึง 12) เพื่อสังเกตถึงผลกระทบต่อผลลัพธ์ต่างๆ ซึ่งได้แก่ ค่าความถูกต้องกรณีบุคคลที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือแทนด้วยตัวอักษร “%CS”, ค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นต่างบุคคล (อัตราความผิดพลาดที่เกิดจากระบบไม่ยอมรับบุคคลที่เป็นผู้เดียวกับที่ได้ลงทะเบียนไว้, FRR: False Rejection Rate) แทนด้วยตัวอักษร “%ES”, ค่าความถูกต้องกรณีที่บุคคลที่รับเข้ามาเป็นต่างบุคคลกัน แทนด้วยตัวอักษร”%CD”, ค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นต่างบุคคลกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นบุคคลเดียวกัน (อัตราความผิดพลาดที่เกิดจากการยอมรับลายนิ้วมือที่มิใช่บุคคลเดียวกับที่ลงทะเบียนไว้, FAR: False Acceptance Rate) แทนด้วยตัวอักษร “%ED”, จำนวนเปอร์เซ็นต์รวมกรณีใช้ชิ้นส่วนข้อมูลลายนิ้วมือเพียงส่วนเดียวในการตรวจสอบแล้วได้ผลลัพธ์ แทนด้วยตัวอักษร “%P1”, จำนวนเปอร์เซ็นต์รวมกรณีใช้ชิ้นส่วนข้อมูลลายนิ้วมือสองส่วนในการตรวจสอบแล้วได้ผลลัพธ์ แทนด้วยตัวอักษร “%P2”, จำนวนเปอร์เซ็นต์รวมกรณีใช้ชิ้นส่วนข้อมูลลายนิ้วมือสามส่วนในการตรวจสอบแล้วได้ผลลัพธ์ แทนด้วยตัวอักษร “%P3”

เนื่องจากจำนวนครั้งในการทดสอบการเปลี่ยนค่าขีดแบ่งทั้ง 5 ค่า เป็นค่าต่างๆ มีจำนวนมาก ซึ่งใช้เวลาในการประมวลผลนาน เพื่อที่จะลดเวลาในการคำนวณหาผลการทดลองลง จึงได้ทำการลดจำนวนภาพลายนิ้วมือที่ใช้ในการทดสอบการเปลี่ยนค่าขีดแบ่งทั้ง 5 ค่า เป็นค่าต่างๆ ลง

UT1	LT1	UT2	LT2	T3	%CS	%ES	%CD	%ED	%P1	%P2	%P3
10	5	9	4	7	100	0	0.778458	99.22154	78.4157	14.47432	7.10998
10	5	9	5	9	98.33334	1.666667	5.130168	94.86984	78.4157	14.47432	7.10998
10	5	11	5	8	98.80953	1.190476	6.776416	93.22359	78.4157	1.417151	20.16715
10	5	13	4	12	90	10	22.03931	77.96069	78.4157	0.036337	21.54797
10	5	14	6	11	90.47619	9.523809	21.6437	78.3563	78.4157	0.036337	21.54797

UT1	LT1	UT2	LT2	T3	%CS	%ES	%CD	%ED	%P1	%P2	%P3
10	6	9	4	7	100	0	0.778458	99.22154	78.4157	14.47432	7.10998
10	6	9	4	11	97.14286	2.857143	7.274119	92.72588	78.4157	14.47432	7.10998
10	6	10	9	7	92.85714	7.142858	16.3221	83.6779	78.4157	21.5843	0
10	6	12	4	11	90.71429	9.285714	21.43951	78.56049	78.4157	0.242248	21.34205
10	6	13	4	8	98.57143	1.428572	7.172027	92.82797	78.4157	0.036337	21.54797
10	6	14	4	7	100	0	2.348137	97.65186	78.4157	0.012112	21.57219
10	7	9	4	8	99.28571	0.714286	2.577846	97.42215	78.7064	14.37742	6.916183
10	7	10	4	10	94.04762	5.952381	15.02042	84.97958	78.7064	5.704942	15.58866
10	7	11	4	11	91.19048	8.809524	20.34201	79.65799	78.7064	1.405039	19.88857
10	7	12	4	9	95	5	14.38234	85.61766	78.7064	0.242248	21.05136
10	7	12	4	12	90	10	21.82236	78.17764	78.7064	0.242248	21.05136
10	7	13	4	10	92.61905	7.380953	19.88259	80.1174	78.7064	0.036337	21.25727
10	7	14	4	11	90.47619	9.523809	21.6437	78.3563	78.7064	0.012112	21.28149
10	8	9	4	7	97.85714	2.142857	5.895865	94.10413	83.70882	11.66425	4.626938
10	8	10	4	10	93.57143	6.428572	16.01583	83.98418	83.70882	4.978198	11.31298
10	8	12	4	10	92.38095	7.619048	20.09954	79.90046	83.70882	0.230136	16.06105
10	8	13	4	8	96.66666	3.333334	10.68147	89.31854	83.70882	0.036337	16.25485
10	8	14	8	12	89.76191	10.2381	22.06483	77.93517	83.70882	4.639051	11.65213
11	5	10	5	8	98.33334	1.666667	8.052578	91.94743	56.22578	18.20494	25.56928
11	5	10	5	11	88.33334	11.66667	25.48494	74.51506	56.22578	18.20494	25.56928
11	5	10	6	7	100	0	2.641654	97.35835	56.22578	18.22917	25.54506
11	5	10	8	12	88.33334	11.66667	26.21235	73.78765	56.22578	28.04021	15.73401
11	5	11	4	12	81.90476	18.09524	38.50179	61.49822	56.22578	6.031977	37.74225
11	5	12	9	12	79.52381	20.47619	43.05768	56.94232	56.22578	27.18023	16.59399
11	5	13	4	12	78.57143	21.42857	44.15518	55.84482	56.22578	0.290698	43.48353
11	5	13	4	8	97.61904	2.380952	11.43441	88.5656	56.22578	0.290698	43.48353
11	5	14	7	11	79.7619	20.2381	42.24094	57.75906	56.22578	1.187016	42.58721
11	5	14	9	12	77.61905	22.38095	44.38489	55.61511	56.22578	25.6783	18.09593
11	6	10	8	12	88.33334	11.66667	26.21235	73.78765	56.22578	28.04021	15.73401

UT1	LT1	UT2	LT2	T3	%CS	%ES	%CD	%ED	%P1	%P2	%P3
11	6	14	7	11	79.7619	20.2381	42.24094	57.75906	56.22578	1.187016	42.58721
11	7	11	5	12	81.90476	18.09524	38.51455	61.48545	56.51648	6.019864	37.46366
11	8	9	5	9	96.66666	3.333334	10.04339	89.95661	61.51889	31.12888	7.352229
12	5	13	5	11	70.95238	29.04762	57.03165	42.96835	36.95494	1.114341	61.93072
12	5	13	5	12	66.66667	33.33334	61.79173	38.20827	36.95494	1.114341	61.93072
12	5	13	8	11	70.95238	29.04762	57.44002	42.55998	36.95494	12.0155	51.02956
12	5	14	6	12	65.71429	34.28572	62.40429	37.59572	36.95494	0.363372	62.68169
12	7	11	8	11	77.85714	22.14286	46.36294	53.63706	37.24564	25.76308	36.99128
12	7	13	6	12	66.66667	33.33334	61.79173	38.20827	37.24564	1.126454	61.62791
13	9	11	4	7	89.04762	10.95238	23.86422	76.13579	44.33139	23.49806	32.17054
13	10	12	8	12	60.95239	39.04762	67.99387	32.00613	66.52132	10.30765	23.17103
14	5	12	4	11	69.7619	30.23809	62.21287	37.78714	14.08673	15.90358	70.00969
14	6	10	8	10	88.80953	11.19048	28.39459	71.60541	14.08673	65.55232	20.36095
14	6	12	4	12	63.80953	36.19048	68.58091	31.41909	14.08673	15.90358	70.00969
14	7	10	8	7	95.71428	4.285715	13.74426	86.25574	14.37742	65.33431	20.28828
14	7	12	5	10	79.04762	20.95238	49.74477	50.25523	14.37742	15.90358	69.71899

ตารางที่ 5.4 ตัวอย่างผลการทดลองบางส่วนของการทดลองเปลี่ยนค่าขีดแบ่งทั้ง 5 ค่าเป็นค่าต่างๆ

บทที่ 6
สรุปผลการวิจัยและข้อเสนอแนะ

6.1 สรุปผลการวิจัย

วิทยานิพนธ์นี้นำเสนอถึงการใช้เทคนิคการแบ่งภาพลายนิ้วมือที่ต้องการตรวจสอบออกเป็น 3 ส่วนย่อยๆ เพื่อแยกการเปรียบเทียบลายนิ้วมือเป็น 3 ลำดับ โดยวิธีที่ได้นำเสนอในงานวิทยานิพนธ์นี้ ได้ช่วยให้สามารถประมวลผลได้กับสมาร์ตคาร์ดที่มีหน่วยความจำชั่วคราวขนาดเล็กกว่าข้อมูลภาพลายนิ้วมือทั้งหมด จากเดิมที่อัลกอริทึมทั่วไปไม่สามารถประมวลผลได้ เนื่องจากวิธีการใหม่ที่นำเสนอในงานวิทยานิพนธ์นี้จะลดจำนวนพื้นที่หน่วยความชั่วคราวที่ใช้ในการประมวลผลลง เพราะขนาดของข้อมูลที่ใช้ในการประมวลผลในแต่ละครั้งลดลง และการใช้เทคนิคการแบ่งค่าขีดแบ่ง ออกเป็นค่าขีดแบ่งระดับบน และค่าขีดแบ่งระดับล่าง จะช่วยลดเวลาที่ใช้ในการประมวลผลลงได้ ซึ่งค่าขีดแบ่งระดับบน จะช่วยลดเวลาในกรณีของภาพลายนิ้วมือที่รับเข้ามาตรวจสอบเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือ โดยมีคุณภาพสูงและไม่มีการเปลี่ยนตำแหน่งของภาพลายนิ้วมือ หรือมีการเปลี่ยนแปลงเพียงเล็กน้อย และไม่มีสัญญาณรบกวน ส่วนค่าขีดแบ่งระดับล่าง จะช่วยลดเวลาในกรณีของภาพลายนิ้วมือที่รับเข้ามาตรวจสอบเป็นต่างบุคคลกับแม่แบบลายนิ้วมือ โดยมีตำแหน่งและชนิดของจุดสำคัญบนเส้นลายนิ้วมือที่แตกต่างกันระหว่างภาพลายนิ้วมือที่รับเข้ามากับแม่แบบลายนิ้วมือ

จากการทดลองทำการเปลี่ยนค่าขีดแบ่งระดับบน1, ค่าขีดแบ่งระดับล่าง1, ค่าขีดแบ่งระดับบน2, ค่าขีดแบ่งระดับล่าง2 และค่าขีดแบ่ง3 พบว่า ระดับค่าที่เหมาะสำหรับการนำไปใช้งานทั่วไป โดยพิจารณาจากระดับค่าขีดแบ่งที่ทำให้ค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือ แต่ระบบให้ผลลัพธ์เป็นต่างบุคคล (อัตราความผิดพลาดที่เกิดจากระบบไม่ยอมรับบุคคลที่เป็นผู้เดียวกับที่ได้ลงทะเบียนไว้, FRR: False Rejection Rate) ใกล้เคียงกับค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นต่างบุคคลกับแม่แบบลายนิ้วมือ แต่ระบบให้ผลลัพธ์เป็นบุคคลเดียวกัน (อัตราความผิดพลาดที่เกิดจากการยอมรับลายนิ้วมือที่มิใช่บุคคลเดียวกับที่ลงทะเบียนไว้, FAR: False Acceptance Rate) จนเกือบจะถือได้ว่าเท่ากัน (EER: Equal Error Rate) โดยมีอัตราความผิดพลาดในระดับต่ำและมีอัตราการใช้ชิ้นส่วนข้อมูลลายนิ้วมือเพียงส่วนเดียวในการตรวจสอบแล้วได้ผลลัพธ์สูงสุด คือ ค่าขีดแบ่ง

ระดับบน1 = 13, ค่าขีดแบ่งระดับล่าง1 = 7, ค่าขีดแบ่งระดับบน2 = 12, ค่าขีดแบ่งระดับล่าง2 = 8 และค่าขีดแบ่งระดับ3 = 12 ระดับค่าที่เหมาะสมสำหรับงานที่ต้องการความปลอดภัยสูง (ค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นต่างบุคคลกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นบุคคลเดียวกันมีค่าต่ำที่สุด โดยไม่คำนึงถึงค่าความผิดพลาดกรณีที่ภาพลายนิ้วมือที่รับเข้ามาเป็นบุคคลเดียวกับแม่แบบลายนิ้วมือแต่ระบบให้ผลลัพธ์เป็นต่างบุคคล) ได้ค่าขีดแบ่งระดับบน1 = 15, ค่าขีดแบ่งระดับล่าง1 = 10, ค่าขีดแบ่งระดับบน2 = 14, ค่าขีดแบ่งระดับล่าง2 = 9 และค่าขีดแบ่ง3 = 12

นอกจากนี้การนำวิธีเพิ่มความถี่สัญญาณนาฬิกาที่จ่ายให้กับสมาร์ตคาร์ด มาใช้งานโดยเพิ่มจาก 3.57 MHz เป็น 20 MHz ทำให้สมาร์ตคาร์ดสามารถประมวลผลได้รวดเร็วขึ้นกว่า 460% ส่งผลให้สมาร์ตคาร์ดสามารถประมวลผลงานที่ซับซ้อน โดยใช้เวลาในการประมวลผลลดลงได้

6.2 ข้อเสนอแนะ

1. การพัฒนาระบบตรวจสอบลายนิ้วมือให้ได้ผลลัพธ์ที่ถูกต้องมากยิ่งขึ้นนั้นสามารถทำได้ ดังนี้

   1.1 เปลี่ยนเครื่องอ่านลายนิ้วมือเป็นแบบที่มีความละเอียดสูงขึ้น, มีขนาดของหน้าสัมผัสเพียงพอกับขนาดของลายนิ้วมือของบุคคลส่วนใหญ่ และไม่มีสัญญาณรบกวนในภาพ

   1.2 พัฒนาอัลกอริทึมในการหาจุดอ้างอิง (Core) ของภาพลายนิ้วมือ ที่สามารถทำงานได้อย่างถูกต้องในกรณีที่ภาพที่รับเข้ามามีคุณภาพต่ำหรือมีสัญญาณรบกวนในพื้นที่จุดอ้างอิง เพื่อใช้ในการปรับตำแหน่งภาพลายนิ้วมือที่ต้องการตรวจสอบให้ตรงกับที่ลงทะเบียนไว้ (ในกรณีที่ภาพลายนิ้วมือที่รับเข้ามามีการเปลี่ยนมุมหรือตำแหน่ง)

   1.3 ปรับปรุงส่วนการประมวลผลภาพเบื้องต้นให้สามารถกำจัดสัญญาณรบกวนของภาพที่เกิดจากเครื่องอ่านลายนิ้วมือหรือฝุ่นได้ และทำการปรับปรุงขั้นตอนการต่อเส้นลายนิ้วมือ ให้มีความถูกต้องมากขึ้น เพื่อลดจำนวนจุดสำคัญบนเส้นลายนิ้วมือปลอม

2. สามารถนำวิธีการที่ได้นำเสนอในวิทยานิพนธ์ฉบับนี้ไปพัฒนาต่อเพื่อประยุกต์ใช้งานกับอุปกรณ์ชนิดอื่นๆ ได้ เช่น โทรศัพท์มือถือ, PDA เป็นต้น

รายการอ้างอิง

1. Smart Cards and Biometrics in Privacy-Sensitive Secure Identification Systems [Computer file]. : Smart Card Alliance, 2002. Available from : http://www.smartcardalliance.org/ [2004, Jan 28]

2. Y. Moon, H. Ho, K. Ng, S. Wan, and S. Wong. Collaborative Fingerprint Authentication by Smart Card and a Trusted Host. Electrical and Computer Engineering, 1 (2000): 108-112.

3. ISO/IEC 7816 [Online]. Available from : http://www.iso.ch

4. D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain. FVC2002: Second Fingerprint Verification Competition. in Proceedings 16th International Conference on Pattern Recognition (ICPR2002), 3 (August 2002): 811-814.

5. เอกรัตน์ จุลวรรณ์. การประเมินผลของขั้นตอนวิธีการทำลายเส้นให้บางเพื่อนำไปใช้กับภาพพิมพ์ลายนิ้วมือ. วิทยานิพนธ์ปริญญามหาบัณฑิต วิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2541.

6. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. Handbook of fingerprint recognition. New York: Springer, 2003.

7. บัตรประชาชน “สมาร์ทการ์ด” เปลี่ยนวิถีชีวิตคนไทยสู่ไฮเทค [Online] : Available from : http://www.banprucity.go.th/smartcard.html/ [2006, Feb 20]

8. Hironori Yahagi, Seigo Igaki, and Fumio Yamagishi. Moving-Window Algorithm For Fast Fingerprint Verification. IEEE Proceedings-1990 Southeastcon (1990): 343-348

9. Bir Bhanu, Michael Boshra, and Xuejun Tan. Logical templates for feature extraction in fingerprint images. Pattern Recognition (2000): 846-850.

10. อุกฤษฎ์ ศรีเสือขาม. การประมวลลายพิมพ์นิ้วมือเบื้องต้นสำหรับระบบตรวจพิสูจน์ลายนิ้วมืออัตโนมัติ. วิทยานิพนธ์ปริญญามหาบัณฑิต วิทยาการคอมพิวเตอร์และเทคโนโลยี-สารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร-ลาดกระบัง, 2541.

11. Byung-Gyu Kim, and Dong-jo Park. Adaptive image normalisation based on block processing for enhancement of fingerprint image. Electron. Lett Vol. 38 No. 14 (2002): 696-698.

12. Lin Hong, Yifei Wan and Anil Jain. Fingerprint Image Enhancement: Algorithm and Performance Evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20, 8 (August 1998): 777-789.

13. Anil K. Jain. Fundamentals of digital image processing. Prentice Hall, 1997.

14. A. Wahab, S.H. Chin, and E.C. Tan. Novel Approach to automated fingerprint recognition. IEE Proc.-Visual Image Signal Process, 145, 3 (June 1998): 160-166.

ภาคผนวก

ภาคผนวก ก

ตัวอย่างภาพลายนิ้วมือบางส่วนที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือ U.are.U 4000B

ขนาดภาพลายนิ้วมือที่แสดงด้านล่างเป็น 21% ของขนาดภาพจริง

 คนที่ 1, มือซ้าย, นิ้วนาง, ครั้งที่ 8	 คนที่ 1, มือซ้าย, นิ้วนาง, ครั้งที่ 9	 คนที่ 1, มือซ้าย, นิ้วนาง, ครั้งที่ 11	 คนที่ 1, มือซ้าย, นิ้วนาง, ครั้งที่ 12	 คนที่ 1, มือซ้าย, นิ้วกลาง, ครั้งที่ 4
 คนที่ 1, มือซ้าย, นิ้วกลาง, ครั้งที่ 10	 คนที่ 1, มือซ้าย, นิ้วกลาง,ครั้งที่ 11	 คนที่ 1, มือซ้าย, นิ้วกลาง, ครั้งที่ 12	 คนที่ 1, มือซ้าย, นิ้วชี้, ครั้งที่ 5	 คนที่ 1, มือซ้าย, นิ้วชี้, ครั้งที่ 6
 คนที่ 1, มือซ้าย, นิ้วชี้, ครั้งที่ 8	 คนที่ 1, มือซ้าย, นิ้วชี้, ครั้งที่ 11	 คนที่ 1, มือซ้าย, นิ้วโป้ง, ครั้งที่ 3	 คนที่ 1, มือซ้าย, นิ้วโป้ง, ครั้งที่ 7	 คนที่ 1, มือซ้าย, นิ้วโป้ง, ครั้งที่ 10
 คนที่ 1, มือซ้าย, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 1, มือขวา, นิ้วนาง, ครั้งที่ 4	 คนที่ 1, มือขวา, นิ้วนาง, ครั้งที่ 5	 คนที่ 1, มือขวา, นิ้วนาง, ครั้งที่ 7	 คนที่ 1, มือขวา, นิ้วนาง, ครั้งที่ 9

 คนที่ 1, มือขวา, นิ้วกลาง, ครั้งที่ 3	 คนที่ 1, มือขวา, นิ้วกลาง, ครั้งที่ 4	 คนที่ 1, มือขวา, นิ้วกลาง, ครั้งที่ 7	 คนที่ 1, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 1, มือขวา, นิ้วชี้, ครั้งที่ 6
 คนที่ 1, มือขวา, นิ้วชี้, ครั้งที่ 7	 คนที่ 1, มือขวา, นิ้วชี้, ครั้งที่ 9	 คนที่ 1, มือขวา, นิ้วชี้, ครั้งที่ 11	 คนที่ 1, มือขวา, นิ้วโป้ง, ครั้งที่ 3	 คนที่ 1, มือขวา, นิ้วโป้ง, ครั้งที่ 5
 คนที่ 1, มือขวา, นิ้วโป้ง, ครั้งที่ 9	 คนที่ 1, มือขวา, นิ้วโป้ง, ครั้งที่ 10	 คนที่ 2, มือซ้าย, นิ้วนาง, ครั้งที่ 5	 คนที่ 2, มือซ้าย, นิ้วนาง, ครั้งที่ 7	 คนที่ 2, มือซ้าย, นิ้วนาง, ครั้งที่ 9
 คนที่ 2, มือซ้าย, นิ้วนาง, ครั้งที่ 12	 คนที่ 2, มือซ้าย, นิ้วกลาง, ครั้งที่ 2	 คนที่ 2, มือซ้าย, นิ้วกลาง, ครั้งที่ 5	 คนที่ 2, มือซ้าย, นิ้วกลาง, ครั้งที่ 11	 คนที่ 2, มือซ้าย, นิ้วกลาง, ครั้งที่ 12
 คนที่ 2, มือซ้าย, นิ้วชี้, ครั้งที่ 6	 คนที่ 2, มือซ้าย, นิ้วชี้, ครั้งที่ 10	 คนที่ 2, มือซ้าย, นิ้วชี้, ครั้งที่ 11	 คนที่ 2, มือซ้าย, นิ้วชี้, ครั้งที่ 12	 คนที่ 2, มือซ้าย, นิ้วโป้ง, ครั้งที่ 1

 คนที่ 2, มือซ้าย, นิ้วโป้ง, ครั้งที่ 2	 คนที่ 2, มือซ้าย, นิ้วโป้ง, ครั้งที่ 4	 คนที่ 2, มือซ้าย, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 2, มือขวา, นิ้วนาง, ครั้งที่ 6	 คนที่ 2, มือขวา, นิ้วนาง, ครั้งที่ 7
 คนที่ 2, มือขวา, นิ้วนาง, ครั้งที่ 9	 คนที่ 2, มือขวา, นิ้วนาง, ครั้งที่ 12	 คนที่ 2, มือขวา, นิ้วกลาง, ครั้งที่ 9	 คนที่ 2, มือขวา, นิ้วกลาง, ครั้งที่ 10	 คนที่ 2, มือขวา, นิ้วกลาง, ครั้งที่ 11
 คนที่ 2, มือขวา, นิ้วกลาง, ครั้งที่ 12	 คนที่ 2, มือขวา, นิ้วชี้, ครั้งที่ 6	 คนที่ 2, มือขวา, นิ้วชี้, ครั้งที่ 8	 คนที่ 2, มือขวา, นิ้วชี้, ครั้งที่ 10	 คนที่ 2, มือขวา, นิ้วชี้, ครั้งที่ 12
 คนที่ 2, มือขวา, นิ้วโป้ง, ครั้งที่ 7	 คนที่ 2, มือขวา, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 2, มือขวา, นิ้วโป้ง, ครั้งที่ 10	 คนที่ 2, มือขวา, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 3, มือซ้าย, นิ้วนาง, ครั้งที่ 2
 คนที่ 3, มือซ้าย, นิ้วนาง, ครั้งที่ 6	 คนที่ 3, มือซ้าย, นิ้วนาง, ครั้งที่ 8	 คนที่ 3, มือซ้าย, นิ้วนาง, ครั้งที่ 9	 คนที่ 3, มือซ้าย, นิ้วชี้, ครั้งที่ 6	 คนที่ 3, มือซ้าย, นิ้วชี้, ครั้งที่ 9

 คนที่ 3, มือซ้าย, นิ้วชี้, ครั้งที่ 11	 คนที่ 3, มือซ้าย, นิ้วชี้, ครั้งที่ 12	 คนที่ 3, มือซ้าย, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 3, มือซ้าย, นิ้วโป้ง, ครั้งที่ 10	 คนที่ 3, มือซ้าย, นิ้วโป้ง, ครั้งที่ 11
 คนที่ 3, มือซ้าย, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 3, มือขวา, นิ้วนาง, ครั้งที่ 2	 คนที่ 3, มือขวา, นิ้วนาง, ครั้งที่ 5	 คนที่ 3, มือขวา, นิ้วนาง, ครั้งที่ 7	 คนที่ 3, มือขวา, นิ้วนาง, ครั้งที่ 10
 คนที่ 3, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 3, มือขวา, นิ้วกลาง, ครั้งที่ 9	 คนที่ 3, มือขวา, นิ้วกลาง, ครั้งที่ 11	 คนที่ 3, มือขวา, นิ้วกลาง, ครั้งที่ 12	 คนที่ 3, มือขวา, นิ้วชี้, ครั้งที่ 7
 คนที่ 3, มือขวา, นิ้วชี้, ครั้งที่ 9	 คนที่ 3, มือขวา, นิ้วชี้, ครั้งที่ 10	 คนที่ 3, มือขวา, นิ้วชี้, ครั้งที่ 11	 คนที่ 3, มือขวา, นิ้วโป้ง, ครั้งที่ 2	 คนที่ 3, มือขวา, นิ้วโป้ง, ครั้งที่ 3
 คนที่ 3, มือขวา, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 3, มือขวา, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 4, มือซ้าย, นิ้วนาง, ครั้งที่ 3	 คนที่ 4, มือซ้าย, นิ้วนาง, ครั้งที่ 8	 คนที่ 4, มือซ้าย, นิ้วนาง, ครั้งที่ 9

 คนที่ 4, มือซ้าย, นิ้วนาง, ครั้งที่ 11	 คนที่ 4, มือซ้าย, นิ้วกลาง, ครั้งที่ 4	 คนที่ 4, มือซ้าย, นิ้วกลาง, ครั้งที่ 7	 คนที่ 4, มือซ้าย, นิ้วกลาง, ครั้งที่ 10	 คนที่ 4, มือซ้าย, นิ้วกลาง, ครั้งที่ 11
 คนที่ 4, มือซ้าย, นิ้วชี้, ครั้งที่ 1	 คนที่ 4, มือซ้าย, นิ้วชี้, ครั้งที่ 2	 คนที่ 4, มือซ้าย, นิ้วชี้, ครั้งที่ 5	 คนที่ 4, มือซ้าย, นิ้วชี้, ครั้งที่ 7	 คนที่ 4, มือซ้าย, นิ้วโป้ง, ครั้งที่ 6
 คนที่ 4, มือซ้าย, นิ้วโป้ง, ครั้งที่ 7	 คนที่ 4, มือซ้าย, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 4, มือซ้าย, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 4, มือขวา, นิ้วนาง, ครั้งที่ 3	 คนที่ 4, มือขวา, นิ้วนาง, ครั้งที่ 9
 คนที่ 4, มือขวา, นิ้วนาง, ครั้งที่ 10	 คนที่ 4, มือขวา, นิ้วนาง, ครั้งที่ 12	 คนที่ 4, มือขวา, นิ้วกลาง, ครั้งที่ 3	 คนที่ 4, มือขวา, นิ้วกลาง, ครั้งที่ 5	 คนที่ 4, มือขวา, นิ้วกลาง, ครั้งที่ 6
 คนที่ 4, มือขวา, นิ้วกลาง, ครั้งที่ 9	 คนที่ 4, มือขวา, นิ้วชี้, ครั้งที่ 2	 คนที่ 4, มือขวา, นิ้วชี้, ครั้งที่ 6	 คนที่ 4, มือขวา, นิ้วชี้, ครั้งที่ 7	 คนที่ 4, มือขวา, นิ้วชี้, ครั้งที่ 10

 คนที่ 4, มือขวา, นิ้วโป้ง, ครั้งที่ 1	 คนที่ 4, มือขวา, นิ้วโป้ง, ครั้งที่ 2	 คนที่ 4, มือขวา, นิ้วโป้ง, ครั้งที่ 3	 คนที่ 4, มือขวา, นิ้วโป้ง, ครั้งที่ 5	 คนที่ 5, มือซ้าย, นิ้วนาง, ครั้งที่ 3
 คนที่ 5, มือซ้าย, นิ้วนาง, ครั้งที่ 6	 คนที่ 5, มือซ้าย, นิ้วนาง, ครั้งที่ 7	 คนที่ 5, มือซ้าย, นิ้วนาง, ครั้งที่ 10	 คนที่ 5, มือซ้าย, นิ้วกลาง, ครั้งที่ 5	 คนที่ 5, มือซ้าย, นิ้วกลาง, ครั้งที่ 7
 คนที่ 5, มือซ้าย, นิ้วกลาง, ครั้งที่ 10	 คนที่ 5, มือซ้าย, นิ้วกลาง, ครั้งที่ 11	 คนที่ 5, มือซ้าย, นิ้วชี้, ครั้งที่ 4	 คนที่ 5, มือซ้าย, นิ้วชี้, ครั้งที่ 5	 คนที่ 5, มือซ้าย, นิ้วชี้, ครั้งที่ 6
 คนที่ 5, มือซ้าย, นิ้วชี้, ครั้งที่ 7	 คนที่ 5, มือซ้าย, นิ้วโป้ง, ครั้งที่ 1	 คนที่ 5, มือซ้าย, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 5, มือซ้าย, นิ้วโป้ง, ครั้งที่ 7	 คนที่ 5, มือซ้าย, นิ้วโป้ง, ครั้งที่ 9
 คนที่ 5, มือขวา, นิ้วนาง, ครั้งที่ 2	 คนที่ 5, มือขวา, นิ้วนาง, ครั้งที่ 3	 คนที่ 5, มือขวา, นิ้วนาง, ครั้งที่ 9	 คนที่ 5, มือขวา, นิ้วนาง, ครั้งที่ 10	 คนที่ 5, มือขวา, นิ้วกลาง, ครั้งที่ 5

 คนที่ 5, มือขวา, นิ้วกลาง, ครั้งที่ 7	 คนที่ 5, มือขวา, นิ้วกลาง, ครั้งที่ 10	 คนที่ 5, มือขวา, นิ้วกลาง, ครั้งที่ 11	 คนที่ 5, มือขวา, นิ้วชี้, ครั้งที่ 6	 คนที่ 5, มือขวา, นิ้วชี้, ครั้งที่ 7
 คนที่ 5, มือขวา, นิ้วชี้, ครั้งที่ 10	 คนที่ 5, มือขวา, นิ้วชี้, ครั้งที่ 12	 คนที่ 5, มือขวา, นิ้วโป้ง, ครั้งที่ 1	 คนที่ 5, มือขวา, นิ้วโป้ง, ครั้งที่ 4	 คนที่ 5, มือขวา, นิ้วโป้ง, ครั้งที่ 5
 คนที่ 5, มือขวา, นิ้วโป้ง, ครั้งที่ 10	 คนที่ 6, มือซ้าย, นิ้วนาง, ครั้งที่ 1	 คนที่ 6, มือซ้าย, นิ้วนาง, ครั้งที่ 2	 คนที่ 6, มือซ้าย, นิ้วนาง, ครั้งที่ 6	 คนที่ 6, มือซ้าย, นิ้วนาง, ครั้งที่ 9
 คนที่ 6, มือซ้าย, นิ้วกลาง, ครั้งที่ 1	 คนที่ 6, มือซ้าย, นิ้วกลาง, ครั้งที่ 7	 คนที่ 6, มือซ้าย, นิ้วกลาง, ครั้งที่ 11	 คนที่ 6, มือซ้าย, นิ้วกลาง, ครั้งที่ 12	 คนที่ 6, มือซ้าย, นิ้วชี้, ครั้งที่ 4
 คนที่ 6, มือซ้าย, นิ้วชี้, ครั้งที่ 5	 คนที่ 6, มือซ้าย, นิ้วชี้, ครั้งที่ 6	 คนที่ 6, มือซ้าย, นิ้วชี้, ครั้งที่ 7	 คนที่ 6, มือซ้าย, นิ้วโป้ง, ครั้งที่ 2	 คนที่ 6, มือซ้าย, นิ้วโป้ง, ครั้งที่ 5

 คนที่ 6, มือซ้าย, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 6, มือซ้าย, นิ้วโป้ง, ครั้งที่ 9	 คนที่ 6, มือขวา, นิ้วนาง, ครั้งที่ 5	 คนที่ 6, มือขวา, นิ้วนาง, ครั้งที่ 6	 คนที่ 6, มือขวา, นิ้วนาง, ครั้งที่ 7
 คนที่ 6, มือขวา, นิ้วนาง, ครั้งที่ 12	 คนที่ 6, มือขวา, นิ้วกลาง, ครั้งที่ 4	 คนที่ 6, มือขวา, นิ้วกลาง, ครั้งที่ 5	 คนที่ 6, มือขวา, นิ้วกลาง, ครั้งที่ 6	 คนที่6, มือขวา, นิ้วกลาง, ครั้งที่ 10
 คนที่ 6, มือขวา, นิ้วโป้ง, ครั้งที่ 2	 คนที่ 6, มือขวา, นิ้วโป้ง, ครั้งที่ 5	 คนที่ 6, มือขวา, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 6, มือขวา, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 7, มือซ้าย, นิ้วนาง, ครั้งที่ 9
 คนที่ 7, มือซ้าย, นิ้วนาง, ครั้งที่ 10	 คนที่ 7, มือซ้าย, นิ้วนาง, ครั้งที่ 11	 คนที่ 7, มือซ้าย, นิ้วนาง, ครั้งที่ 12	 คนที่ 7, มือซ้าย, นิ้วกลาง, ครั้งที่ 3	 คนที่ 7, มือซ้าย, นิ้วกลาง, ครั้งที่ 9
 คนที่ 7, มือซ้าย, นิ้วกลาง, ครั้งที่ 11	 คนที่ 7, มือซ้าย, นิ้วกลาง, ครั้งที่ 12	 คนที่ 7, มือซ้าย, นิ้วชี้, ครั้งที่ 4	 คนที่ 7, มือซ้าย, นิ้วชี้, ครั้งที่ 5	 คนที่ 7, มือซ้าย, นิ้วชี้, ครั้งที่ 6

 คนที่ 7, มือซ้าย, นิ้วชี้, ครั้งที่ 7	 คนที่ 7, มือซ้าย, นิ้วโป้ง, ครั้งที่ 4	 คนที่ 7, มือซ้าย, นิ้วโป้ง, ครั้งที่ 5	 คนที่ 7, มือซ้าย, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 7, มือซ้าย, นิ้วโป้ง, ครั้งที่ 9
 คนที่ 7, มือขวา, นิ้วนาง, ครั้งที่ 9	 คนที่ 7, มือขวา, นิ้วนาง, ครั้งที่ 10	 คนที่ 7, มือขวา, นิ้วนาง, ครั้งที่ 11	 คนที่ 7, มือขวา, นิ้วนาง, ครั้งที่ 12	 คนที่ 7, มือขวา, นิ้วกลาง, ครั้งที่ 6
 คนที่ 7, มือขวา, นิ้วกลาง, ครั้งที่ 7	 คนที่ 7, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 7, มือขวา, นิ้วกลาง, ครั้งที่ 9	 คนที่ 7, มือขวา, นิ้วโป้ง, ครั้งที่2	 คนที่ 7, มือขวา, นิ้วโป้ง, ครั้งที่ 4
 คนที่ 7, มือขวา, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 7, มือขวา, นิ้วโป้ง, ครั้งที่ 7	 คนที่ 8, มือซ้าย, นิ้วนาง, ครั้งที่ 6	 คนที่ 8, มือซ้าย, นิ้วนาง, ครั้งที่ 7	 คนที่ 8, มือซ้าย, นิ้วนาง, ครั้งที่ 8
 คนที่ 8, มือซ้าย, นิ้วนาง, ครั้งที่ 11	 คนที่ 8, มือซ้าย, นิ้วกลาง, ครั้งที่ 1	 คนที่ 8, มือซ้าย, นิ้วกลาง, ครั้งที่ 3	 คนที่ 8, มือซ้าย, นิ้วกลาง, ครั้งที่ 7	 คนที่ 8, มือซ้าย, นิ้วกลาง, ครั้งที่ 11

ภาคผนวก ข

ตัวอย่างภาพลายนิ้วมือบางส่วนที่เก็บข้อมูลจากอาสาสมัครผ่านเครื่องอ่านลายนิ้วมือ U.are.U 2000

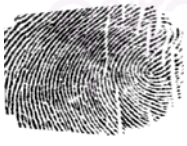
ขนาดภาพลายนิ้วมือที่แสดงด้านล่างเป็น 25% ของขนาดภาพจริง

 คนที่ 20, มือซ้าย, นิ้วนาง, ครั้งที่ 2	 คนที่ 20, มือซ้าย, นิ้วนาง, ครั้งที่ 5	 คนที่ 20, มือซ้าย, นิ้วนาง, ครั้งที่ 7	 คนที่ 20, มือซ้าย, นิ้วนาง, ครั้งที่ 8	 คนที่ 20, มือซ้าย, นิ้วกลาง, ครั้งที่ 1
 คนที่ 20, มือซ้าย, นิ้วกลาง, ครั้งที่ 3	 คนที่ 20, มือซ้าย, นิ้วกลาง, ครั้งที่ 6	 คนที่ 20, มือซ้าย, นิ้วกลาง, ครั้งที่ 8	 คนที่ 20, มือซ้าย, นิ้วชี้, ครั้งที่ 7	 คนที่ 20, มือซ้าย, นิ้วชี้, ครั้งที่ 9
 คนที่ 20, มือซ้าย, นิ้วชี้, ครั้งที่ 10	 คนที่ 20, มือซ้าย, นิ้วชี้ , ครั้งที่ 12	 คนที่ 20, มือซ้าย, นิ้วโป้ง , ครั้งที่ 2	 คนที่ 20, มือซ้าย, นิ้วโป้ง , ครั้งที่ 3	 คนที่ 20, มือซ้าย, นิ้วโป้ง , ครั้งที่ 8
 คนที่ 20, มือซ้าย, นิ้วโป้ง , ครั้งที่ 11	 คนที่ 20, มือขวา, นิ้วนาง, ครั้งที่ 2	 คนที่ 20, มือขวา, นิ้วนาง, ครั้งที่ 5	 คนที่ 20, มือขวา, นิ้วนาง, ครั้งที่ 7	 คนที่ 20, มือขวา, นิ้วนาง, ครั้งที่ 8
 คนที่ 20, มือขวา, นิ้วกลาง, ครั้งที่ 1	 คนที่ 20, มือขวา, นิ้วกลาง, ครั้งที่ 3	 คนที่ 20, มือขวา, นิ้วกลาง, ครั้งที่ 6	 คนที่ 20, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 20, มือขวา, นิ้วชี้, ครั้งที่ 7

 คนที่ 20, มือขวา, นิ้วชี้, ครั้งที่ 9	 คนที่ 20, มือขวา, นิ้วชี้, ครั้งที่ 10	 คนที่ 20, มือขวา, นิ้วชี้ , ครั้งที่ 12	 คนที่ 20, มือขวา, นิ้วโป้ง , ครั้งที่ 2	 คนที่ 20, มือขวา, นิ้วโป้ง , ครั้งที่ 3
 คนที่ 20, มือขวา, นิ้วโป้ง , ครั้งที่ 8	 คนที่ 20, มือขวา, นิ้วโป้ง , ครั้งที่ 11	 คนที่ 21, มือซ้าย, นิ้วนาง, ครั้งที่ 3	 คนที่ 21, มือซ้าย, นิ้วนาง, ครั้งที่ 5	 คนที่ 21, มือซ้าย, นิ้วนาง, ครั้งที่ 7
 คนที่ 21, มือซ้าย, นิ้วนาง, ครั้งที่ 8	 คนที่ 21, มือซ้าย, นิ้วกลาง, ครั้งที่ 5	 คนที่ 21, มือซ้าย, นิ้วกลาง, ครั้งที่ 9	 คนที่ 21, มือซ้าย, นิ้วกลาง, ครั้งที่ 11	 คนที่ 21, มือซ้าย, นิ้วกลาง, ครั้งที่ 12
 คนที่ 21, มือซ้าย, นิ้วชี้, ครั้งที่ 2	 คนที่ 21, มือซ้าย, นิ้วชี้, ครั้งที่ 3	 คนที่ 21, มือซ้าย, นิ้วชี้, ครั้งที่ 11	 คนที่ 21, มือซ้าย, นิ้วชี้, ครั้งที่ 12	 คนที่ 21, มือซ้าย, นิ้วโป้ง, ครั้งที่ 5
 คนที่ 21, มือซ้าย, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 21, มือซ้าย, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 21, มือซ้าย, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 21, มือขวา, นิ้วนาง, ครั้งที่ 7	 คนที่ 21, มือขวา, นิ้วนาง, ครั้งที่ 8
 คนที่ 21, มือขวา, นิ้วนาง, ครั้งที่ 10	 คนที่ 21, มือขวา, นิ้วนาง, ครั้งที่ 11	 คนที่ 21, มือขวา, นิ้วกลาง, ครั้งที่ 2	 คนที่ 21, มือขวา, นิ้วกลาง, ครั้งที่ 4	 คนที่ 21, มือขวา, นิ้วกลาง, ครั้งที่ 7

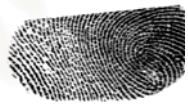
 คนที่ 21, มือขวา, นิ้วกลาง, ครั้งที่ 11	 คนที่ 21, มือขวา, นิ้วชี้, ครั้งที่ 2	 คนที่ 21, มือขวา, นิ้วชี้, ครั้งที่ 3	 คนที่ 21, มือขวา, นิ้วชี้, ครั้งที่ 7	 คนที่ 21, มือขวา, นิ้วชี้, ครั้งที่ 12
 คนที่ 21, มือขวา, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 21, มือขวา, นิ้วโป้ง, ครั้งที่ 9	 คนที่ 21, มือขวา, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 21, มือขวา, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 22, มือซ้าย, นิ้วนาง, ครั้งที่ 5
 คนที่ 22, มือซ้าย, นิ้วนาง, ครั้งที่ 7	 คนที่ 22, มือซ้าย, นิ้วนาง, ครั้งที่ 8	 คนที่ 22, มือซ้าย, นิ้วนาง, ครั้งที่ 10	 คนที่ 22, มือซ้าย, นิ้วกลาง, ครั้งที่ 1	 คนที่ 22, มือซ้าย, นิ้วกลาง, ครั้งที่ 4
 คนที่ 22, มือซ้าย, นิ้วกลาง, ครั้งที่ 5	 คนที่ 22, มือซ้าย, นิ้วกลาง, ครั้งที่ 11	 คนที่ 22, มือซ้าย, นิ้วชี้, ครั้งที่ 2	 คนที่ 22, มือซ้าย, นิ้วชี้, ครั้งที่ 5	 คนที่ 22, มือซ้าย, นิ้วชี้, ครั้งที่ 7
 คนที่ 22, มือซ้าย, นิ้วชี้, ครั้งที่ 12	 คนที่ 22, มือซ้าย, นิ้วโป้ง, ครั้งที่ 2	 คนที่ 22, มือซ้าย, นิ้วโป้ง, ครั้งที่ 5	 คนที่ 22, มือซ้าย, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 22, มือซ้าย, นิ้วโป้ง, ครั้งที่ 11
 คนที่ 22, มือขวา, นิ้วนาง, ครั้งที่ 1	 คนที่ 22, มือขวา, นิ้วนาง, ครั้งที่ 3	 คนที่ 22, มือขวา, นิ้วนาง, ครั้งที่ 7	 คนที่ 22, มือขวา, นิ้วนาง, ครั้งที่ 10	 คนที่ 22, มือขวา, นิ้วกลาง, ครั้งที่ 3

 คนที่ 22, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 22, มือขวา, นิ้วกลาง, ครั้งที่ 9	 คนที่ 22, มือขวา, นิ้วกลาง, ครั้งที่ 11	 คนที่ 22, มือขวา, นิ้วชี้, ครั้งที่ 3	 คนที่ 22, มือขวา, นิ้วชี้, ครั้งที่ 5
 คนที่ 22, มือขวา, นิ้วชี้, ครั้งที่ 6	 คนที่ 22, มือขวา, นิ้วชี้, ครั้งที่ 11	 คนที่ 22, มือขวา, นิ้วโป้ง, ครั้งที่ 4	 คนที่ 22, มือขวา, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 22, มือขวา, นิ้วโป้ง, ครั้งที่ 9
 คนที่ 22, มือขวา, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 23, มือซ้าย, นิ้วนาง, ครั้งที่ 2	 คนที่ 23, มือซ้าย, นิ้วนาง, ครั้งที่ 3	 คนที่ 23, มือซ้าย, นิ้วนาง, ครั้งที่ 5	 คนที่ 23, มือซ้าย, นิ้วนาง, ครั้งที่ 12
 คนที่ 23, มือซ้าย, นิ้วกลาง, ครั้งที่ 1	 คนที่ 23, มือซ้าย, นิ้วกลาง, ครั้งที่ 5	 คนที่ 23, มือซ้าย, นิ้วกลาง, ครั้งที่ 8	 คนที่ 23, มือซ้าย, นิ้วกลาง, ครั้งที่ 9	 คนที่ 23, มือซ้าย, นิ้วชี้, ครั้งที่ 3
 คนที่ 23, มือซ้าย, นิ้วชี้, ครั้งที่ 4	 คนที่ 23, มือซ้าย, นิ้วชี้, ครั้งที่ 7	 คนที่ 23, มือซ้าย, นิ้วชี้, ครั้งที่ 10	 คนที่ 23, มือซ้าย, นิ้วโป้ง, ครั้งที่ 4	 คนที่ 23, มือซ้าย, นิ้วโป้ง, ครั้งที่ 6
 คนที่ 23, มือซ้าย, นิ้วโป้ง, ครั้งที่ 9	 คนที่ 23, มือซ้าย, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 23, มือขวา, นิ้วนาง, ครั้งที่ 1	 คนที่ 23, มือขวา, นิ้วนาง, ครั้งที่ 8	 คนที่ 23, มือขวา, นิ้วนาง, ครั้งที่ 10

 คนที่ 23, มือขวา, นิ้วนาง, ครั้งที่ 12	 คนที่ 23, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 23, มือขวา, นิ้วกลาง, ครั้งที่ 10	 คนที่ 23, มือขวา, นิ้วกลาง, ครั้งที่ 11	 คนที่ 23, มือขวา, นิ้วกลาง, ครั้งที่12
 คนที่ 23, มือขวา, นิ้วชี้, ครั้งที่ 3	 คนที่ 23, มือขวา, นิ้วชี้, ครั้งที่ 8	 คนที่ 23, มือขวา, นิ้วชี้, ครั้งที่ 9	 คนที่ 23, มือขวา, นิ้วชี้, ครั้งที่ 11	 คนที่ 23, มือขวา, นิ้วโป้ง, ครั้งที่ 1
 คนที่ 23, มือขวา, นิ้วโป้ง, ครั้งที่ 4	 คนที่ 23, มือขวา, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 23, มือขวา, นิ้วโป้ง, ครั้งที่ 10	 คนที่ 24, มือซ้าย, นิ้วนาง, ครั้งที่ 5	 คนที่ 24, มือซ้าย, นิ้วนาง, ครั้งที่ 7
 คนที่ 24, มือซ้าย, นิ้วนาง, ครั้งที่ 10	 คนที่ 24, มือซ้าย, นิ้วนาง, ครั้งที่ 11	 คนที่ 24, มือซ้าย, นิ้วกลาง, ครั้งที่ 4	 คนที่ 24, มือซ้าย, นิ้วกลาง, ครั้งที่ 6	 คนที่ 24, มือซ้าย, นิ้วกลาง, ครั้งที่ 7
 คนที่ 24, มือซ้าย, นิ้วกลาง, ครั้งที่ 10	 คนที่ 24, มือซ้าย, นิ้วชี้, ครั้งที่ 1	 คนที่ 24, มือซ้าย, นิ้วชี้, ครั้งที่ 2	 คนที่ 24, มือซ้าย, นิ้วชี้, ครั้งที่ 8	 คนที่ 24, มือซ้าย, นิ้วชี้, ครั้งที่ 11
 คนที่ 24, มือซ้าย, นิ้วโป้ง, ครั้งที่ 3	 คนที่ 24, มือซ้าย, นิ้วโป้ง, ครั้งที่ 7	 คนที่ 24, มือซ้าย, นิ้วโป้ง, ครั้งที่ 9	 คนที่ 24, มือซ้าย, นิ้วโป้ง, ครั้งที่ 10	 คนที่ 24, มือขวา, นิ้วนาง, ครั้งที่ 1

 คนที่ 24, มือขวา, นิ้วนาง, ครั้งที่ 3	 คนที่ 24, มือขวา, นิ้วนาง, ครั้งที่ 8	 คนที่ 24, มือขวา, นิ้วนาง, ครั้งที่ 11	 คนที่ 24, มือขวา, นิ้วกลาง, ครั้งที่ 2	 คนที่ 24, มือขวา, นิ้วกลาง, ครั้งที่ 6
 คนที่ 24, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 24, มือขวา, นิ้วกลาง, ครั้งที่ 9	 คนที่ 24, มือขวา, นิ้วชี้, ครั้งที่ 1	 คนที่ 24, มือขวา, นิ้วชี้, ครั้งที่ 3	 คนที่ 24, มือขวา, นิ้วชี้, ครั้งที่ 5
 คนที่ 24, มือขวา, นิ้วชี้, ครั้งที่ 7	 คนที่ 24, มือขวา, นิ้วโป้ง, ครั้งที่ 3	 คนที่ 24, มือขวา, นิ้วโป้ง, ครั้งที่ 4	 คนที่ 24, มือขวา, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 24, มือขวา, นิ้วโป้ง, ครั้งที่ 8
 คนที่ 25, มือซ้าย, นิ้วนาง, ครั้งที่ 4	 คนที่ 25, มือซ้าย, นิ้วนาง, ครั้งที่ 7	 คนที่ 25, มือซ้าย, นิ้วนาง, ครั้งที่ 9	 คนที่ 25, มือซ้าย, นิ้วนาง, ครั้งที่ 12	 คนที่ 25, มือซ้าย, นิ้วกลาง, ครั้งที่ 1
 คนที่ 25, มือซ้าย, นิ้วกลาง, ครั้งที่ 3	 คนที่ 25, มือซ้าย, นิ้วกลาง, ครั้งที่ 7	 คนที่ 25, มือซ้าย, นิ้วกลาง, ครั้งที่ 12	 คนที่ 25, มือซ้าย, นิ้วชี้, ครั้งที่ 2	 คนที่ 25, มือซ้าย, นิ้วชี้, ครั้งที่ 3
 คนที่ 25, มือซ้าย, นิ้วชี้, ครั้งที่ 8	 คนที่ 25, มือซ้าย, นิ้วชี้, ครั้งที่ 11	 คนที่ 25, มือซ้าย, นิ้วโป้ง, ครั้งที่ 2	 คนที่ 25, มือซ้าย, นิ้วโป้ง, ครั้งที่ 5	 คนที่ 25, มือซ้าย, นิ้วโป้ง, ครั้งที่ 10

 คนที่ 25, มือซ้าย, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 25, มือขวา, นิ้วนาง, ครั้งที่ 3	 คนที่ 25, มือขวา, นิ้วนาง, ครั้งที่ 4	 คนที่ 25, มือขวา, นิ้วนาง, ครั้งที่ 7	 คนที่ 25, มือขวา, นิ้วนาง, ครั้งที่ 11
 คนที่ 25, มือขวา, นิ้วกลาง, ครั้งที่ 2	 คนที่ 25, มือขวา, นิ้วกลาง, ครั้งที่ 3	 คนที่ 25, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 25, มือขวา, นิ้วกลาง, ครั้งที่ 9	 คนที่ 25, มือขวา, นิ้วชี้, ครั้งที่ 1
 คนที่ 25, มือขวา, นิ้วชี้, ครั้งที่ 3	 คนที่ 25, มือขวา, นิ้วชี้, ครั้งที่ 4	 คนที่ 25, มือขวา, นิ้วชี้, ครั้งที่ 11	 คนที่ 25, มือขวา, นิ้วโป้ง, ครั้งที่ 1	 คนที่ 25, มือขวา, นิ้วโป้ง, ครั้งที่ 5
 คนที่ 25, มือขวา, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 25, มือขวา, นิ้วโป้ง, ครั้งที่ 10	 คนที่ 26, มือซ้าย, นิ้วนาง, ครั้งที่ 3	 คนที่ 26, มือซ้าย, นิ้วนาง, ครั้งที่ 5	 คนที่ 26, มือซ้าย, นิ้วนาง, ครั้งที่ 7
 คนที่ 26, มือซ้าย, นิ้วนาง, ครั้งที่ 8	 คนที่ 26, มือซ้าย, นิ้วกลาง, ครั้งที่ 5	 คนที่ 26, มือซ้าย, นิ้วกลาง, ครั้งที่ 9	 คนที่ 26, มือซ้าย, นิ้วกลาง, ครั้งที่ 11	 คนที่ 26, มือซ้าย, นิ้วกลาง, ครั้งที่ 12
 คนที่ 26, มือซ้าย, นิ้วชี้, ครั้งที่ 2	 คนที่ 26, มือซ้าย, นิ้วชี้, ครั้งที่ 3	 คนที่ 26, มือซ้าย, นิ้วชี้, ครั้งที่ 11	 คนที่ 26, มือซ้าย, นิ้วชี้, ครั้งที่ 12	 คนที่ 26, มือซ้าย, นิ้วโป้ง, ครั้งที่ 5

 คนที่ 26, มือซ้าย, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 26, มือซ้าย, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 26, มือซ้าย, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 26, มือขวา, นิ้วนาง, ครั้งที่ 7	 คนที่ 26, มือขวา, นิ้วนาง, ครั้งที่ 8
 คนที่ 26, มือขวา, นิ้วนาง, ครั้งที่ 10	 คนที่ 26, มือขวา, นิ้วนาง, ครั้งที่ 11	 คนที่ 26, มือขวา, นิ้วกลาง, ครั้งที่ 2	 คนที่ 26, มือขวา, นิ้วกลาง, ครั้งที่ 4	 คนที่ 26, มือขวา, นิ้วกลาง, ครั้งที่ 7
 คนที่ 26, มือขวา, นิ้วกลาง, ครั้งที่ 11	 คนที่ 26, มือขวา, นิ้วชี้, ครั้งที่ 2	 คนที่ 26, มือขวา, นิ้วชี้, ครั้งที่ 3	 คนที่ 26, มือขวา, นิ้วชี้, ครั้งที่ 7	 คนที่ 26, มือขวา, นิ้วชี้, ครั้งที่ 12
 คนที่ 26, มือขวา, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 26, มือขวา, นิ้วโป้ง, ครั้งที่ 9	 คนที่ 26, มือขวา, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 26, มือขวา, นิ้วโป้ง, ครั้งที่ 12	 คนที่ 27, มือซ้าย, นิ้วนาง, ครั้งที่ 5
 คนที่ 27, มือซ้าย, นิ้วนาง, ครั้งที่ 7	 คนที่ 27, มือซ้าย, นิ้วนาง, ครั้งที่ 8	 คนที่ 27, มือซ้าย, นิ้วนาง, ครั้งที่ 10	 คนที่ 27, มือซ้าย, นิ้วกลาง, ครั้งที่ 1	 คนที่ 27, มือซ้าย, นิ้วกลาง, ครั้งที่ 4
 คนที่ 27, มือซ้าย, นิ้วกลาง, ครั้งที่ 5	 คนที่ 27, มือซ้าย, นิ้วกลาง, ครั้งที่ 11	 คนที่ 27, มือซ้าย, นิ้วชี้, ครั้งที่ 2	 คนที่ 27, มือซ้าย, นิ้วชี้, ครั้งที่ 5	 คนที่ 27, มือซ้าย, นิ้วชี้, ครั้งที่ 7

 คนที่ 27, มือซ้าย, นิ้วชี้, ครั้งที่ 12	 คนที่ 27, มือซ้าย, นิ้วโป้ง, ครั้งที่ 2	 คนที่ 27, มือซ้าย, นิ้วโป้ง, ครั้งที่ 5	 คนที่ 27, มือซ้าย, นิ้วโป้ง, ครั้งที่ 8	 คนที่ 27, มือซ้าย, นิ้วโป้ง, ครั้งที่ 11
 คนที่ 27, มือขวา, นิ้วนาง, ครั้งที่ 1	 คนที่ 27, มือขวา, นิ้วนาง, ครั้งที่ 3	 คนที่ 27, มือขวา, นิ้วนาง, ครั้งที่ 7	 คนที่ 27, มือขวา, นิ้วนาง, ครั้งที่ 10	 คนที่ 27, มือขวา, นิ้วกลาง, ครั้งที่ 3
 คนที่ 27, มือขวา, นิ้วกลาง, ครั้งที่ 8	 คนที่ 27, มือขวา, นิ้วกลาง, ครั้งที่ 9	 คนที่ 27, มือขวา, นิ้วกลาง, ครั้งที่ 11	 คนที่ 27, มือขวา, นิ้วชี้, ครั้งที่ 3	 คนที่ 27, มือขวา, นิ้วชี้, ครั้งที่ 5
 คนที่ 27, มือขวา, นิ้วชี้, ครั้งที่ 6	 คนที่ 27, มือขวา, นิ้วชี้, ครั้งที่ 11	 คนที่ 27, มือขวา, นิ้วโป้ง, ครั้งที่ 4	 คนที่ 27, มือขวา, นิ้วโป้ง, ครั้งที่ 6	 คนที่ 27, มือขวา, นิ้วโป้ง, ครั้งที่ 9
 คนที่ 27, มือขวา, นิ้วโป้ง, ครั้งที่ 11	 คนที่ 28, มือซ้าย, นิ้วนาง, ครั้งที่ 5	 คนที่ 28, มือซ้าย, นิ้วนาง, ครั้งที่ 6	 คนที่ 28, มือซ้าย, นิ้วนาง, ครั้งที่ 10	 คนที่ 28, มือซ้าย, นิ้วนาง, ครั้งที่ 11
 คนที่ 28, มือซ้าย, นิ้วกลาง, ครั้งที่ 1	 คนที่ 28, มือซ้าย, นิ้วกลาง, ครั้งที่ 6	 คนที่ 28, มือซ้าย, นิ้วกลาง, ครั้งที่ 8	 คนที่ 28, มือซ้าย, นิ้วกลาง, ครั้งที่ 9	 คนที่ 28, มือซ้าย, นิ้วชี้, ครั้งที่ 3

ประวัติผู้เขียนวิทยานิพนธ์

นายชัยรัตน์ องค์วิศิษฐ์ เกิดเมื่อวันที่ 2 มกราคม พ.ศ. 2525 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษา หลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2544 และเข้าศึกษาในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ปีการศึกษา 2545

งานวิจัยที่ได้รับการตีพิมพ์ในการประชุมวิชาการมีด้วยกัน 1 ชิ้น เรื่องการพัฒนาอัลกอริทึมเปรียบเทียบลายนิ้วมือเพื่อใช้ประมวลผลบนสมาร์ตคาร์ด”,“Development of Fingerprint Matching Algorithm for Processing on Smart card” โดย ชัยรัตน์ องค์วิศิษฐ์ และ สาธิต วงศ์ประทีป ในงานประชุมวิชาการ “The 7th National Computer Science and Engineering Conference (NCSEC2003)” ซึ่งจัดโดยภาควิชาวิทยาศาสตร์คอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยบูรพา 169 ถนนลงหาดบางแสน ตำบลแสนสุข อำเภอเมือง จังหวัดชลบุรี ในระหว่างวันที่ 28-30 ตุลาคม 2546