เครื่องรักษาความปลอดภัยในรถยนต์ด้วยระบบตรวจสอบลายนิ้วมือ

CAR SECURITY USING FINGERPRINT SENSOR

โดย

นายภูเบศ ธรรมจิโรจ

นายศุภวุฒิ สมรรถจิตต์

นายธนกร รุ่งธีรวัฒนานนท์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2551

เครื่องรักษาความปลอดภัยในรถยนต์ด้วยระบบตรวจสอบลายนิ้วมือ

CAR SECURITY USING FINGERPRINT SENSOR

โดย

นายภูเบศ	ธรรมจิโรจ	48010574
นายศุภวุฒิ	สมรรถจิตต์	48010918
นายธนกร	รุ่งธีรวัฒนานนท์	48012018

อาจารย์ที่ปรึกษา

รศ.สมยศ จุณณะปิยะ

ผศ.ดร.พิเชฐ ม่วงนวล

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2551

ปริญญานิพนธ์ปีการศึกษา 2551

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง เครื่องรักษาความปลอดภัยในรถยนต์ด้วยระบบตรวจสอบลายนิ้วมือ

CAR SECURITY USING FINGERPRINT SENSOR

ผู้จัดทำ

1. นายภูเบศ ธรรมจิโรจ 48010574
2. นายศุภวุฒิ สมรรถจิตต์ 48010918
3. นายธนกร รุ่งธีรวัฒนานนท์ 48012018

..... อาจารย์ที่ปรึกษา

(รศ. สมยศ จุณณะปิยะ)

..... อาจารย์ที่ปรึกษา

(ผศ.ดร. พิเชฐ ม่วงนวล)

เครื่องรักษาความปลอดภัยในรถยนต์ด้วยระบบตรวจสอบลายนิ้วมือ

CAR SECURITY USING FINGERPRINT SENSOR

โดย นายภูเบศ ธรรมจิโรจ 48010574

นายศุภวุฒิ สมรรถจิตต์ 48010918

นายธนกร รุ่งธีรวัฒนานนท์ 48012018

อาจารย์ที่ปรึกษา รศ. สมยศ จุณณะปิยะ

ผศ.ดร.พิเชฐ ม่วงนวล

บทคัดย่อ

ในปัจจุบันนี้สภาพเศรษฐกิจมีสภาพย่ำแย่ จึงส่งผลให้มีมิจฉาชีพมากขึ้น ซึ่งรถยนต์ก็เป็นเป้าหมายหนึ่งของมิจฉาชีพ และเทคโนโลยีที่มีอยู่อาจจะไม่เพียงพอ เช่น เครื่องล็อคประเภทต่างๆ ก็จะติดปัญหาคล้ายๆกันคือ การต้องพกกุญแจซึ่งก็สามารถปลอมได้ไม่ยาก ซึ่งทำให้เจ้าของรถยนต์เป็นกังวล เราจึงแก้ปัญหาเหล่านี้โดยใช้เทคโนโลยีด้านอิเล็กทรอนิกส์และไบโอเมตริก มาเป็นระบบล็อคการทำงานของรถยนต์ซึ่งเป็นการป้องกัน ที่มีขีดความสามารถมากกว่า

ABSTRACT

Recently years, the economic system has gone badly which made the criminal rate increased and the vehicle is one of the target for them and the technology we had may be not enough such as key locker system usually has same problem, carrying key which it can easily copied. The vehicle owner may get nervous. We can solve this problem by using electronic and biometric technology to put in car security which it had a higher ability for secure the vehicle.

สารบัญ

สารบัญ(ต่อ)

สารบัญรูปภาพ

สารบัญรูปภาพ(ต่อ)

หน้า

สารบัญรูปภาพ(ต่อ)

สารบัญตาราง

บทที่1

บทนำ

ในปัจจุบันตลาดรถยนต์ยิ่งมีขนาดใหญ่มากขึ้น สังเกตได้จากจำนวนรถบนท้องถนนที่มีมากขึ้นทุกๆวัน มีทั้งรุ่นที่มีราคาแพงแสนแพง รถยี่ห้อดังที่หรูหรา แต่ไม่ว่าจะเป็นรถรุ่นไหนสำหรับเจ้าของรถก็ย่อมมีความรู้สึกหวงแหน ไม่อยากให้หายไปไหนแต่มันก็คู่สวนทางกับพวกมิจฉาชีพที่จ้องจะขโมยรถทั้งๆที่เจ้าของรถก็พยายามหาวิธีต่างๆเพื่อมาป้องกันรถยนต์ของตัวเอง แต่ไม่ว่าจะเป็นการล็อคด้วยวิธีพื้นฐานใดๆ เช่น ล็อคกุญแจที่เบรก, คลัช, พวงมาลัยหรือระบบเทคโนโลยีทางอิเล็กทรอนิกส์เข้ามาช่วย เช่น ระบบล็อคด้วยรีโมทคอนโทรลไร้สายก็ดูเหมือนไม่เพียงพอดังนั้นเราจึงได้นำระบบตรวจสอบลายนิ้วมือระบุตัวบุคคลมาใช้ป้องกันเนื่องจากมีความปลอดภัยสูงกว่า

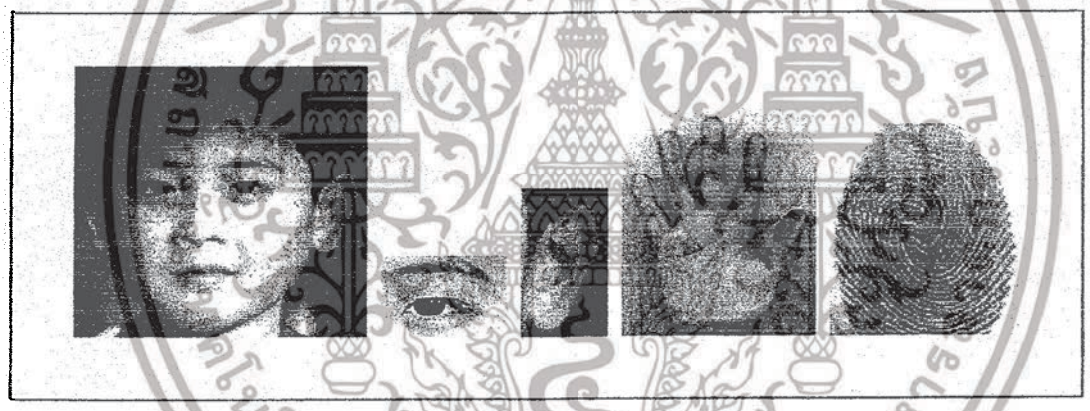
โครงงานฉบับนี้จึงมีจุดมุ่งหมายเพื่อที่จะนำเสนอการรักษาความปลอดภัยในรถยนต์ โดยใช้หลักการตรวจสอบลายนิ้วมือของแต่ละบุคคลที่มีสิทธิ์ได้รับอนุญาตด้วยเครื่องสแกนลายนิ้วมือโดยมีหลักการทำงานที่สำคัญดังนี้ คือขั้นตอนแรกจะทำการเก็บลายนิ้วมือ โดยสแกนลายนิ้วมือผ่านเครื่องสแกนลายนิ้วมือ ข้อมูลที่ได้จะอยู่ในรูปเวกเตอร์ของภาพ หรือเก็บข้อมูลในส่วนที่เป็นองค์ประกอบที่สำคัญของภาพ การที่ต้องใช้การเปรียบเทียบลายนิ้วมือด้วยเวกเตอร์นั้น เนื่องจากว่าการเปรียบเทียบดังกล่าวมีค่าความผิดพลาดต่ำมากหรือแทบไม่มีความผิดพลาดเลย ขั้นตอนต่อไปคือการเก็บข้อมูลของผู้ที่ได้รับอนุญาตในการใช้ไว้ในฐานข้อมูลที่เราสร้างขึ้นซึ่งมีข้อมูลที่สำคัญเพื่อยืนยันถึงตัวบุคคลที่เป็นเจ้าของลายนิ้วมือ ซึ่งเมื่อมีการใช้งานระบบจะทำการตรวจสอบข้อมูลจากฐานข้อมูลที่ได้บันทึกไว้ หากถูกต้องตรงกับฐานข้อมูลที่มีอยู่จึงสามารถเข้าใช้งานได้

บทที่ 2
ทฤษฎีและหลักการ

2.1 ไบโอเมตริกซ์

2.1.1 นิยามและความหมายของไบโอเมตริกซ์

คำว่าไบโอเมตริกซ์(Biometrics) หรือ Biometry มีการนำมาใช้กันนับร้อยปีแล้ว โดยเป็นศาสตร์ด้านหนึ่งในการนำเอาวิธีการทางคณิตศาสตร์หรือวิธีการทางสถิติมาใช้ในการวิเคราะห์แก้ไขปัญหาทางด้านชีววิทยาต่างๆ เช่น การใช้วิธีทางสถิติวิเคราะห์ผลกระทบของมลพิษที่มีผลต่อสุขภาพของบุคคล, การวิเคราะห์ข้อมูลสภาพอากาศที่มีผลต่อการเพาะปลูก เป็นต้น แต่ความหมายของ Biometrics ด้านนี้ไม่ใช่วัตถุประสงค์หลักของกลุ่มวิจัยนี้ แต่เป็นอีกความหมายหนึ่งของ Biometrics ซึ่งเป็นศาสตร์ที่เกี่ยวข้องกับการใช้กระบวนการในการระบุตัวบุคคลหรือตรวจสอบตัวบุคคลโดยอัตโนมัติ โดยใช้ลักษณะทางกายภาพที่แตกต่างกันแต่ละบุคคล เช่น รูปแบบของลายนิ้วมือ(Fingerprint), รูปลักษณ์ของมือ(Hand Geometry), ลักษณะของเรตินา(Retina Pattern), ลักษณะของม่านตา(Iris Pattern), รูปลักษณ์ใบหน้า(Facial) เป็นต้น หรือใช้ลักษณะทางพฤติกรรมของแต่ละบุคคล เช่น เสียง(Voice) ,เอกลักษณ์ในการพิมพ์(Keystroke Dynamics), ลักษณะท่าทางในการเดิน(Gait recognition) เป็นต้น



รูปที่ 2.1 การตรวจสอบตัวบุคคล โดยใช้ลักษณะทางกายภาพที่แตกต่างกันของแต่ละบุคคล

กระบวนการที่ทำให้ระบบคอมพิวเตอร์สามารถระบุบุคคลได้โดยอัตโนมัตินั้นเป็นการเลียนแบบพฤติกรรมของมนุษย์ประเภทหนึ่ง มนุษย์เราใช้วิธีการทางไบโอเมตริกซ์ในการระบุตัวบุคคลอยู่ตลอดเวลา เราใช้ลักษณะจำเพาะทางรูปร่าง ใบหน้า น้ำเสียง หรือแม้กระทั่งกลิ่น ของแต่ละบุคคลในการระบุว่าคนที่เราพบเป็นคนที่เรารู้จักหรือไม่ ดังนั้นจึงถือได้ว่าไบโอเมตริกซ์ เป็นรูปแบบหนึ่งของปัญญาประดิษฐ์(Artificial Intelligence) นั่นเอง

เทคโนโลยีด้านนี้เริ่มมีการนำมาประยุกต์ใช้งานมานับสิบปีแล้ว ทั้งในภาครัฐบาลและภาคเอกชน แต่ประสิทธิภาพและความน่าเชื่อถือได้ยังเป็นที่น่าสงสัยอยู่ อย่างไรก็ตามการที่บุคคลโดยทั่วไปเริ่มมีการใช้งานระบบคอมพิวเตอร์เพิ่มมากขึ้น ความจำเป็นและความสำคัญในการใช้ Biometric ในการตรวจสอบตัวบุคคลก็มีความสำคัญและจำเป็นเพิ่มขึ้นไปด้วย

การระบุตัวบุคคลโดยใช้ไบโอเมตริกซ์ สามารถนำมาประยุกต์ใช้งานได้ทั้งในภาครัฐบาลและภาคเอกชน เช่น งานทางด้านรักษาความปลอดภัย, ช่วยผู้รักษากฎหมายในการจับตัวผู้กระทำผิด, ช่วยในการ

ตรวจสอบผู้ใช้งานของระบบเครือข่ายคอมพิวเตอร์, การจัดการระบบบริหารงานบุคคล (เช่น งานตรวจสอบเวลาการทำงาน), ช่วยในการตรวจสอบบุคคลในการซื้อขายสินค้าผ่านทางอินเตอร์เน็ต, การจัดการเรื่องการพิสูจน์ตัวบุคคลของสถาบันการเงิน เป็นต้น

2.1.2 ข้อดีของการนำเอาไบโอเมตริกซ์มาใช้งานในการตรวจสอบหรือระบุตัวบุคคล

การใช้ไบโอเมตริกซ์ทำให้ผู้ใช้ไม่จำเป็นต้องใช้ความจำหรือจำเป็นต้องถือบัตรผ่านใดๆ ทำให้สะดวกและรวดเร็ว ผู้ใช้ไม่จำเป็นต้องพกบัตรและไม่ต้องจำรหัสผ่านอีกทั้งยังเป็นการช่วยเพิ่มความปลอดภัยและป้องกันการสูญหายของบัตรผ่านหรือการลักลอบนำเอารหัสผ่านไปใช้ไบโอเมตริกซ์ยากต่อการปลอมแปลงและยากต่อการลักลอบนำไปใช้

การใช้ไบโอเมตริกซ์ ทำให้ผู้ใช้ไม่สามารถปฏิเสธความรับผิดชอบได้ เช่น ในกรณีของการใช้รหัสผ่านหรือบัตรผ่าน เจ้าของบัตรอาจอ้างได้ว่ารหัสผ่านหรือบัตรถูกผู้อื่นลักลอบนำไปใช้ แต่ถ้าใช้การตรวจสอบหรือระบุตัวบุคคลด้วยไบโอเมตริกซ์ ทำให้ผู้ใช้ไม่สามารถปฏิเสธความรับผิดชอบได้และช่วยลดค่าใช้จ่าย เช่น ช่วยในการป้องกันพนักงานลงเวลาแทนกัน (Buddy Punching)

2.1.3 ประเภทของไบโอเมตริกซ์

ไบโอเมตริกซ์สามารถแบ่งออกเป็น 2 ประเภทใหญ่ๆ คือ การใช้ลักษณะทางกายภาพ (Physiological Biometrics) และการใช้ลักษณะทางพฤติกรรม (Behavioral Biometrics) ในการระบุตัวบุคคล

- ลักษณะทางกายภาพ (Physiological Biometrics) ได้แก่ ลายนิ้วมือ(Fingerprint), ลักษณะบนใบหน้า (Facial Recognition), ลักษณะของมือ(Hand Geometry) , ลักษณะใบหู(Ear Shape) , Iris และ Retina ภายในดวงตา , กลิ่น(Human Scent)
- ลักษณะทางพฤติกรรม (Behavioral Biometrics) ได้แก่ การพิมพ์(Keystroke Dynamics), การเดิน (Gait Recognition), เสียง(Voice Recognition), การเซ็นต์ชื่อ(Signature)

2.1.4 กระบวนการในการตรวจสอบ หรือระบุตัวบุคคลด้วยไบโอเมตริกซ์

ไม่ว่าจะเป็นการใช้ลักษณะเฉพาะแบบใดก็ตาม จะมีขั้นตอนเหมือนกันดังต่อไปนี้

1. ผู้ใช้ระบบต้องทำการให้ตัวอย่าง (Samples) ของลักษณะทางไบโอเมตริกซ์ที่จะใช้ หรือเป็นการลงทะเบียนเริ่มต้นก่อนที่จะทำการใช้ระบบ
2. ตัวอย่างทางไบโอเมตริกซ์ที่ถูกเก็บมาในขั้นตอนแรกจะถูกทำการแปลง และจัดเก็บให้เป็นแม่แบบ (Template) ที่จะใช้ในการเปรียบเทียบ
3. เมื่อผู้ใช้ต้องการที่จะใช้ระบบก็จะถูกตรวจสอบหรือระบุผู้ใช้ โดยการทำการเก็บตัวอย่างทางไบโอ-เมตริกซ์ของผู้ใช้และทำการเปรียบเทียบกับแม่แบบที่เก็บไว้ แล้วทำการตรวจสอบเหมือนของตัวอย่างกับแม่แบบจากนั้นก็จะทำการอนุญาตหรือปฏิเสธการเข้ามาใช้งานระบบของผู้ใช้

เราเรียกขั้นตอนที่1 และ 2 ว่าเป็นขั้นตอนของการลงทะเบียน (Enrolment) ซึ่งจะเป็นการทำเพียงครั้งเดียว ก่อนการที่จะเริ่มใช้งาน ส่วนที่ 3 เป็นกระบวนการตรวจสอบ (Authentication) หรือ ระบุตัวผู้ใช้ (Identification) ซึ่งผลของการตรวจสอบหรือระบุตัวผู้ใช้นี้มีผลออกมาได้ 4 กรณีดังนี้

1. Correct Accept : อนุญาตให้ผู้ใช้ที่มีสิทธิใช้ระบบ เข้าใช้ระบบได้
2. Correct Reject : ปฏิเสธผู้ที่ไม่มีสิทธิใช้ระบบ

3. False Accept : อนุญาตให้ผู้ที่ไม่มีสิทธิเข้าใช้ระบบ จำนวนของ False Accept ถ้าคำนวณออกมาเป็นเปอร์เซ็นต์ จะเรียกว่า อัตราการอนุญาตผิดพลาด (False Accept Rate หรือ FAR)

4. False Reject : ปฏิเสธผู้ใช้ที่มีสิทธิใช้ระบบไม่ให้เข้าใช้ระบบ จำนวนของ False Reject ถ้าคำนวณออกมาเป็นเปอร์เซ็นต์ จะเรียกว่า(False Reject Rate หรือ FRR)

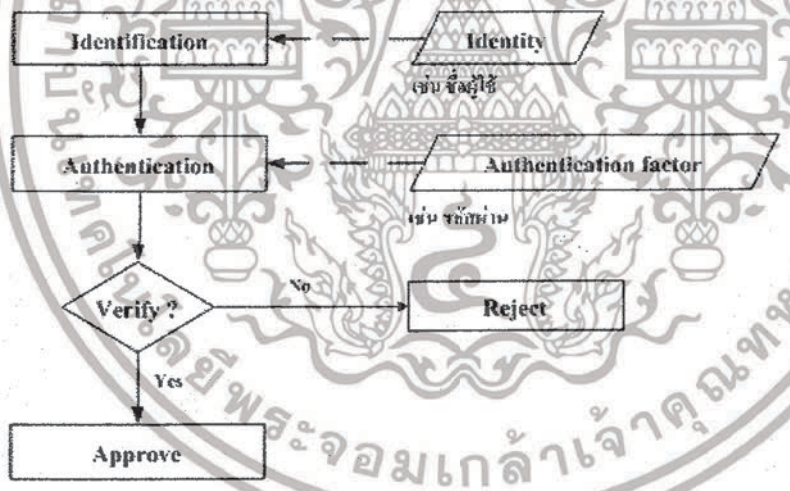
2.2 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

- การระบุตัวตน (Identification) คือขั้นตอนที่ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้ (User Name)

- การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบซึ่งในขั้นตอนนี้คือ การระบุตัวตนและในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ



รูปที่ 2.2 แผนผังแสดงกระบวนการพิสูจน์ตัวตน

หลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด

- Actual identify คือหลักฐานที่สามารถบ่งบอกได้ว่า ในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร
- Electronic identify คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเลคทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้ 3 คุณลักษณะ คือ

1. สิ่งที่คุณมี (Possession factor) เช่น กุญแจหรือเครดิตการ์ด เป็นต้น
2. สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน หรือ การใช้พิน เป็นต้น
3. สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา หรือใช้รูปแบบเสียง เป็นต้น

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้างทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี (Possession factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูง อย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องการลงทุนที่สูง เป็นต้น

ดังนั้นจึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน (Multi-factor authentication) ตัวอย่างเช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกันเช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิตหรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATM เป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูล

ตารางที่ 2.1 ข้อดี – ข้อเสียของการพิสูจน์ตัวตนแต่ละชนิด

การพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
1. ไม่มีการพิสูจน์ตัวตน	- ง่ายต่อการใช้งานและค่าใช้ง่ายต่ำ	- ความปลอดภัยของข้อมูลจะขึ้นอยู่กับผู้ใช้ว่าจะนำข้อมูลเหล่านั้น ไปใช้ในทางที่ควรหรือไม่
2. การพิสูจน์ตัวตนโดยใช้รหัสผ่าน	- สามารถใช้ได้กับทุกระบบ	- จะไม่ปลอดภัยเมื่อมีการส่งข้ามระบบเครือข่ายที่เป็นสาธารณะหรือไม่มีการเข้ารหัสข้อมูล
3. การพิสูจน์ตัวตนโดยใช้ PIN	- ง่ายต่อการจำและความปลอดภัยค่อนข้างดี (บัตร ATM) - สามารถสื่อสารข้ามเครือข่ายสาธารณะได้อย่างปลอดภัย	- ต้องใช้ฮาร์ดแวร์เฉพาะในการอ่าน PIN - ไม่สามารถใช้กับต่างระบบกันได้ - ราคาแพง
4. การพิสูจน์ตัวตนโดยใช้ password authenticators หรือ tokens แบบซิงโครนัส	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่านแบบธรรมดา -ไม่ต้องใช้เครื่องอ่านการ์ด	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - Authenticator เป็นวัตถุซึ่งง่ายต่อการสูญหาย
5. การพิสูจน์ตัวตนโดยใช้ password authenticators หรือ tokens แบบอะซิงโครนัส	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่านแบบธรรมดา - ไม่ต้องใช้เครื่องอ่านการ์ด - เป็นวิธีการป้องกันที่ดีที่สุดเมื่อเปรียบเทียบกับวิธีการใช้การพิสูจน์ตัวตนโดยใช้ password authenticators	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - Authenticator เป็นวัตถุจึงง่ายต่อการสูญเสียและการถูกขโมยได้ ไม่สามารถป้องกันผู้ที่ละเมิดเข้ามาในระบบได้
6. การพิสูจน์ตัวตนโดยวิธี One – Time Password	- ทำให้การเดาหรือขโมยรหัสผ่านเป็นไปได้ยาก	- ไม่สะดวกต่อการใช้งานเพราะผู้ใช้ต้องจำรหัสผ่านหลายตัว - ถ้าผู้ใช้จำรหัสผ่านไม่ได้ หรือทำรหัสผ่านสูญหาย ก็ไม่สามารถเข้าใช้ระบบได้

ตารางที่ 2.1(ต่อ) ข้อดี – ข้อเสียของการพิสูจน์ตัวตนแต่ละชนิด

การพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
7. การพิสูจน์ตัวตนโดยการเข้ารหัสแบบคู่รหัสกุญแจ	- การจัดการกุญแจทำได้ปลอดภัย เพราะการใช้กุญแจในการเข้ารหัสและการถอดรหัสต่างกัน - สามารถระบุใช้ โดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์	- ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก - ต้องใช้ระบบที่สนับสนุนการทำงาน
8. การพิสูจน์โดยการใช้ลายเซ็นต์ดิจิตอล	- สามารถระบุตัวผู้ส่งได้ชัดเจน - ป้องกันข้อมูลถูกแก้ไขระหว่างการส่งได้ หรือสามารถตรวจสอบข้อมูลได้ว่าผ่านการแก้ไขมาหรือไม่	- ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก
9. การพิสูจน์ตัวตนโดยวิธี zero-knowledge proofs	- ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้และเซิร์ฟเวอร์เท่านั้นที่ทราบ	- ความซับซ้อนของระบบเพิ่มขึ้นตามความสามารถของระบบ
10. การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล	- มีความปลอดภัยสูงเพราะเลียบแบบกันได้ยาก	- ระบบมีความซับซ้อนสูง - ยังไม่ได้รับความนิยมกันอย่างแพร่หลาย - ค่าใช้จ่ายสูง

2.3 ลายนิ้วมือ (Fingerprint)

2.3.1 ลายนิ้วมือเกิดขึ้นได้อย่างไร

ผิวหนังบริเวณฝ่ามือและฝ่าเท้าของเราจะมีลักษณะพิเศษ คือ นอกจากจะมีความหนามากกว่าส่วนอื่นแล้ว ก็ยังมีส่วนที่เป็นสัน (Ridge) และส่วนที่เป็นร่อง (Furrow) ซึ่งจะประกอบขึ้นเป็นลวดลายที่ไม่ซ้ำกันเลย ไม่ว่าจะเป็นลายที่บริเวณปลายนิ้ว ฝ่ามือและฝ่าเท้า สันและร่องเหล่านี้จะก่อให้เกิดความฝืด ทำให้เราหยิบจับของได้สะดวกขึ้น

2.3.2 ประวัติของลายนิ้วมือ

คนเรารู้จักใช้ลายนิ้วมือให้เป็นประโยชน์กันมานานแล้ว โดยชาวจีนและชาวอัสซีเรียนจะเป็นกลุ่มแรกที่ใช้รอยพิมพ์ของลายนิ้วมือบนดินเหนียวแทนการเซ็นต์ชื่อทางการค้าขาย

ลายนิ้วมือถูกนำมาใช้เป็นเครื่องมือในการระบุตัวอาชญากรครั้งแรกในแคว้นเบงกอลประเทศอินเดีย โดยตำรวจชาวอังกฤษชื่อ Sir Edward Richard Henry

ในปี พ.ศ.2445 สหรัฐฯ เริ่มใช้ลายนิ้วมือในการจำแนกบุคคล และในปีต่อมาเรือนจำแห่งรัฐนิวยอร์กก็เริ่มการพิสูจน์ยืนยันตัวผู้ต้องขังโดยใช้ลายนิ้วมือ

2.3.3 ความรู้เบื้องต้นของลายนิ้วมือ

บริเวณปลายนิ้วมือของมนุษย์โดยทั่วไป จะเห็นลายนิ้วมือที่มีลักษณะประกอบไปด้วยเส้น 2 ลักษณะ คือ เส้นนูน (Ridges) และ เส้นร่อง (Furrows) ซึ่งเส้นทั้ง 2 ลักษณะจะอยู่สลับกันไปตลอด

- จุดลักษณะสำคัญบนลายนิ้วมือ (Characteristics) คือ ตำหนิต่างๆบนลายนิ้วมือ สามารถแบ่งได้เป็น 2 ลักษณะ ดังนี้

1. ตำหนิและลักษณะต่างๆของลายเส้นทั่วไป เช่น เส้นตรง เส้นโค้ง จุด เส้นแตก เส้นวกกลับ เส้นขาด เส้นทะเลสาบ เส้นหักมุม

2. ลักษณะพิเศษบางอย่าง เช่น

- ไบฟูร์เคชั่น คือ เส้นขอบหนึ่งที่ได้ถูกแยกออกเป็น 2 เส้นหรือมากกว่า 2 เส้น
- ไดเวอร์เจนซ์ คือ เส้นขอบที่วิ่งขนานกันมาหรือเกือบจะขนานและได้แยกถ่างออกไป
- จุดมินูเทีย (Minutiae) คือ จุดปลายเส้นหยุดหรือเส้นแยก

- คำจำกัดความที่สำคัญบนลายนิ้วมือ

เป็นการอธิบายคุณลักษณะหลักสำคัญใหญ่ๆที่ต้องการศึกษาและทำความเข้าใจเพราะมีคุณประโยชน์ที่แสดงให้เห็นถึงความแตกต่างของแต่ละลายนิ้วมือซึ่งมีอยู่ 4 ข้อ ได้แก่

เส้นขอบ (Type line) เส้นคู่ขนานคู่ในสุดซึ่งได้คู่กันมาพอสมควร แล้วแยกออกเพื่อจะโอบล้อมบริเวณลายพิมพ์ที่อยู่ภายใน เส้นขอบไม่จำเป็นต้องเป็นเส้นยาว อาจจะเป็นเพียงเส้นสั้นๆ ที่คู่ขนานกันมาแล้วแยกออก เส้นแตกจะเป็นเส้นขอบไม่ได้ เว้นแต่เส้นแตกนั้นได้แตกออกมาแล้วขนานกันพอสมควรและแยกออกเพื่อโอบล้อมรูปลักษณะในลายนิ้วมือ

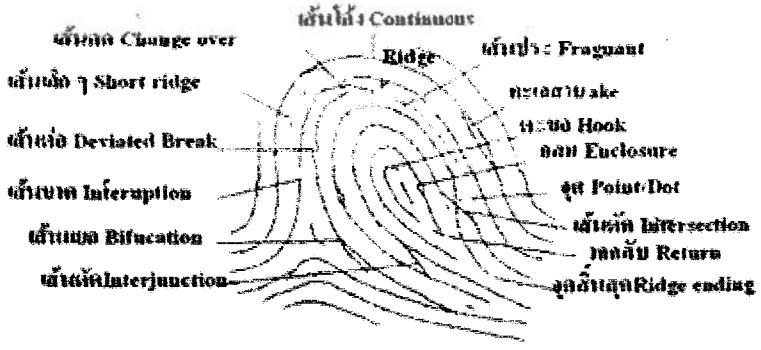
สันดอน (Delta) คือ ลายเส้นในลายนิ้วมือซึ่งอยู่ตรงหน้าและใกล้ที่สุดกับกึ่งกลางของปากทางแยกของเส้นขอบ หรือเกือบกึ่งกลางของปากทางแยกของเส้นขอบ สันดอนอาจเป็นจุด เส้นแตก ปลายเส้น เส้นสอง เส้นที่มาพบกันหรือเส้นหักมุม หรือจุดใดจุดหนึ่งบนเส้น

ใจกลาง (Core) คือ เป็นส่วนที่ใช้อธิบายถึงลักษณะที่ช่วยให้สังเกตเห็นคุณสมบัติโดยทั่วไปของภาพที่ทำการบันทึก ที่อยู่ในลักษณะของลายนิ้วมือที่มีลักษณะเป็นเส้นโค้ง ซึ่งเป็นส่วนที่สำคัญที่จะเป็นตัวยืนยัน หรือข้อมูลสำคัญในการตรวจสอบว่าเป็นคนๆนั้น หรือเฉพาะบุคคลไป บริเวณลายนิ้วมือที่อยู่ภายใน (Pattern Area) คือ พื้นที่บริเวณภายในลายนิ้วมือที่ถูกเส้นขอบโอบล้อม

2.4 วิธีวิเคราะห์ลายนิ้วมือ

สำหรับคนๆหนึ่ง รูปแบบลายนิ้วมือจะคงเดิมตั้งแต่ตอนเกิดไม่มีการเปลี่ยนแปลง มีเพียงการเปลี่ยนแปลงเล็กน้อยที่ยอมรับและอธิบายได้ ได้แก่ การยืดขยายของผิวหนัง เมื่อร่างกายโตขึ้น คาบสกปรกติดลายนิ้วมือ รอยขูดขีดและรอยแผลจากอุบัติเหตุต่างๆ

ผิวหนังบริเวณปลายนิ้วมือประกอบด้วยลาย 2 ชนิด คือ เส้นนูน และ เส้นร่อง จะอยู่สลับกันตลอดไป โดยถ้าใช้หมึกสีดำทาบนนิ้วมือแล้วกดนิ้วมือลงบนกระดาษขาวจะได้ลายเส้นสีดำและขาวสลับกัน เรียกเส้นสีดำว่าเส้นนูน เรียกเส้นสีขาวว่าเส้นร่อง เราสามารถแยกลักษณะของลายนิ้วมือที่เป็นจุดสำคัญต่างๆดังนี้

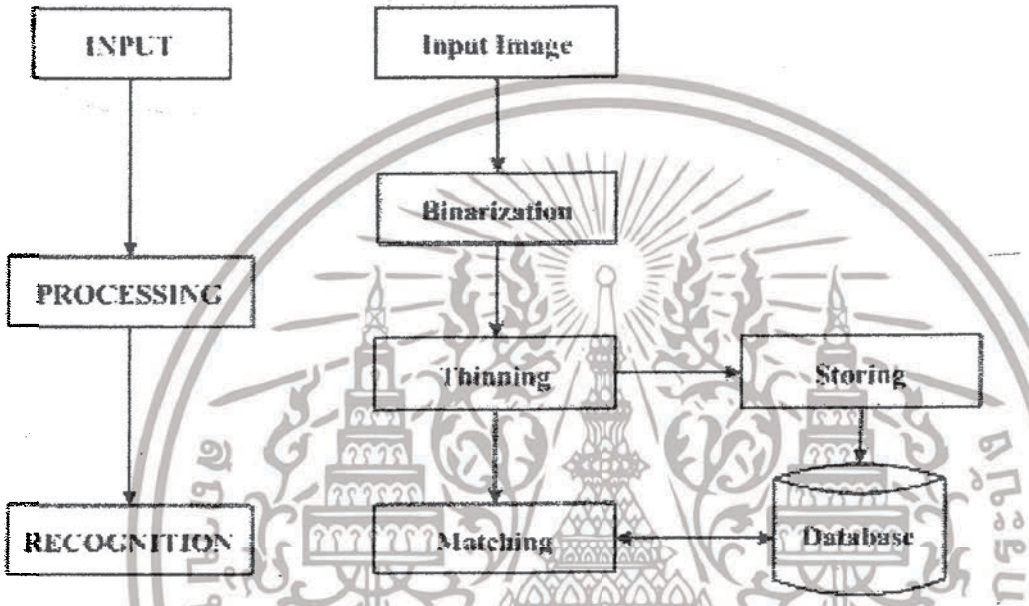


รูปที่ 2.3 ส่วนประกอบของลายนิ้วมือ

เนื่องจากลายนิ้วมือของคนเราโดยทั่วไปจะมีจุด Core และจุด Delta เป็นจุดสำคัญอยู่บนลายนิ้วมือซึ่งสามารถนำมาใช้ประโยชน์ได้ในการวิเคราะห์ ซึ่งในคนเราโดยทั่วไปจะมีจุดสำคัญในแต่ละนิ้วเป็นร้อยๆจุด แต่การที่จะยืนยันว่าลายนิ้วมือนั้นเป็นของใครนั้นใช้แค่ 8-10 จุดก็เพียงพอแล้ว

2.4.1 การศึกษากระบวนการรู้จำลายนิ้วมือ

กระบวนการในการรู้จำลายนิ้วมือจะประกอบไปด้วยกระบวนการต่างๆดังนี้



รูปที่ 2.4 ขั้นตอนการรู้จำลายนิ้วมือ

- กระบวนการรับภาพ

ลายนิ้วมือที่จะถูกพิจารณาจะถูกอ่านเข้าสู่ระบบ โดยผ่านอุปกรณ์อินพุท ซึ่งอาจทำได้ 2 วิธี วิธีแรกใช้หมึกพิมพ์ลายนิ้วมือลงบนวัสดุ เช่น กระดาษหรือแผ่นพลาสติก แล้วจึงใช้เครื่องสแกนเนอร์ที่มีความละเอียดสูงอ่านค่าเข้าไป และวิธีที่สอง ใช้เครื่องอ่านลายนิ้วมือโดยเฉพาะ อ่านลายนิ้วมือเข้าสู่ระบบ 256 ระดับสีเทา

- กระบวนการเบื้องต้น (Preprocessing)

การปรับข้อมูลภาพให้เป็นข้อมูลสองระดับ

เนื่องจากข้อมูลภาพที่รับเข้ามาสู่ระบบนั้นเป็นข้อมูลดิจิตอล 256 ระดับสีเทานั้นจะถูกนำมาแปลงให้เป็นข้อมูลภาพสองระดับ (Binary image) ซึ่งวิธีในการแปลงข้อมูลภาพนั้นมีการใช้ฟังก์ชั่นในการแปลงหลากหลายฟังก์ชั่น เช่น

$$g(x,y) = \begin{cases} 1, f(x,y) > t \\ 0, f(x,y) \leq t \end{cases}$$

เมื่อ $g(x,y)$ คือข้อมูลภาพลายนิ้วมือที่เป็นระดับสีเทา

t คือ ค่า Threshold

- ขั้นตอนวิธีการทำให้ภาพบาง

เป็นขั้นตอนที่ลดขนาดลายเส้นของภาพลายนิ้วมือ เพื่อให้ทราบถึงโครงสร้างที่แท้จริงของลายนิ้วมือ จึงต้องมีการปรับลายเส้นให้เหลือเพียงเส้นขนาด 1 จุดภาพ ซึ่งมีด้วยกันหลายวิธีซึ่งในที่นี้ไม่ขอกล่าวถึง

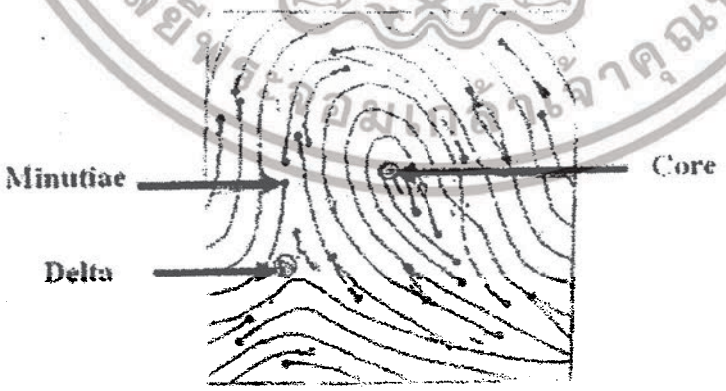
รูปที่ 2.5 ซ้าย : ภาพลายนิ้วมือก่อนการทำ thinning
ขวา : ภาพที่ได้จากการทำ thinning

- ลักษณะการทำงานของระบบ AFIS (Automated Fingerprint Identification System)

ระบบ AFIS จะค้นหาจุดสำคัญบนลายนิ้วมือ และหาความสัมพันธ์ระหว่างจุดต่างๆเหล่านั้นซึ่งจุดสำคัญดังกล่าว จะหาได้จากตำแหน่งของลายเส้นที่เป็น "จุดปลาย" หรือ "จุดแยก" โดยอาศัยหลักการ"ความสัมพันธ์" หรือ "Relation" นั่นเอง

ส่วนประกอบสำคัญของลายพิมพ์นิ้วมือที่ใช้วิธีประมวลผลด้วยเครื่องคอมพิวเตอร์

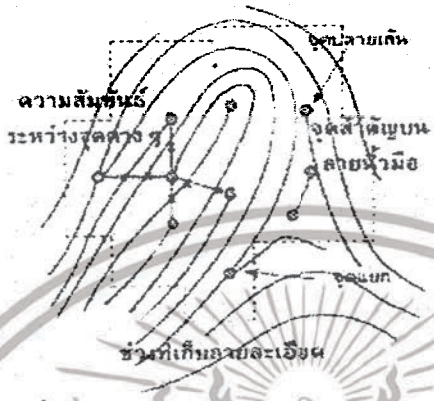
1. ประเภทของลายนิ้วมือหรือ Pattern Type คือ โค้ง มัดหวาย ก้นหอย
2. จุดใจกลางของลายพิมพ์นิ้วมือหรือ Core
3. จุดนัยสำคัญ Minutiae
4. สันดอน Delta



รูปที่ 2.6 ภาพแสดงจุด Core จุด Delta และจุด Minutiae

การที่ AFIS ใช้หลักค้นหา "จุดสำคัญ" แทนการจำภาพลายนิ้วมือทั้งหมดนั้น เนื่องจากการจำภาพลายนิ้วมือทั้งหมดเป็นการจำที่ค่อนข้างยาก และลายนิ้วมือเดียวแต่มาพิมพ์คนละครั้ง อาจให้ผลไม่เหมือนกัน บางคนอาจเอียงซ้ายหรือเอียงขวา ความหนักเบาของการพิมพ์ การจดจำลายเส้นก็จะผิดพลาดได้มากขึ้น

การใช้เทคโนโลยีมาพิสูจน์ลายนิ้วมือ จะใช้วิธีหาจุดสำคัญบนลายนิ้วมือ 2 จุดเท่านั้น คือ จุดปลาย เส้นลายนิ้วมือคนเราจะประกอบด้วยเส้นมากมาย จะมีบางเส้นที่วิ่งๆมาก็หยุดหายไปเลย จุดปลายจุดนี้จึงเป็นจุดที่สำคัญจุดหนึ่ง "จุดแยก" หรือ ตัว "Y" เพราะมีแค่ 1 เส้น แต่แยกเป็น 2 เส้น ซึ่งจุดนี้จะมีอยู่ในทุกคน อยู่ที่แต่ละคนจะอยู่ตำแหน่งไหนเท่านั้นเอง เมื่อหาจุดสำคัญบนลายนิ้วมือได้แล้ว ก็จะสร้างความสัมพันธ์ของแต่ละจุดเข้าด้วยกัน ดังรูปที่ 2.7

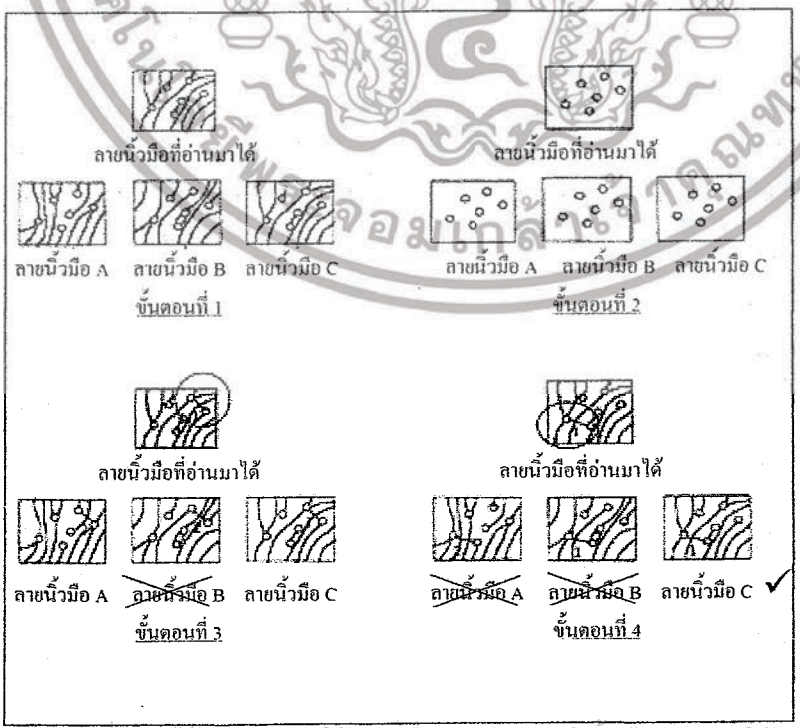


รูปที่ 2.7 แสดงความสัมพันธ์ระหว่างจุดต่างๆ

ตัวอย่างในรูปที่2.8 (ขั้นตอนที่1) เปรียบเทียบลายนิ้วมือที่เก็บมาได้กับลายนิ้วมือที่ได้บันทึกไว้ในฐานข้อมูลซึ่งสมมุติว่าเป็นลายนิ้วมือของผู้ใช้งานที่มีอยู่ในคอมพิวเตอร์ จะเห็นว่าลายนิ้วมือ A B C ที่ค้นพบจะไม่เหมือนกัน

คอมพิวเตอร์ก็ใช้หลักการจับลักษณะจุดสำคัญของลายนิ้วมือที่มีในฐานข้อมูล จากนั้นเครื่องจะทำการตรวจสอบว่าระหว่างจุดแต่ละจุด มีเส้นอยู่ระหว่างจุดที่สนใจกี่เส้น ซึ่งพบว่ามีเส้นอยู่ระหว่างจุดที่สนใจอยู่ 1 เส้น เพราะฉะนั้น ก็จะรู้ได้ทันทีว่า B ไม่ใช่ลายนิ้วมือที่ถูกต้อง

หลังจากทดสอบ ขั้นที่ 2 จะเหลือผู้ใช้งานที่เป็นไปได้อยู่ 2 คน ก็จะตรวจไปเรื่อยๆ จุดที่สนใจของ A มีเส้นอยู่ระหว่าง 2 เส้น C มีอยู่เส้นเดียว เพราะฉะนั้น C จึงเป็นลายนิ้วมือที่ถูกต้อง



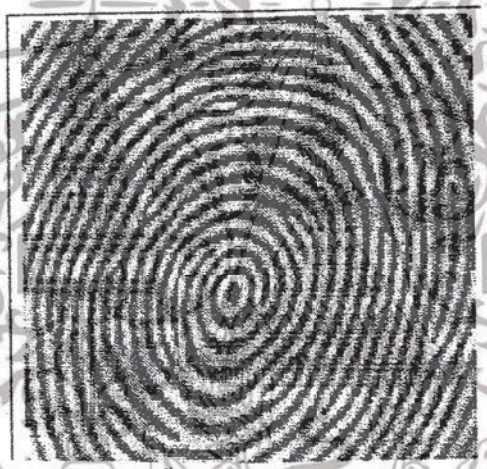
รูปที่ 2.8 ขั้นตอนการเปรียบเทียบลายนิ้วมือ

2.4.2 กระบวนการเปรียบเทียบลายนิ้วมือ

จากทฤษฎี Automated Fingerprint Identification System (AFIS) มีหลักการคือ ระบบ AFIS จะตรวจสอบและค้นหาจุดสำคัญบนลายนิ้วมือ และหาความสัมพันธ์ระหว่างจุดต่างๆเหล่านั้น

รูปที่ 2.9 แสดงกระบวนการวิเคราะห์ลายนิ้วมือ

วิธีการเปรียบเทียบนี้เริ่มจากการรับข้อมูลลายนิ้วมือจากอุปกรณ์สแกนลายนิ้วมือ โดยรูปที่ได้จากอุปกรณ์สแกนลายนิ้วมือจะประกอบไปด้วยอัตราของสีที่ไม่สม่ำเสมอ ดังนั้นก่อนส่งรูปภาพนี้ไปเก็บในไลบรารีของการพิสูจน์ตนจะต้องทำการกรองรูปภาพ (Filter) ก่อน



รูปที่ 2.10 แสดงลายนิ้วมือที่ได้จากอุปกรณ์สแกนลายนิ้วมือ

การกรองรูปภาพที่ได้รับมาจากการสแกนลายนิ้วมือนั้น เป็นการทำให้รูปภาพมีขอบเขตของสีอยู่ระหว่างช่วงสีดำ – สีขาว (0-255) โดยจะทำให้รูปภาพที่มีสีเทาเข้มกลายเป็นสีดำ และสีเทาอ่อนกลายเป็นสีขาว กระบวนการกรองรูปภาพมีรายละเอียดดังนี้

ถ้าเป็นสีขาวหรือสีเทาอ่อน จะพิจารณาให้เป็นขอบนอกของลายนิ้วมือ และแปลงเป็นสีขาวจำนวนสีที่เกิดขึ้นในแต่ละโทนสีเทาในลายนิ้วมือจะถูกบันทึกไว้ โดยสีเทาที่เข้มที่สุดถูกพิจารณาให้เป็นเสมือนสันเขา (Ridges) และสีเทาที่อ่อนที่สุดเปรียบเสมือนหุบเขา (Valleys) ความแตกต่างระหว่างสันเขากับหุบเขาถูกคำนวนและแบ่งครึ่ง โดยค่าของสีเทาที่เข้มกว่าสีดำ(0) จนถึงค่าที่น้อยกว่าสีเทาที่เข้มที่สุดที่เป็นแนวสันเขาบวกกับค่าความแตกต่างจะต้องเปลี่ยนเป็นสีดำทั้งหมด แล้วสีเทาที่เข้มกว่าแนวหุบเขาจนถึงค่าที่เทาอ่อนบวกกับค่าความแตกต่างจะต้องเปลี่ยนเป็นสีขาวดังสมการ

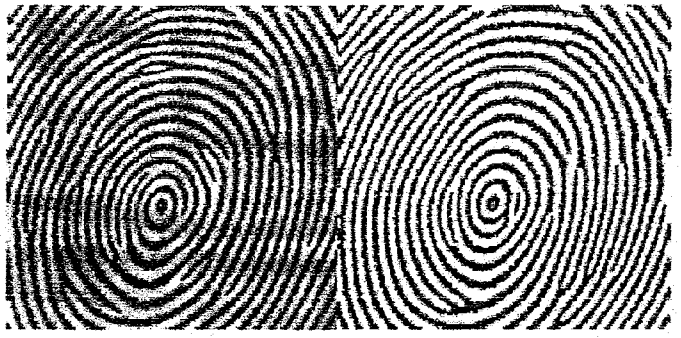
l = สีเทาที่เข้มที่สุด

d = สีเทาที่เข้มน้อยที่สุด

x = (l-d)/2

Ridges = 0<= l <= (l+x)

Valleys = (l+x)< d <= 255



รูปที่ 2.11 แสดงลายนิ้วมือก่อนและหลังการทำการกรอง

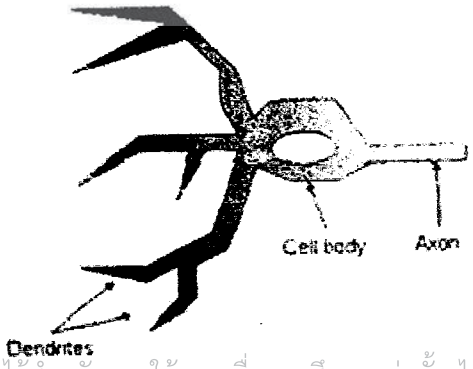
หลังจากที่ได้รูปที่ผ่านกระบวนการกรองออกมาแล้ว ก็นำรูปภาพนั้นไปทำการเปรียบเทียบและวิเคราะห์ โดยการเปรียบเทียบจะพิจารณาในส่วนของสันเขาและหุบเขา การค้นหานั้นเริ่มต้นด้วยการเลือกจุดเริ่มต้น และทำการพิจารณาไปตามแนวสันเขาจนกระทั่งพบจุดปลายของรูปแบบลายนิ้วมือแบบ Bifurcation หรือ Ridge Ending ก็จะทำเครื่องหมายเอาไว้ว่าอยู่ตำแหน่งพิกัด (x,y) ที่เท่าไหร่ โดยกระบวนการเช่นนี้จะทำไปเรื่อยๆ จนกระทั่งหมดทั้งรูปภาพ จากนั้นพิจารณาพิกัด x,y ที่ได้ออกมาเพื่อนำไปเปรียบเทียบกับข้อมูลที่เก็บไว้ว่าตรงกันหรือไม่ ในการเปรียบเทียบนั้นจะทำการหมุนภาพลายนิ้วมือที่ได้มาใหม่จนกระทั่งพบว่ามันถูกต้องตรงกันหรือเกิดความล้มเหลวในการเปรียบเทียบ โดยอัตราการเปรียบเทียบนั้นจะเปรียบเทียบภายใน 30 พิกเซลต้องมีอย่างน้อย 20 พิกเซลขึ้นไปที่ถูกต้องตรงกันจึงสามารถบอกได้ว่าถูกต้อง

2.5 โครงข่ายประสาทเทียม (Neural Network)

เครื่อข่ายประสาทเทียม คือ โมเดลทางคณิตศาสตร์สำหรับประมวลผลสารสนเทศ เพื่อจำลองการทำงานของเครือข่ายประสาทในสมองมนุษย์ให้มีความสามารถในการเรียนรู้การจดจำรูปแบบ (Pattern Recognition) และการอุปมาความรู้ (Knowledge deduction) เช่นเดียวกับความสามารถที่มีในสมองมนุษย์

- โครงข่ายประสาทในสมองมนุษย์

ในสมองมนุษย์ ประกอบด้วย เซลล์ประสาท หรือ “นิวรอน” และจุดประสานประสาท (Synapses) แต่ละเซลล์ประสาทประกอบด้วยปลายในการรับกระแสประสาท เรียกว่า เดนไดรท์ (Dendrite) ซึ่งเป็น input และปลายในการส่งกระแสประสาทเรียกว่า แอคซอน (Axon) ซึ่งเป็นเหมือนoutput ของเซลล์ เซลล์เหล่านี้ทำงานด้วยปฏิกิริยาไฟฟ้าเคมี เมื่อมีการกระตุ้นด้วยสิ่งเร้าภายนอกหรือกระตุ้นด้วยเซลล์ด้วยกัน กระแสประสาทจะวิ่งผ่านเดนไดรท์เข้าสู่นิวเคลียสซึ่งจะเป็นตัวตัดสินว่าต้องกระตุ้นเซลล์อื่นๆต่อไปหรือไม่ ถ้ากระแสประสาทแรงพอนิวเคลียสก็จะกระตุ้นเซลล์อื่นๆต่อไปผ่านทางแอคซอนของมัน ตามโมเดลนี้ข่ายงานประสาทเกิดจากการเชื่อมต่อระหว่างเซลล์ประสาท จนเป็นเครือข่ายที่ทำงานร่วมกัน

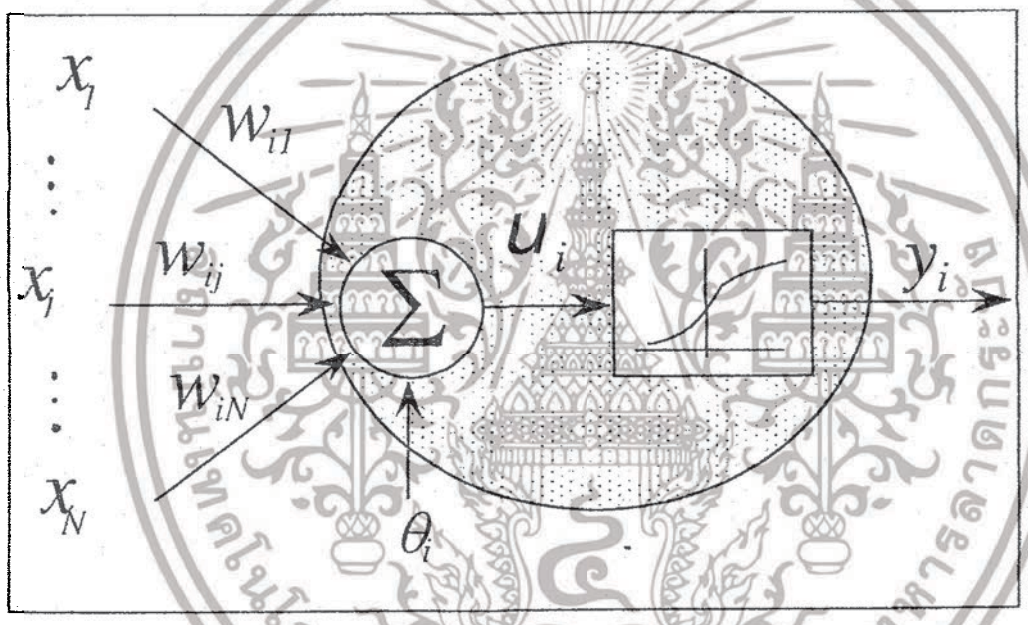


รูปที่ 2.12 แสดง Model ของ Neuron ในสมองมนุษย์

- โครงข่ายประสาทเทียม

โครงข่ายประสาทเทียมหรือที่เรียกกันว่า Artificial Neural Network (ANN) เป็นแบบจำลองแบบหนึ่งในแขนงของงานวิจัยทางด้านปัญญาประดิษฐ์หรือ Artificial Intelligence (AI) โดยมีการอ้างอิงมาจากการทำงานของเซลล์ประสาทในสมองของมนุษย์ แต่ในโครงข่ายของเซลล์ประสาทในสมองของมนุษย์จริง มีขั้นตอนการทำงานที่ซับซ้อนกว่ามาก แต่กระนั้น ANN ก็ยังสามารถที่จะนำมาใช้ประโยชน์ได้จริงในงานด้านวิทยาการคอมพิวเตอร์และวิศวกรรมโดยทั่วไป

ในสมองของมนุษย์นั้นจะประกอบไปด้วยเซลล์ประสาทหรือ Neuron ประมาณ 10^{11} ตัว โดยที่เซลล์ประสาทหนึ่งๆ จะมีการเชื่อมโยงต่อไปยังเซลล์ประสาทอื่นๆอีกประมาณ 10^{4} ตัวและเวลาที่ใช้ในการแลกเปลี่ยนข้อมูลระหว่าง Neurons นั้นจะอยู่ในหลัก 10^{-3} วินาที โดยการทำงานของ Neurons ในสมองมนุษย์นั้นจะมีลักษณะการประมวลผลแบบขนานขั้นสูงอีกด้วย (Highly Parallel Processing) จึงทำให้มนุษย์สามารถทำการเรียนรู้และจดจำหน้าแม่ของตัวเองได้ภายในเวลาเพียงไม่กี่วินาที



รูปที่ 2.13 แสดงโครงสร้างของเครือข่ายประสาทเทียม

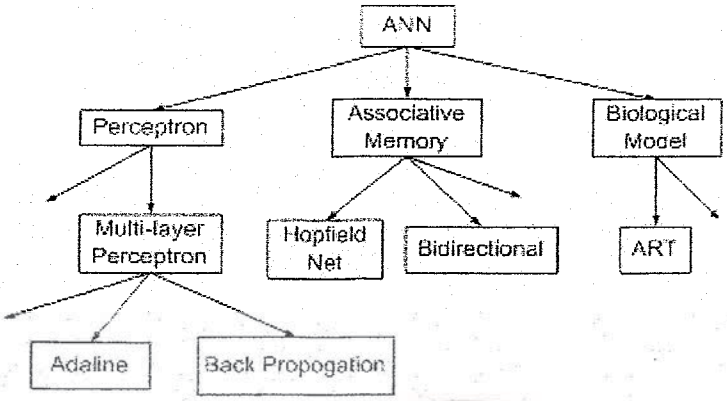
เป้าหมายหลักของการนำเอา ANN มาใช้ในงานด้านวิศวกรรมและวิทยาการคอมพิวเตอร์นั้นคือการพัฒนากระบวนการเรียนรู้ของเครื่องจักรหรือที่เรียกกันว่า Machine Learning ให้มีประสิทธิภาพสูง การนำ ANN มาใช้งานแบ่งเป็น 2 ขั้นตอนหลัก คือ ขั้นตอนการฝึกหัด(Training) หรือเรียนรู้(Learning) และขั้นตอนการทดสอบ(Testing) หรือใช้งานจริง(working) โดยในขั้นตอนของการ Training นั้นยังสามารถแบ่งออกได้เป็น 2 กลุ่มหลักคือ

1. การเรียนรู้แบบมีครูสอน (Supervised Learning Algorithm)
2. การเรียนรู้แบบไม่มีครูสอน (Unsupervised Learning Algorithm)

แบบจำลองของ ANN ที่ได้รับความนิยมสามารถจำแนกออกได้เป็น 3 กลุ่มใหญ่ ดังนี้ คือ

1. Perceptron
2. Associative Memory
3. Biological Model

โดยสามารถแบ่งย่อยลงไปได้อีกดังในรูปที่ 2.14



รูปที่ 2.14 แสดงแบบจำลองหลักๆ ของ ANN

2.6 ฟิงเกอร์พริ้นต์เซนเซอร์ และบอร์ดควบคุม FDA01

รูปที่ 2.15 ฟิงเกอร์พริ้นต์เซนเซอร์และบอร์ดควบคุม FDA01

เป็นบอร์ดควบคุมซึ่งมีหน้าที่ควบคุมการทำงานต่างๆ และจัดการกับข้อมูลลายนิ้วมือที่ได้จากเซนเซอร์ ทั้งในส่วนของการรู้จำลายนิ้วมือ และการจัดเก็บข้อมูลในรูปของเท็มเพลตลงยังหน่วยความจำแบบแฟลชที่อยู่บนบอร์ดเอง

2.6.1 คุณสมบัติโดยทั่วไปของฟิงเกอร์พริ้นต์เซนเซอร์ และบอร์ดควบคุม FDA01 มีดังนี้

- ฟิงเกอร์พริ้นต์เซนเซอร์รุ่น OPP01 เป็นเซนเซอร์แบบ Optical CMOS Image Sensor
- ความละเอียดของภาพ (Resolution) จากฟิงเกอร์พริ้นต์เซนเซอร์เท่ากับ 500 จุดต่อนิ้ว(DPI)
- เท็มเพลตของข้อมูล (Data Template) ที่ใช้ในระบบมีขนาด 400-800 ไบต์
- ความสามารถในการบันทึกข้อมูลของผู้ใช้แปรตามขนาดความจุของข้อมูลของหน่วยความจำแบบแฟลต (Flash Memory) บนบอร์ดควบคุมของฟิงเกอร์พริ้นต์เซนเซอร์
- ขนาด 1 เมกะไบต์ สามารถเก็บข้อมูลเท็มเพลตข้อมูลของผู้ใช้ได้ 720 ราย
- ขนาด 2 เมกะไบต์ สามารถเก็บข้อมูลเท็มเพลตข้อมูลของผู้ใช้ได้ 2000 ราย
- ขนาด 4 เมกะไบต์ สามารถเก็บข้อมูลเท็มเพลตข้อมูลของผู้ใช้ได้ 4560 ราย

-สามารถบันทึกเหตุการณ์ต่างๆที่เกิดขึ้นกับระบบ (เช่น เกิดการสแกนลายนิ้วมือขึ้นเมื่อไร ผู้ที่ผ่านเข้าออกระบบเป็นใคร เป็นต้น) ได้ 8192 รายการ

- กำหนดจำนวนผู้มีสิทธิพิเศษในการเข้าไปเปลี่ยนแปลงข้อมูล 5 คน

- เวลาที่ใช้การตรวจสอบลายนิ้วมือน้อยกว่า 1 วินาที

- ทำงานที่แรงดันไฟเลี้ยง 5 โวลต์กินกระแสไฟฟ้า 270 มิลลิแอมป์

2.6.2 จุดเด่นของบอร์ดควบคุม FDA01: firmware version 1.3M

- สามารถบันทึกลายนิ้วมือจาก 2 นิ้ว สำหรับทนตัวผู้ใช้แต่ละราย

- มุมในการวางนิ้วบนเซนเซอร์ เพื่ออ่านข้อมูลในเวอร์ชันเดิมๆ จะสามารถทำมุมได้ไม่เกิน 15 องศา แต่สำหรับเวอร์ชันนี้จะสามารถวางนิ้วมือบนผิวตรวจสอบของฟิงเกอร์พริ้นต์เซนเซอร์ทำมุมได้ถึง 360 องศา

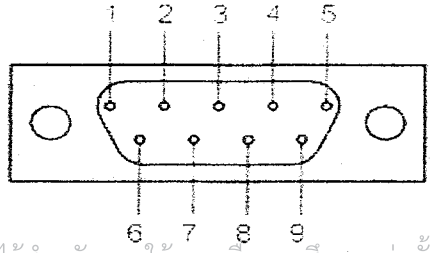
- ความเร็วได้การค้นหาและเปรียบเทียบข้อมูลน้อยกว่าเวอร์ชันเก่า

2.7 มาตรฐานพอร์ทอนุกรมแบบ RS – 232

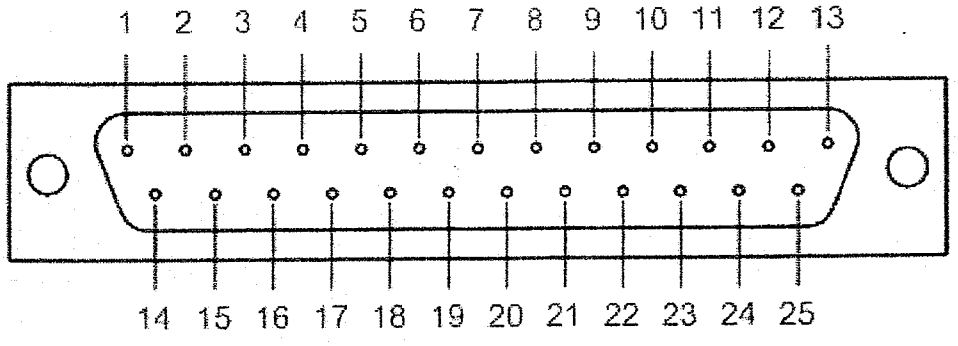
มาตรฐานการเชื่อมต่อแบบ RS – 232 เป็นมาตรฐานอุตสาหกรรมที่ออกแบบมาเพื่อใช้ในการส่งข้อมูลอนุกรมแบบอะซิงโครนัส 2 ทิศทาง โดยมาตรฐาน RS – 232 ในอดีตนั้นถูกออกแบบมาเพื่อการส่งผ่านข้อมูลจากคอมพิวเตอร์ไปยังโมเด็มเพียงอย่างเดียว เพื่อที่จะนำข้อมูลจากโมเด็มนี้สื่อสารผ่านสายโทรศัพท์ไปยังคอมพิวเตอร์อีกชุดซึ่งอยู่ห่างไกลกัน โดยคณะกรรมการที่เรียกว่าสมาคมอุตสาหกรรมอิเล็กทรอนิกส์ (Electronic Industries Association : EIA) ได้วางมาตรฐานที่มีชื่อเรียกกันว่า EIA RS-232 มาตรฐานนี้ในช่วงแรกจะใช้คอนเน็กเตอร์เป็นแบบดีบีเก้าสิบห้า (DB-25) โดยกำหนดความยาวของสายสัญญาณไว้ที่ 50 ฟุต มีระดับสัญญาณตั้งแต่ -3 ถึง -15 โวลท์ แสดงว่ามีข้อมูล(Mark) และ +3 ถึง +15 แสดงว่าเป็นช่องว่าง (Space)

มาตรฐาน RS – 232 ได้กำหนดรูปแบบของอุปกรณ์เชื่อมต่อข้อมูลไว้ว่าอุปกรณ์ DTE จะต้องเป็นอุปกรณ์ที่มีการประมวลผลในตัว เช่น ไมโครคอนโทรลเลอร์ หรือ ไมโครคอมพิวเตอร์ ซึ่งมีความสามารถในการสร้างบิตข้อมูลอนุกรมได้ ส่วนอุปกรณ์ DCE จะทำหน้าที่เป็นเพียงตัวรับข้อมูลที่ส่งมาจาก DTE เท่านั้น โดยการรับส่งข้อมูลระหว่างอุปกรณ์ทั้งสองจะกระทำผ่านมาตรฐาน RS – 232 ข้อแตกต่างของอุปกรณ์ DTE และอุปกรณ์ DCE คือ คอนเน็กเตอร์ของ DTE จะเป็นตัวผู้ ส่วนคอนเน็กเตอร์ของ DCE จะเป็นตัวเมีย ซึ่งพอร์ตอนุกรมของคอมพิวเตอร์ที่ใช้กันอยู่ทั่วไปจะเป็นแบบ DTE ส่วนคอนเน็กเตอร์ที่อยู่ที่โมเด็มจะเป็นแบบ DCE

สำหรับการใช้งานบนคอมพิวเตอร์พอร์ทอนุกรม RS – 232 มักถูกใช้เชื่อมต่อกับโมเด็ม หรือ เมาส์ โดยสามารถรับส่งข้อมูลได้ที่ความยาวของสายสัญญาณสูงสุดถึง20 เมตรและคอนเน็กเตอร์สำหรับพอร์ทRS–232 จะใช้คอนเน็กเตอร์แบบ DB – 25 ตัวผู้ หรือ DB – 9 ตัวผู้ซึ่งคอนเน็กเตอร์แบบ DB – 25 จะมีขาต่อใช้งานเพียง 9 เส้น เช่นเดียวกับคอนเน็กเตอร์แบบ DB – 9 เนื่องจากขาอื่นๆ ที่เคยใช้งานในอดีต ปัจจุบันมีการใช้งานไม่มากนัก จึงถูกยกเลิกไปโดยแสดงรูปร่างและตำแหน่งขา ดังรูปที่ 2.16



(ก) คอนเน็กเตอร์อนุกรม 9 ขา หรือแบบ DB – 9 (มองจากด้านหลังคอมพิวเตอร์)

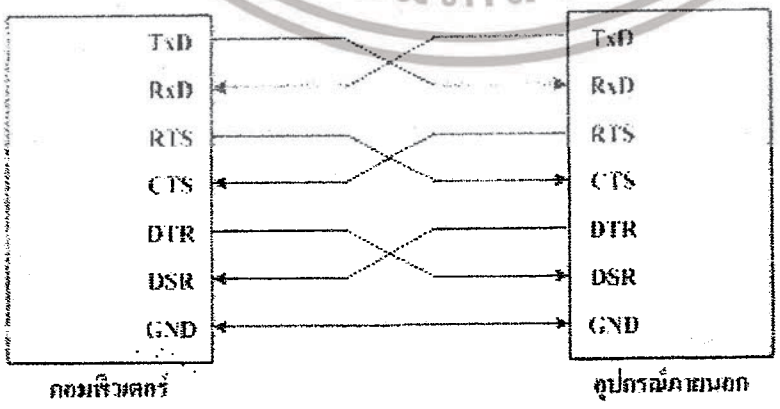


(ข) คอนเน็กเตอร์อนุกรม 25 ขา หรือแบบ DB – 25 (มองจากด้านหลังคอมพิวเตอร์)

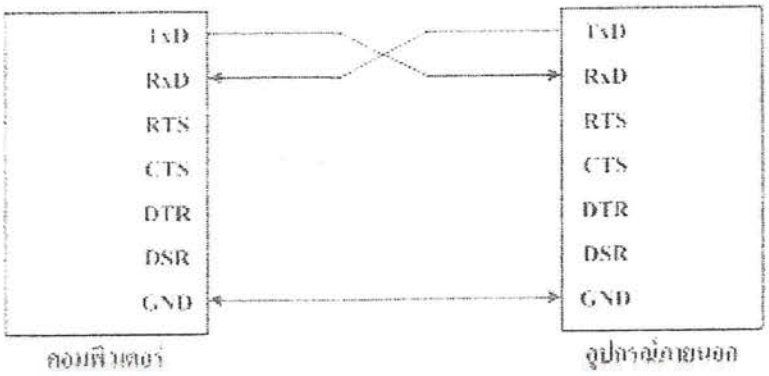
รูปที่ 2.16 การจัดขาของคอนเน็กเตอร์พอร์ทอนุกรมตามมาตรฐาน RS – 232
ทั้งแบบ (ก)DB – 9 และ (ข)DB – 25

ตารางที่ 2.2 แสดงตำแหน่งและชื่อขาของ DB – 9 และ DB – 25

คอนเน็กเตอร์ DB - 9	คอนเน็กเตอร์ DB - 25	ชื่อของสายสัญญาณ	ชนิดของสายสัญญาณ
1	8	Data Carrier Detect : DCD	อินพุต
2	3	Received Data : RxD	อินพุต
3	2	Transmitted Data : TxD	เอาท์พุต
4	20	Data Terminal Ready : DTR	เอาท์พุต
5	7	Signal Ground : GND	
6	6	Data Set Ready : DSR	อินพุต
7	4	Request To Send : RTS	เอาท์พุต
8	5	Clear To Send : CTS	อินพุต
9	22	Ring Indicator : RI	อินพุต



(ก) การต่ออุปกรณ์ภายนอกเข้ากับคอมพิวเตอร์แบบนัลโมเด็ม (Null modem)



(ข) การต่ออุปกรณ์ภายนอกเข้ากับคอมพิวเตอร์แบบ RS – 232 โดยใช้สายสัญญาณเพียง 3 เส้น

รูปที่ 2.17 การต่ออุปกรณ์ภายนอกกับพอร์ตอนุกรมของคอมพิวเตอร์ในลักษณะต่างๆ

สำหรับการเชื่อมต่อคอมพิวเตอร์กับอุปกรณ์ภายนอกดังในรูปที่ 2.10 ลูกศรในรูปแสดงถึงทิศทางของข้อมูล ในรูปที่ 2.17 (ก) เป็นการเชื่อมต่อแบบนัลโมเด็ม (Null modem) หรือการเชื่อมต่อโดยตรง โดยไม่ต้องผ่านโมเด็ม โดยมีการตรวจสอบหรือแฮนด์เช็กเต็มรูปแบบ ส่วนในรูปที่ 2.17 (ข) เป็นการเชื่อมต่อแบบนัลโมเด็ม ในลักษณะที่ใช้สายสัญญาณเพียง 3 เส้น โดยเส้นหนึ่งสำหรับส่งข้อมูล อีกเส้นสำหรับรับข้อมูล และเส้นสุดท้ายเป็นกราวด์ สำหรับรายละเอียดหน้าที่การทำงานในแต่ละขาของพอร์ตอนุกรม RS-232 มีดังนี้

Data Carrier Detect : DCD หรืออาจเรียกว่า Carrier Detect : CD ขานี้จะแอคทีฟเมื่อมีการส่งสัญญาณพาห์จากอุปกรณ์สื่อสารข้อมูล เช่น โมเด็ม สำหรับการใช้งานปกติ ขานี้จะไม่ได้ถูกใช้งานมากนัก

Received Data : RD หรือ RxD ขานี้ใช้เพื่อรับสัญญาณอนุกรมเข้ามายังคอมพิวเตอร์ โดยนำข้อมูลที่อ่านได้เก็บไว้ในรีจิสเตอร์ บัฟเฟอร์

Transmitted Data : TD หรือ TxD ขานี้ใช้เพื่อส่งข้อมูลออกจากคอมพิวเตอร์ โดยนำข้อมูลที่เก็บอยู่ในบัฟเฟอร์สำหรับส่งข้อมูลออกไป

Data Terminal Ready : DTR เป็นขาสัญญาณที่ส่งออกจากคอมพิวเตอร์เพื่อให้อุปกรณ์ปลายทางรับรู้ว่า ต้องการติดต่อด้วย โดยขา DTR นี้จะต้องเชื่อมต่อกับขา DSR ของอุปกรณ์ปลายทาง และขา DTR ของอุปกรณ์ปลายทางจะต้องเชื่อมต่อกับขา DSR ของคอมพิวเตอร์ ถ้าใช้การเชื่อมต่อเป็นแบบนัลโมเด็ม ซึ่งใช้สายในการเชื่อมต่อเพียง 3 เส้น จะต้องต่อขา DTR และ DSR ของตัวมันเองเข้าด้วยกันและต้องต่อกับขา DCD ด้วย ในกรณีที่โปรแกรมสื่อสารที่ใช้มีการตรวจจับสัญญาณพาห์

Signal Ground : GND ขากราวด์ของระบบ

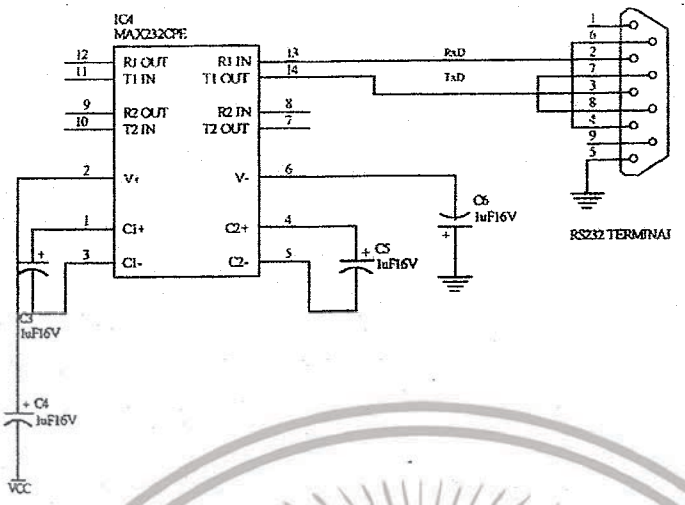
Data Set Ready : DSR ขานี้จะใช้คู่กับขา DTR เพื่อตรวจสอบการเชื่อมต่อกันระหว่างคอมพิวเตอร์กับอุปกรณ์ปลายทาง ซึ่งขา DSR นี้จะเป็นขาสำหรับรับข้อมูลจากภายนอกซึ่งถูกส่งมาจากขา DTR

Request To Send : RTS เป็นขาสำหรับส่งสัญญาณร้องขอให้ทางอุปกรณ์ปลายทางส่งข้อมูลกลับมายังคอมพิวเตอร์โดยขาที่รับสัญญาณ RTS ก็คือขา CTSในกรณีที่ใช้การเชื่อมต่อแบบนัลโมเด็ม 3สาย จะต้องเชื่อมต่อขา DTS และ CTS ของตัวมันเองเข้าด้วยกัน เพื่อจะให้การรับและส่งข้อมูลสามารถเกิดขึ้นได้ตลอดเวลา

Clear To Send : CTS ขานี้จะคอยรับสัญญาณจากขา RTS เมื่อรับสัญญาณได้ ข้อมูลที่ขา TxD จะถูกส่งออกไป ดังนั้นขานี้จึงถูกใช้เพื่อตรวจสอบอุปกรณ์ต่อพ่วงว่าพร้อมที่จะรับข้อมูลหรือไม่

Ring Indicator : RI ใช้แสดงสถานะสัญญาณเรียกจากสายโทรศัพท์ ปกติในการสื่อสารโดยทั่วไปสายนี้จะไม่ถูกใช้งาน จะใช้งานก็ต่อเมื่อมีการเชื่อมต่อกับโมเด็มและโปรแกรมมีการตรวจสอบสัญญาณนี้เท่านั้น

2.8 ระดับแรงดันที่ใช้งานสำหรับพอร์ทอนุกรม RS – 232



รูปที่ 2.18 แสดงวงจรขับแบบ RS – 232 โดยใช้ MAX 232

มาตรฐานการสื่อสารข้อมูลของพอร์ทอนุกรม ได้ระบุช่วงระดับแรงดันสำหรับการทำงานของพอร์ทอนุกรมไว้ว่าที่ลอจิก “0” จะมีระดับสัญญาณ +3 ถึง +15 โวลต์ ส่วนลอจิก “1” จะมีระดับสัญญาณ -3 ถึง -15 โวลต์ ระดับสัญญาณนี้ทำให้ไม่สามารถที่จะนำขาเอาท์พุตใดๆ ต่อเข้ากับลอจิกเกตเพื่อใช้งานได้โดยตรง จะต้องผ่านวงจรเพื่อปรับระดับแรงดันเสียก่อน นั่นก็คือวงจรขับอุปกรณ์ขับแบบมาตรฐาน RS – 232 นั้น ในด้านภาคส่งต้องสามารถเปลี่ยนสัญญาณลอจิกให้เป็นระดับแรงดันตามค่าที่กำหนดไว้ได้ และสำหรับของในส่วนของวงจรภาครับ ก็ต้องสามารถตรวจจับระดับแรงดันที่รับเข้ามาแล้วเปลี่ยนกลับให้เป็นสัญญาณลอจิกได้อย่างถูกต้องด้วยเช่นกัน โดยปกติจะใช้ไอซีจำพวก RS - 232 Transceiver ที่นิยมมาก คือ MAX 232 หรือ ICL 232 ไอซีในกลุ่มนี้จะทำหน้าที่แปลงระดับแรงดันของ RS - 232 ให้กลับมาอยู่ในระดับทีทีแอล โดยลอจิก “0” ซึ่งเดิมมีระดับสัญญาณ +3 ถึง +5 โวลต์ จะถูกแปลงเป็น 0โวลต์ ส่วนลอจิก “1” ซึ่งมีระดับสัญญาณ -3 ถึง -15 โวลต์ จะแปลงเป็น +5 โวลต์ ทั้งนี้เพื่อให้สามารถเชื่อมต่อกับอุปกรณ์ดิจิตอลอื่นที่ใช้ระดับแรงดันทีทีแอลได้

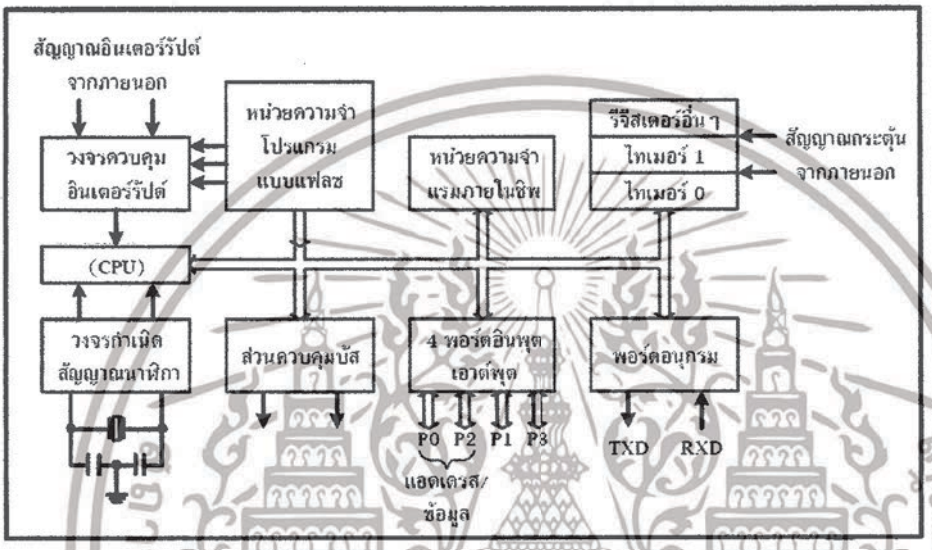
2.9 คุณลักษณะพื้นฐานของ MCS-51

คุณสมบัติของไมโครคอนโทรลเลอร์ ตระกูล MCS-51 อนุกรม AT89xx

1. เป็นไมโครคอนโทรลเลอร์ที่ใช้ซีพียูขนาด 8 บิต
2. มีหน่วยความจำโปรแกรมชนิดแฟลชเมโมรี (Flash Memory) หรือชนิดที่เขียนและลบได้รวดเร็ว ทนต่อการเขียนลบได้ 1000 ครั้ง และคงค่าข้อมูลไว้ได้นาน 10 ปี
3. หน่วยความจำข้อมูลพื้นฐานเป็นหน่วยความจำแบบแรม ในบางเบอร์จะมีหน่วยความจำแบบอีพรอมเพิ่มเติม
4. ขาพอร์ทเป็นแบบสองทิศทาง สามารถใช้งานเป็นได้ทั้งอินพุทและเอาท์พุท
5. มีวงจรสื่อสารอนุกรมแบบฟูลดูเพล็กซ์
6. มีไทม์เมอร์/เคาน์เตอร์ขนาด 16 บิต อย่างน้อย 2 ตัว
7. สามารถรองรับแหล่งกำเนิดอินเตอร์รัพต์ได้ 6 ประเภท

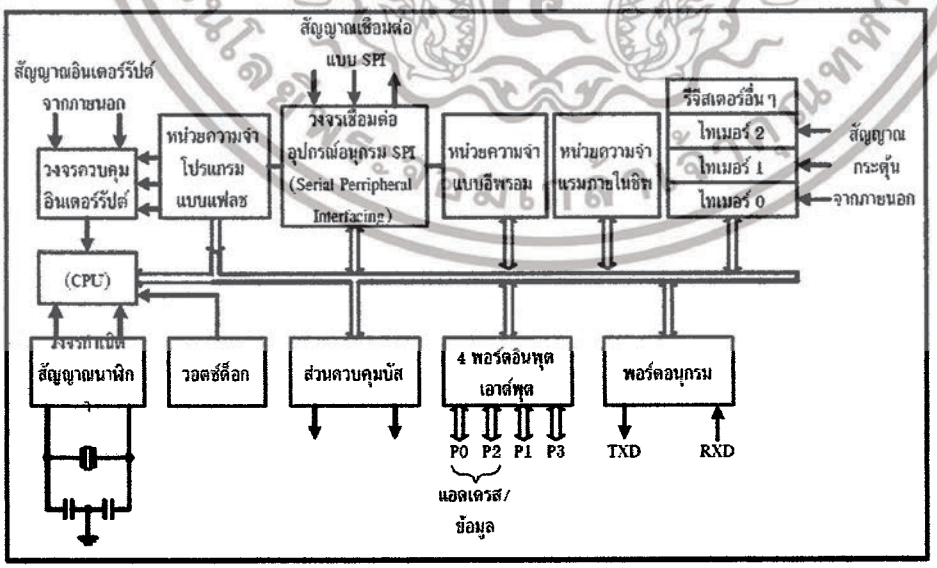
8. สามารถขยายหน่วยความจำภายนอกเพิ่มเติมได้สูงสุด 64 กิโลไบต์
9. มีวงจรกำเนิดสัญญาณนาฬิกาอยู่ภายในชิป
10. มีวงจรสื่อสารอนุกรม แบบ SPI สำหรับในกลุ่ม AT89Sxx
11. มีวอตซ์ด็อกไทเมอร์ในตัว สำหรับกลุ่ม AT89Sxx

ซึ่งไมโครคอนโทรลเลอร์ MCS-51 ของ บริษัท Atmel ที่ผลิตขึ้นมาและเป็นที่นิยมใช้งานกันในปัจจุบัน จะมีอยู่ 2 กลุ่ม คือ AT89Cxx และ AT89Sxx โดยที่ AT89Cxx จะมีโครงสร้างเหมือนกับ ไมโครคอนโทรลเลอร์ตระกูล MCS-51 พื้นฐานดัง แสดงใน รูปที่ 2.19



รูปที่ 2.19 โครงสร้างพื้นฐานของ MCS-51 แบบแฟลชในกลุ่ม AT89Cxx

กลุ่ม AT89Sxx จะมีส่วนประกอบที่แตกต่างจากกลุ่ม AT89Cxx อยู่หลายส่วน อาทิ วงจรเชื่อมต่อแบบอนุกรมแบบ SPI ในกลุ่มนี้สามารถที่จะทำการเขียนโปรแกรมลงไปในชิพได้เลย โดยไม่ต้องถอดชิพออกไปจากระบบ เรียกว่าการโปรแกรมในวงจร และ อื่นๆอีกดังแสดงใน ภาพที่ 2.20



รูปที่ 2.20 โครงสร้างพื้นฐานของ MCS-51 แบบแฟลชในกลุ่มAT89Sxx

หมายเหตุ : รายละเอียดบางส่วนของ MCS-51 แบบแฟลชในกลุ่ม AT89Cxx และ ในกลุ่ม AT89Sxx ของทาง บริษัท Atmel ที่ผลิตออกมาใช้งานกันในปัจจุบัน จะแสดงในตารางที่ 2.3

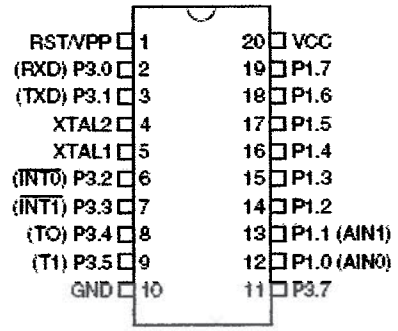
ตารางที่ 2.3 รายละเอียดบางส่วนของ MCS-51 แบบแฟลชของ บริษัท Atmel ที่นิยมใช้งาน

เบอร์ MCU	หน่วยความจำโปรแกรม	หน่วยความจำข้อมูล	จำนวณไทเมอร์/เคาท์เตอร์16 บิต
AT89C1051	แบบแฟลช ขนาด 1 กิโลไบต์	แรม 64 ไบต์	1
AT89C2051	แบบแฟลช ขนาด 2 กิโลไบต์	แรม 128 ไบต์	2
AT89C51	แบบแฟลช ขนาด 4 กิโลไบต์	แรม 128 ไบต์	3
AT89C52	แบบแฟลช ขนาด 8 กิโลไบต์	แรม 256 ไบต์	3
AT89C55	แบบแฟลช ขนาด 20 กิโลไบต์	แรม 256 ไบต์	3
AT89S8252	แบบแฟลช ขนาด 8 กิโลไบต์	แรม 256 ไบต์ อีอีพรอม 2 กิโลไบต์	3
AT89S53	แบบแฟลช ขนาด 12 กิโลไบต์	แรม 256 ไบต์	3

2.10 ลักษณะการจัดขาของ MCS-51

โครงสร้างของไมโครคอนโทรลเลอร์ ตระกูล MCS-51 ทุกเบอร์จะใช้แรงดันไฟฟ้ากระแสตรงเพียง +5V ในการทำงาน ในส่วนของกระแสไฟฟ้าที่ใช้งานจะแตกต่างกันออกไปตามแต่ละชนิดของเทคโนโลยีที่ใช้ในกระบวนการผลิต เบอร์ของ MCS-51 ในตระกูลที่มี C อยู่ตรงกลาง เช่น เบอร์ AT89C52 จะเป็นเบอร์ของชิพที่อาศัยเทคโนโลยี CHMOS ซึ่งใช้พลังงานน้อยกว่า และควบคุมการใช้พลังงานของชิพ ได้ด้วยโปรแกรม เพื่อการประหยัดพลังงานของระบบ

ไมโครคอนโทรลเลอร์ ตระกูล MCS-51 ทุกเบอร์มีตำแหน่งขาพื้นฐานที่เหมือนกันดังแสดงใน รูปที่ 2.21



รูปที่ 2.21 แสดงการจัดขาพื้นฐานของไมโครคอนโทรลเลอร์ MCS-51 ในอนุกรมของ AT89Cxx

- ขา +VCC (ขา 40) ใช้สำหรับต่อไฟเลี้ยง

- ขา GND (ขา 20) สำหรับต่อกราวด์ของระบบ

- ขา พอร์ต 0 (ขา 32 ถึง 39) จะมี 8 ขา คือ P0.0-P0.7 โดยสามารถกำหนดให้เป็นได้ทั้งอินพุตและเอาต์พุต โดยหากต้องการให้ขา พอร์ต 0 ขาใดเป็นอินพุตก็สามารถทำได้โดยการเขียนข้อมูล "1" ไปยังขาที่ต้องการติดต่อด้วยแต่ถ้าต้องการเป็นเอาต์พุตก็สามารถทำได้โดยการเขียนข้อมูลส่งไปยังขาที่ต้องกาติดต่อ และยังใช้ในการติดต่อกับขาแอดเดรสไบต์ต่ำของหน่วยความจำภายนอก (A0-A7) และขาข้อมูล (D0-D7) โดยใช้กระบวนการมัลติเพล็กซ์เข้าช่วยในการทำงาน

- ขา พอร์ต 1 (ขา 1-8) จะมี 8 ขา คือ P1.0-P1.7 โดยสามารถกำหนดให้เป็นได้ทั้ง อินพุต และเอาต์พุต โดยหากต้องการให้ขา พอร์ต 1 ขาใดเป็นอินพุตก็สามารถทำได้โดยการเขียนข้อมูล "1" ไปยังขาที่ต้องการติดต่อด้วยและนอกจากนี้ในกลุ่มของ AT89Sxx จะใช้ขาP1.0 เป็นขาอินพุต สำหรับค่าของไทเมอร์ 1 และ P1.1 เป็นขาอินพุต สำหรับค่าของไทเมอร์ 2 ในขณะที่ P1.4-P1.7 ใช้เป็นขาเชื่อมต่อแบบ SPI เพื่อทำการโปรแกรมข้อมูลในระบบ

- ขา พอร์ต 2 (ขา 21-28) จะมี 8 ขา คือ P2.0-P2.7 ใช้เป็นอินพุตและเอาท์พุตพอร์ตและใช้งานในการติดต่อกับขาแอดเดรสไบต์สูงของหน่วยความจำภายนอก A8-A15

- ขา พอร์ต 3 (ขา 10-17) จะมี 8 ขา คือ P3.0-P3.7 ใช้เป็นอินพุตและเอาท์พุตพอร์ตและถูกใช้งานในหน้าที่พิเศษอื่นๆอีกหลายอย่างดังนี้

P3.0 ใช้เป็นขาอินพุตสำหรับรับข้อมูลจากการสื่อสารแบบอนุกรมหรือขา RXD

P3.1 ใช้เป็นขาอินพุตสำหรับส่งข้อมูลจากการสื่อสารแบบอนุกรมหรือขา TXD

P3.2 ใช้เป็นขาอินพุตรับสัญญาณอินเตอร์รัปต์จากภายนอกช่อง 0 หรือขา INT0****

P3.3 ใช้เป็นขาอินพุตรับสัญญาณอินเตอร์รัปต์จากภายนอกช่อง 1 หรือขา INT1****

P3.4 ใช้เป็นขาอินพุตสำหรับรับสัญญาณไทเมอร์จากช่อง 0 หรือขา T0

P3.5 ใช้เป็นขาอินพุตสำหรับรับสัญญาณไทเมอร์จากช่อง 1 หรือขา T1

P3.6 ใช้เป็นขาอินพุตหรือเป็นขา WR ในกรณีที่ใช้เชื่อมต่อกับหน่วยความจำภายนอก

P3.7 ใช้เป็นขาอินพุตหรือเป็นขา RD ในกรณีที่ใช้เชื่อมต่อกับหน่วยความจำภายนอก

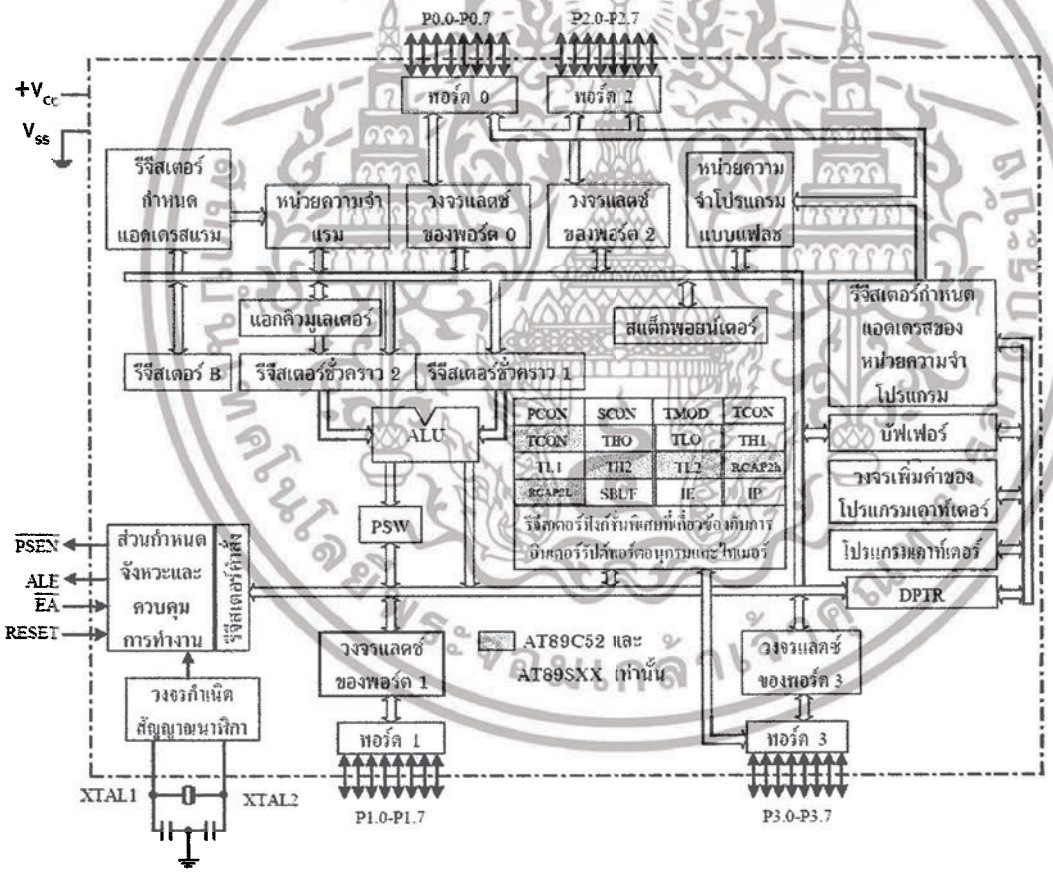
- ขา RESET (ขา9) ใช้ในการรีเซ็ตการทำงานของไมโครคอนโทรลเลอร์เพื่อเริ่มต้นการทำงานใหม่

- ขา ALE/PROG (ขา30) เป็นขาควบคุมการแลตช์ของขาพอร์ต 0 เมื่อมีการใช้งานหน่วยความจำภายนอกหากขานี้มีสถานะเป็นลอจิก '0' และใช้เป็นขาสำหรับใช้รับพัลส์ของการโปรแกรมข้อมูลลงในไมโครคอนโทรลเลอร์ MCS-51 ถ้ามีสถานะเป็นลอจิก '1' ในรุ่นที่มีหน่วยความจำเป็นแบบอีพรอม

- ขา PSEN (ขา9) ใช้ส่งสัญญาณร้องขอติดต่อกับหน่วยความจำโปรแกรมภายนอกในช่วงของการอ่านเขียนข้อมูลกับหน่วยความจำภายนอก เมื่อใช้โปรแกรมจากหน่วยความจำโปรแกรมภายในชิพ จะไม่ส่งสัญญาณออกมาที่ขานี้

- ขา EA/VPP (ขา31) ใช้สำหรับเลือกให้ MCS-51 ติดต่อกับหน่วยความจำโปรแกรมภายนอกหรือจากหน่วยความจำภายใน MCS-51 เองโดยหากมีสถานะเป็น '0' จะเลือกใช้โปรแกรมภายนอก หากมีสถานะเป็น "1" จะเลือกใช้หน่วยความจำภายใน MCS-51 และใช้เป็นขาอินพุตสำหรับรับแรงดันไฟสูง สำหรับการโปรแกรมหน่วยความจำภายใน สำหรับ MCS-51 แบบแฟลช ต้องการแรงดันในการโปรแกรม +12VDC

- ขา XTAL1 และ XTAL2 (ขา 19 และ ขา 18) เป็นขาต่อคริสตอล เพื่อสร้างสัญญาณนาฬิกาในการกำหนดจังหวะในการทำงานของ MCS-51



รูปที่ 2.22 โครงสร้างภายในของ MCS-51 แบบแฟลชของ Atmel

2.11 โครงสร้างของหน่วยความจำภายใน MCS-51

ไมโครคอนโทรลเลอร์ MCS-51 แบบแฟลชของ Atmel จะแบ่ง ออกเป็น 2 ส่วน คือ

- หน่วยความจำสำหรับเก็บโปรแกรม (Program Memory)

- หน่วยความจำสำหรับเก็บข้อมูล (Data Memory)

2.11.1 หน่วยความจำสำหรับเก็บโปรแกรม (Program Memory)

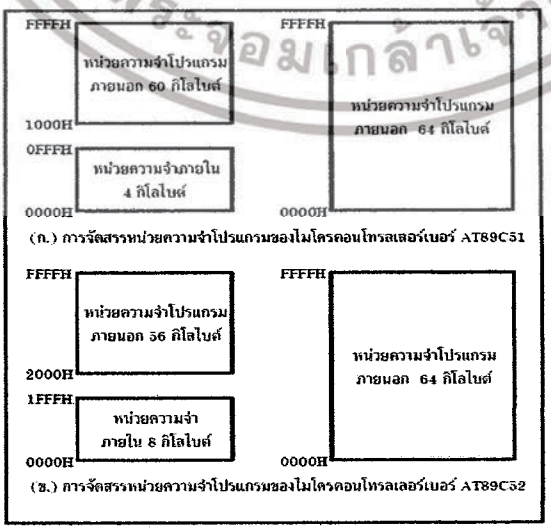
ในไมโครคอนโทรลเลอร์ตระกูล MCS-51 จะมีหน่วยความจำสำหรับเก็บโปรแกรมอยู่ 2 ลักษณะ คือ หน่วยความจำภายใน และหน่วยความจำภายนอก ในกลุ่มของ AT89xx ของ Atmel ก็เช่นกันยกตัวอย่างเช่น เบอร์ AT89C51 และ AT89C52 สามารถติดต่อหน่วยความจำได้สูงสุด 64 กิโลไบต์ โดยสามารถเลือกใช้หน่วยความจำโปรแกรมภายในอย่างเดียวหรือ ใช้ร่วมกับหน่วยความจำภายนอก หากต้องการใช้เฉพาะหน่วยความจำภายนอกอย่างเดียวก็ได้ โดยในเบอร์ AT89C51 จะมีหน่วยความจำภายใน 4 กิโลไบต์ และเบอร์ AT89C52 จะมีขนาด 8 กิโลไบต์ หากอยู่ในกรณีที่ใช้หน่วยความจำภายในและภายนอกรวมกันนั้นเบอร์ AT89C51 สามารถที่จะติดต่อกับหน่วยความจำภายนอกได้ 60 กิโลไบต์ หากเป็นเบอร์ AT89C52 สามารถติดต่อกับหน่วยความจำภายนอกได้เพียง 56 กิโลไบต์ หน่วยความจำสำหรับโปรแกรมนี้จะใช้สำหรับเก็บโปรแกรมการทำงานของระบบโดยจะมีแอดเดรสเริ่มต้นที่ 0000H และเมื่อไมโครคอนโทรลเลอร์ได้รับการรีเซ็ต จะกลับมาเริ่มต้นที่แอดเดรสนี้เสมอ ในกรณีที่ใช้ MCS-51 แบบแฟลช แบบมีหน่วยความจำภายในแต่ต้องการติดต่อกับหน่วยความจำภายนอกด้วย ต้องกำหนดแอดเดรสของหน่วยความจำภายนอก ให้ต่อที่แอดเดรสสุดท้ายของหน่วยความจำโปรแกรมภายในของ MCS-51 ยกตัวอย่าง MCS-51 เบอร์ AT89C51 มีหน่วยความจำภายใน 4 กิโลไบต์ มีแอดเดรสอยู่ในช่วง 0000H-0FFFHหากทำการต่อหน่วยความจำภายนอกเข้ามาในระบบ จะต้องกำหนดแอดเดรสให้อยู่ในช่วง1000H-FFFFH

2.11.2 หน่วยความจำสำหรับเก็บข้อมูล (Data Memory)

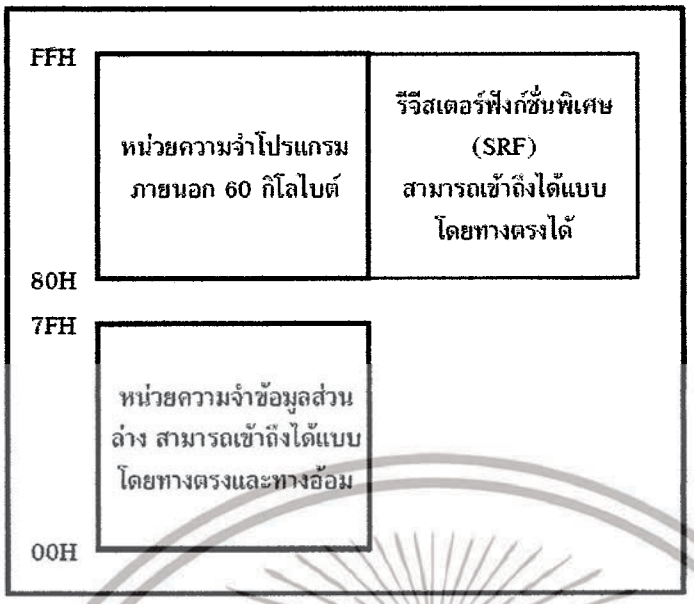
หน่วยความจำสำหรับเก็บข้อมูล จะมีอยู่ด้วยกัน 2 แบบ คือ หน่วยความจำข้อมูลภายในและภายนอก สำหรับไมโครคอนโทรลเลอร์ MCS-51 แบบแฟลช ในอนุกรมของ AT89xx ทุกเบอร์ จะมีหน่วยความจำข้อมูลภายในแบบ แรม (RAM:Random 14 Access Memory) โดยในแต่ละเบอร์จะมีขนาดแตกต่างกันออกไป ในเบอร์ AT89C51 จะมีขนาดหน่วยความจำข้อมูลภายใน 128 ไบต์ ในขณะที่เบอร์ AT89C52 มีขนาด 256 ไบต์ ในการจัดสรรหน่วยความจำข้อมูลแบ่งออกเป็น 3 ส่วน คือ

- หน่วยความจำข้อมูลส่วนล่าง(Lower)
- หน่วยความจำข้อมูลส่วนบน (Upper)
- รีจีสเตอร์ฟังก์ชั่นพิเศษ (SFR:Special Function Register) ซึ่งในแต่ละส่วนมีขนาด 128 ไบต์

การจัดสรรหน่วยความจำข้อมูลส่วนล่าง หน่วยความจำข้อมูลส่วนบนและรีจีสเตอร์ฟังก์ชั่นพิเศษ ของ MCS-51 แสดงดังรูปที่ 2.23 รูปที่ 2.24 และ รูปที่ 2.25



รูปที่ 2.23 การจัดสรรหน่วยความจำโปรแกรมของ MCS-51 แบบแฟลช



รูปที่ 2.24 การจัดสรรพื้นที่ของหน่วยความจำข้อมูลภายในของ MCS-51 แบบแฟลช

รูปที่ 2.25 โครงสร้างหน่วยความจำข้อมูลส่วนล่างของ MCS-51

2.12 ไทม์เมอร์/เคาน์เตอร์

การใช้งานไทม์เมอร์/เคาน์เตอร์ภายใน MCS-51 จะต้องมีการกำหนดรูปแบบการใช้งานต่างๆ เสียก่อน จึงจะทำงานได้อย่างถูกต้อง การกำหนดค่าเริ่มต้นของรีจีสเตอร์ในการใช้งานไทม์เมอร์/เคาน์เตอร์ จำเป็นต้องเข้าใจหลักการของไทม์เมอร์/เคาน์เตอร์ ดังนี้

เคาน์เตอร์ (Counter) ความหมายของเคาน์เตอร์ก็คือตัวนับสัญญาณ เช่น การนับของจำนวนพัลส์ของอินพุตที่มาจากภายนอก

รูปที่ 2.26 แสดงเคาน์เตอร์

ไทม์เมอร์ (Timer) ความหมายของไทม์เมอร์ก็คือ การเป็นตัวตั้งเวลาด้วยโปรแกรม เมื่อถึงเวลาที่กำหนดจะแสดงผลออกมาให้รู้เหมือนกับนาฬิกาปลุกซึ่งแสดงออกให้รู้โดยการส่งเสียงออกมา ใน MCS-51 การใช้งานเป็นไทม์เมอร์จะแสดงผลออกมาให้รู้โดยแฟลกซ์ (TF) ซึ่งถ้าเราเปรียบเทียบระหว่างไทม์เมอร์และเคาน์เตอร์จะเห็นข้อแตกต่างดังรูป

รูปที่ 2.27 แสดงการเปรียบเทียบข้อแตกต่างระหว่างไทม์เมอร์กับเคาน์เตอร์

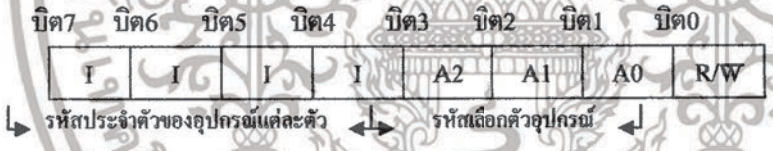
2.13 ความรู้เรื่องการสื่อสารแบบ I2C-Bus

I2C-Bus ย่อมาจาก Inter Integrate Circuit Bus ซึ่งนิยมเรียกสั้นๆว่า "I2C Bus" ซึ่งเป็นชื่อของวิธีการติดต่อสื่อสารอนุกรมแบบหนึ่ง ซึ่งถูกคิดค้นและพัฒนาโดย"PHILIPS SEMICONDUCTOR" เมื่อหลายปีก่อน แต่เพิ่งมาได้รับความนิยมอย่างแพร่หลายในระยะหลังๆมานี้เอง ซึ่งในยุคแรกๆนั้นอุปกรณ์จำพวกที่ใช้วิธีการเชื่อมต่อแบบ I2C-Busนี้จะมีเพียง"PHILIPS SEMICONDUCTOR"เท่านั้นที่ทำการผลิตออกใช้งานแต่ในปัจจุบันเริ่มมีผู้ผลิตรายอื่นๆ หันมาให้ความสนใจและผลิตอุปกรณ์ต่างๆที่ใช้วิธีการเชื่อมต่อแบบ I2C-Bus นี้ กันมากขึ้น เช่น บริษัท ATMEL บริษัท MICROCHIPS บริษัท DALLAS เป็นต้น เนื่องจากรูปแบบในการเชื่อมต่ออุปกรณ์ด้วยระบบบัสนี้ จะมีข้อดี คือ ใช้สัญญาณในการเชื่อมต่อเพียงสองเส้น (SCL และ SDA) แต่สามารถเชื่อมต่อ

อุปกรณ์หลายๆตัวร่วมในบัสเดียวกันได้ ซึ่งในปัจจุบันถือได้ว่าเป็นยุคสมัยของไมโครคอนโทลเลอร์ขนาดเล็ก เนื่องจากระบบการทำงานของวงจรต่างๆจะมุ่งเน้นออกแบบให้มีขนาดเล็กกะทัดรัดและสามารถใช้งานได้หลากหลาย ดั้งนั้นอุปกรณ์จำพวก Chips Support ต่างๆ ไม่ว่าจะเป็นไอซีหน่วยความจำ ไอซี ADC ไอซีฐานเวลา (RTC) หรือไอซีจำพวก Port I/O ต่างๆ ก็เริ่มมีการออกแบบให้ใช้การเชื่อมต่อกับ CPU เป็นบัสแบบ I2C Bus กันมากยิ่งขึ้น ซึ่งข้อกำหนดของการเชื่อมต่อบัสนี้จะมีรูปแบบเป็นมาตรฐานเหมือนกัน แต่อาจมีความแตกต่างกันบ้างในบางจุด เช่น จำนวนของไบต์ของข้อมูลที่ใช้ในการสื่อสารของอุปกรณ์แต่ละประเภท อาจใช้จำนวนไบต์มากน้อยไม่เท่ากัน แต่รูปแบบโดยรวมจะมีความเหมือนกัน ซึ่งมีรายละเอียดและข้อกำหนดพอสังเขปดังต่อไปนี้

2.14 การรับส่งข้อมูลของ I2C Bus

การรับส่งข้อมูลของอุปกรณ์ I2C Bus จะเริ่มต้นด้วยการที่ตัวแม่สร้างสภาวะเริ่มต้น () เพื่อขอใช้บัส จากนั้นจึงเริ่มการส่งรหัสควบคุม() เพื่อใช้ระบุตำแหน่งแอดเดรสของตัวลูกที่ต้องการจะติดต่อด้วยในระบบบัส โดยค่าตำแหน่งแอดเดรสนี้ อุปกรณ์แต่ละตัวจะมีรหัสแอดเดรสเฉพาะตัวที่แตกต่างกันออกไป ไม่มีการซ้ำกันในระบบบัสเดียวกัน Control byte นี้จะมีขนาด8 บิตซึ่ง7 บิตแรก(เริ่มจากMSB) จะเป็นค่าตำแหน่งแอดเดรสของตัวลูก ส่วนบิตที่8 (LSB) จะเป็นบิตสุดท้ายของไบต์ใช้สำหรับระบุทิศทางของข้อมูลในการรับส่ง(R/W) โดยถ้าบิต LSB มีค่าเป็น"0" จะหมายถึงตัวแม่(CPU) เขียนข้อมูลไปให้ตัวลูก(อุปกรณ์) แต่ถ้าบิตLSB มีค่าเป็น"1" จะหมายถึงตัวแม่(CPU) ต้องการอ่านข้อมูลจากตัวลูก(อุปกรณ์) โดยข้อมูลจะทำการรับส่งกันครั้งละ1 ไบต์(8บิต) และปิดท้ายข้อมูลของแต่ละไบต์ด้วยบิตแสดงการตอบรับ (Acknowledge bit) โดยลักษณะโครงสร้างของControl byte ของอุปกรณ์แบบI2C มีดังนี้

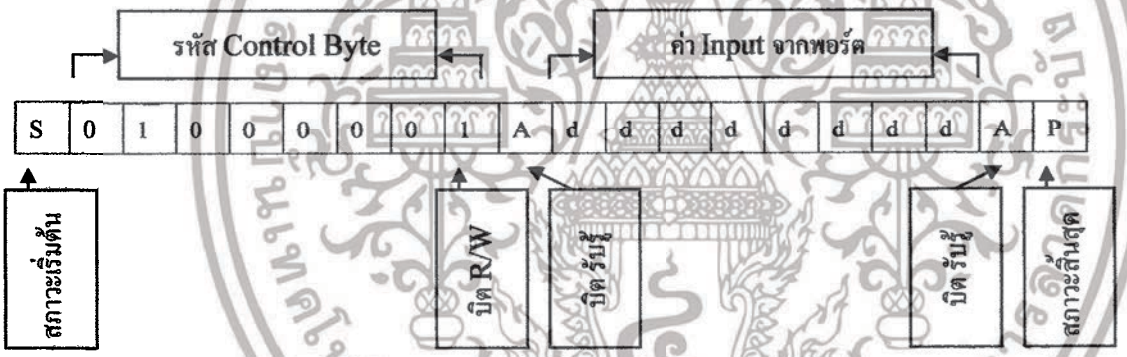


รูปที่ 2.28 แสดงลักษณะของ Control Byte ของ I2C Bus

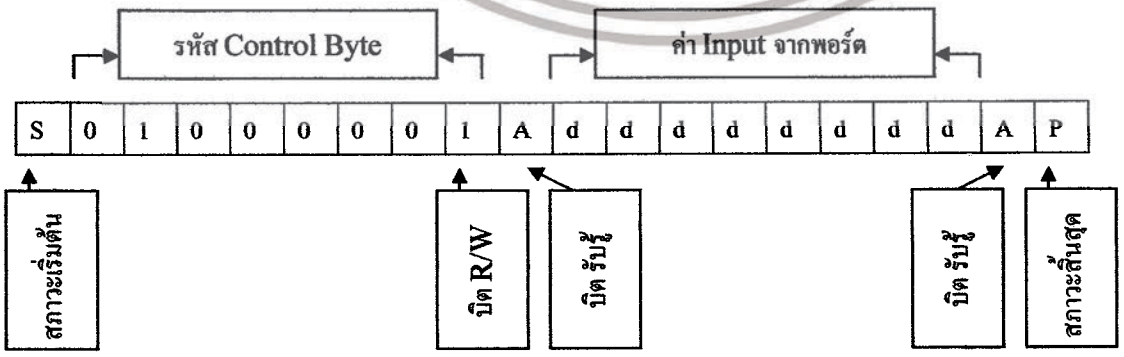
ซึ่งจะเห็นได้ว่ารหัส control byte ของอุปกรณ์ I2Cนั้น จะมีขนาด8 บิต โดยที่ บิต7 ถึงบิต4 จะเป็นรหัสประจำตัวของอุปกรณ์แต่ละตัวที่ถูกกำหนดไว้ตายตัวจากโรงงาน ซึ่งผู้ใช้งานต้องศึกษาจากคู่มือData sheet ของอุปกรณ์นั้นๆเองว่า อุปกรณ์ที่จะนำมาใช้งานมีรหัสประจำตัวเป็นเท่าไร ส่วน บิต3 ถึงบิต1 นั้นจะมีไว้สำหรับเลือกเบอร์อุปกรณ์ที่ต่ออยู่ในบัส โดยค่าของทั้งสามบิตนี้จะต้องมีค่าตรงกับการกำหนดสถานะทางลอจิกให้เข้าขาสัญญาณA2 ,A1 ,A0 ของอุปกรณ์ด้วย ตัวอย่างเช่น อุปกรณ์ที่มีรหัสประจำตัวเป็น"0111"อาจถูกออกแบบให้สามารถต่อร่วมกันภายในบัสเดียวกันได้จำนวน 8 ตัว โดยการกำหนดสภาวะลอจิกให้กับขาสัญญาณ A2 ,A1 ,A0 ของอุปกรณ์ให้มีความแตกต่างกันจากวงจรที่ต่ออยู่ดังนั้นเมื่อตัวแม่ต้องการติดต่ออุปกรณ์ที่มีรหัสประจำตัว "0111"ตัวใดในระบบบัสก็จะส่งค่าControl byte ตัวค่าในบิต3-บิต1 ตรงกับสถานะทางลอจิกของอุปกรณ์ตัวนั้นๆออกไป ตัวอย่างเช่น ถ้าตัวแม่ส่งรหัสControl byte ด้วยค่า"01110000" ออกไปในบัส ก็จะหมายถึงว่า ตัวแม่ต้องการจะเขียนข้อมูลไปยังอุปกรณ์ที่มีรหัสประจำตัว"0111" ตัวที่ขาสัญญาณ A2 ,A1 ,A0 มีค่าเป็น"0" อยู่ส่วนตัวอุปกรณ์ที่มีรหัส"0111" แต่มีสภาวะลอจิกของขาสัญญาณ A2 ,A1 ,A0 ไม่ตรงกับ "000" ก็จะไม่สนใจรหัสนั้น

แต่อย่างไรก็ตามอุปกรณ์I2C บางตัว อาจถูกออกแบบให้ต่อได้ในระบบบัสเดียวกันเพียงตัวเดียวโดยไม่มีขาสัญญาณในการเลือกตำแหน่งของอุปกรณ์อยู่ด้วย ค่าของControl byte ในตำแหน่งบิต3-บิต1 ก็อาจถูกกำหนดไว้ตายตัวเป็น "000" เสมอก็เป็นได้ ส่วนค่าControl Byte ในตำแหน่งของบิต0 นั้นจะใช้เป็นบิตกำหนดทิศทางของข้อมูล โดยถ้าบิต0 มีค่าเป็น"0" จะหมายถึงตัวแม่ต้องการเขียนค่าไปยังอุปกรณ์ แต่ถ้าค่าในบิต0 มีค่าเป็น "1" จะหมายถึงตัวแม่ต้องการอ่านค่าข้อมูลจากอุปกรณ์ เป็นต้น

สำหรับจำนวน ไบต์ ข้อมูลในการรับส่งกันนั้น ไม่มีข้อกำหนดตายตัวว่าจะต้องส่งกันครั้งละกี่ไบต์ขึ้นอยู่กับข้อตกระหว่างอุปกรณ์แต่ละชนิดจะกำหนดขึ้นโดยในการรับส่งแต่ละครั้งนั้น ตัวแม่จะเป็นตัวควบคุมการรับส่งเองทั้งหมด ซึ่งในกรณีที่ตัวแม่ต้องการติดต่อกับอุปกรณ์หลายๆตัวนั้น หลังจากตัวแม่สร้างสภาวะเริ่มต้น(Start condition) ขึ้นมาและทำการรับส่งข้อมูลกับอุปกรณ์ตัวหนึ่งเสร็จแล้ว ไม่จำเป็นต้องสร้างสภาวะสิ้นสุด (Stop condition) เพื่อกับไปเริ่มต้นรับส่งข้อมูลกับอุปกรณ์ตัวต่อไปอีกก็ได้ แต่ตัวแม่สามารถสร้างสภาวะเริ่มต้นขึ้นมาซ้ำใหม่พร้อมกับส่งค่าControl byte ซึ่งระบุตำแหน่งแอดเดรสของอุปกรณ์ต่อไปที่ต้องการติดต่อด้วยได้ทันที แต่เมื่อทำการติดต่อรับส่งข้อมูลกับอุปกรณ์ทุกตัวในบัสเสร็จเรียบร้อยแล้วจึงสร้างสภาวะสิ้นสุด เพื่อเป็นการเลิกใช้บัสและทำให้บัสอยู่ในสภาวะว่างในภายหลังก็ได้เช่นกัน



รูปที่ 2.29 แสดงตัวอย่างรูปแบบของการอ่านข้อมูลจากอุปกรณ์ I/O แบบ I2C Bus ตัวหนึ่ง



รูปที่ 2.30 แสดงตัวอย่างรูปแบบของการเขียนข้อมูลจากอุปกรณ์ I/O แบบ I2C Bus ตัวหนึ่ง

2.15 สัญญาณอินเตอร์รัปต์ภายนอก

เป็นการตรวจสอบสัญญาณที่ส่งเข้ามายังขา INT0 และ INT1 หากตรงตามเงื่อนไขที่กำหนดก็จะทำให้เกิดการอินเตอร์รัปต์ขึ้น โดยการอีนาเบิลการอินเตอร์รัปต์แบบนี้สามารถกระทำได้การกำหนดค่าในรีจิสเตอร์ IE ที่บิต EX0 สำหรับสัญญาณอินเตอร์รัปต์ขา INT0 และบิต EX1 สำหรับสัญญาณอินเตอร์รัปต์ที่ขา INT1 และทำการเลื่อนเงื่อนไขของการตรวจสอบสัญญาณในรีจิสเตอร์ TCON ที่บิต IE0 สำหรับสัญญาณอินเตอร์รัปต์ที่ขา INT0 และบิต IE1 สำหรับสัญญาณอินเตอร์รัปต์ที่ขา INT1

เงื่อนไขการตรวจสอบสัญญาณอินเตอร์รัปต์ที่ขา INT0 และ INT1 มีด้วยกัน 2 ลักษณะคือ

1. ตรวจสอบระดับลอจิก ถ้าหากบิต Iex ในรีจิสเตอร์ TCON เป็น "0" จะเกิดการอันเตอร์รัปต์จากภายนอกที่ขา INT หรือ INT1 ได้ก็ต่อเมื่อตรวจพบระดับลอจิกต่ำหรือ "0" เมื่อเกิดการอินเตอร์รัปต์แล้ว ให้ดำเนินการให้สัญญาณที่ขานี้กลับสู่ระดับลอจิก "1" ก่อนที่การบริการอินเตอร์รัปต์เสร็จสิ้น เพื่อป้องกันการเกิดอินเตอร์รัปต์ซ้อน

2. ตรวจสอบขอบขาของสัญญาณ ถ้าหากบิต Iex ในรีจิสเตอร์ TCON เป็น "1" จะเกิดการอินเตอร์รัปต์จากภายนอกที่ขา INT0 หรือ INT1 ได้ก็ต่อเมื่อตรวจพบการเปลี่ยนแปลงของสัญญาณที่ขา INT0 หรือ INT1 จาก "1" เป็น "0" หรือตรวจสอบพบขอบขาลงของสัญญาณที่ป้อนมาขังขา INT0 หรือ INT1 และต้องมีการรักษาสถานะลอจิก "0" นี้เป็นเวลาอย่างน้อย 1 แมชชีนไซเคิล จึงถือว่าเกิดการอินเตอร์รัปต์อย่างสมบูรณ์ เมื่อเกิดการอินเตอร์รัปต์ขึ้นซีพียูภายในไมโครคอนโทรลเลอร์ จะกระโดดไปยังแอดเดรส 0003H สำหรับการอินเตอร์รัปต์ที่ขา INT0 และ 0003H สำหรับการอินเตอร์รัปต์ที่ขา INT1

2.16 ลำดับความสำคัญของการอินเตอร์รัปต์ในไมโครคอนโทรลเลอร์ MCS-51

การกำเนิดสัญญาณอินเตอร์รัปต์ในไมโครคอนโทรลเลอร์ MCS-51 มีได้จาก 5-6 แหล่ง ดังนั้นจึงต้องมีการจัดลำดับความสำคัญ ในกรณีที่เกิดการอินเตอร์รัปต์ขึ้นพร้อมๆ กัน จากหลายแหล่งกำเนิดโดยสามารถกำหนดความสำคัญได้ที่รีจิสเตอร์ IP

อย่างไรก็ตาม ลำดับความสำคัญของการอินเตอร์รัปต์โดยปกติหรือในกรณีกำหนดข้อมูลในรีจิสเตอร์ IP ให้เป็น "1" ทุกบิต (ยกเว้น 6 และ 7) จะเรียงลำดับจากความสำคัญสูงสุดไปจนถึงต่ำสุดดังนี้

1. อินเตอร์รัปต์ภายนอกที่ขา INT0 หรือการเซตของบิต IE0
2. อินเตอร์รัปต์จากไทเมอร์ 0 หรือการเซตบิตของบิต TF0
3. อินเตอร์รัปต์ภายนอกที่ขา INT1 หรือการเซตของบิต IE1
4. อินเตอร์รัปต์จากไทเมอร์ 1 หรือการเซตของบิต TF1
5. อินเตอร์รัปต์จากพอร์ตอนุกรม หรือการเซตของบิต RI หรือ TI
6. อินเตอร์รัปต์จากไทเมอร์ 2 หรือการเซตของบิต TF2 หรือ EXF2

2.17 โครงสร้าง LCD Module

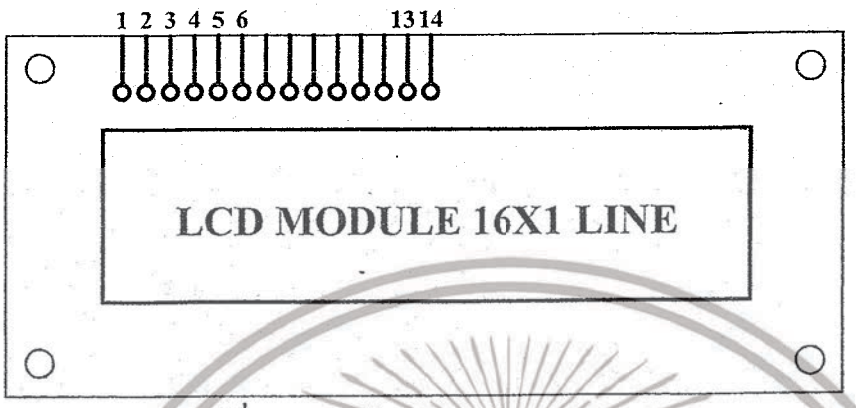
ใน LCD Module จะมีส่วนประกอบหลักๆ 3 ส่วนดังนี้

1. ตัวแสดงผล(Display) ภายในผลึกเหลวที่สามารถแสดงผลให้เห็นโดยอาศัยแสงจากภายนอก ดังนั้นจึงต้องมีมุมมองข้อมูลที่แสดงผลบนจอ

2. ตัวควบคุม(Controller) เป็นตัวรับข้อมูลจากอุปกรณ์ภายนอกมาควบคุมการทำงานของ LCD Module เช่น ลบจอภาพ แสดงตัวอักษร หรือเลื่อนเคอร์เซอร์ เป็นต้น ตัวควบคุมนี้ใช้ชิปควบคุมโดยเฉพาะชิปที่นิยมใช้คือ

เบอร์ HD44780 และ HD61830 โดย HD44780 จะใช้ควบคุม LCD แบบอักขระ ส่วนHD61830 ใช้ควบคุมLCD แบบกราฟิก

3. ตัวขับ(Driver) เป็นตัวรับสัญญาณจากตัวควบคุมมาขับให้ตัวแสดงผล แสดงข้อมูลตามที่กำหนด ชิปที่ใช้ทำหน้าที่นี้ได้แก่เบอร์ HD44100H และ MSM5259 เป็นต้น



รูปที่ 2.31 แสดงลักษณะของตัว LCD Module

LCD Module มีอยู่หลายรุ่นและคุณสมบัติแตกต่างกันไปซึ่งแบ่งได้เป็น 2 แบบคือ แบบ Dot matrix และ Graphic โดยแบบ Dot matrix จะแสดงผลเป็นแบบ 5×8 Dot. หรือ 5×10 Dot. มีตั้งแต่ 1 Line, 2 Line และ 4 Line ซึ่งการใช้งานแต่ละแบบจะใกล้เคียงกัน ลักษณะขาสัญญาณของ LCD Module แบบ 1 Line ดังรูปที่ 2.31

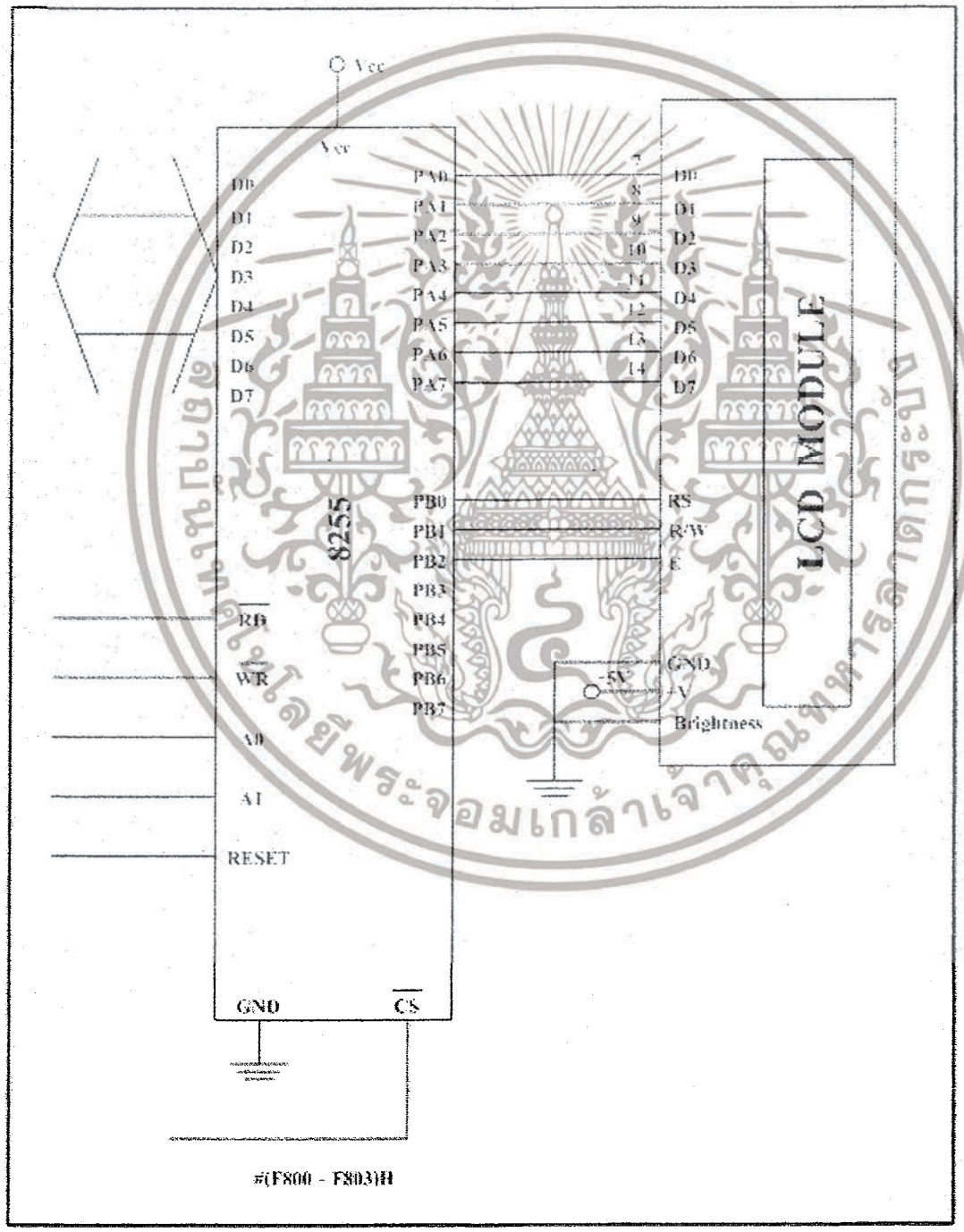
ตารางที่ 2.4 หน้าที่ของแต่ละขาของตัว LCD Module

ขา1 (GND)	เป็น Ground ใช้ต่อกับระบบ Ground ของไมโครคอนโทรลเลอร์
ขา2 (VCC)	เป็นไฟเลี้ยงวงจรของ LCD มีขนาด +5 VCC
ขา3 (V_{ee})	เป็นขาสำหรับปรับความเข้มของจอ LCD โดยที่เมื่อต่อกับ VCC จะมีความเข้มต่ำสุด และเมื่อต่อกับ Ground จะมีความเข้มมากที่สุด โดยปกติจะต่ออยู่กับ Ground เสมอเพื่อความสะดวกในการต่อ
ขา4 (RS)	Register Select ใช้สำหรับบอก LCD ทราบว่าข้อมูลที่ส่งให้นั้นเป็น Instruction หรือ Data โดยเมื่อขานี้ เป็น "0" หมายถึง Instruction เป็น "1" หมายถึง Data
ขา5 ($R/\overline{W}$)	ใช้สำหรับกำหนดว่าเป็นการอ่านหรือเขียนข้อมูลให้กับ LCD โดยเมื่อขานี้ เป็น "0" หมายถึงเป็นการเขียนข้อมูล เป็น "1" หมายถึงเป็นการอ่านข้อมูล
ขา6 (E)	เป็นขา Enable ขานี้ เป็น "1" ใช้สำหรับบอก LCD ว่าอุปกรณ์ภายนอก ต้องการติดต่อด้วย เป็น "0" ตัว LCD จะไม่สนในสัญญาณ RS, $R/\overline{W}$ และ ($DB_7 - DB_0$)
ขา7-14 ($DB_7 - DB_0$)	เป็นขา Data Bus สำหรับอ่านหรือเขียนข้อมูลให้กับตัว LCD

2.18 การเชื่อมต่อ LCD Module เข้ากับไมโครคอนโทรลเลอร์

การเชื่อมต่อ LCD Module เข้ากับไมโครคอนโทรลเลอร์สามารถต่อได้โดยตรงกับตัว MCS-51 หรือต่อผ่าน 8255 ก็ได้ ในที่นี้จะต่อโดยผ่าน 8255 ดังรูปที่ 2.32

- ขาสัญญาณข้อมูล D0 – D7 (ขา 7-14) ต่อเข้ากับ 8255 พอร์ทA
- ขา RS(ขา14) ต่อเข้ากับ 8255 พอร์ท B บิต 0
- ขา R/$\overline{W}$ (ขา5) ต่อเข้ากับ8255 พอร์ท B บิต 1
- ขา E (ขา6) ต่อเข้ากับ 8255 พอร์ท B บิต 2



รูปที่ 2.32 แสดงการเชื่อมต่อ LCD Module เข้ากับ 8255

2.19 การเขียนคำสั่งและข้อมูลให้แก่โมดูล LCD

ในการเขียนข้อมูลเพื่อควบคุมให้โมดูล LCD แสดงผลตามที่ผู้ใช้งานต้องการ ต้องส่งคำสั่ง(Instruction) แล้วกำหนดโหมดการทำงานให้แก่โมดูล LCD ก่อน จากนั้นจึงค่อยส่งข้อมูล(Data) ที่ต้องการแสดงผล เนื่องจากบัสข้อมูลของโมดูล LCD มี 8 เส้นคือ D0 ถึง D7 และใช้เป็นทางผ่านของทั้งคำสั่งและข้อมูล ดังนั้นในการส่งคำสั่งและข้อมูลจึงต้องอาศัยการกำหนดสัญญาณลอจิกที่ขา RS ถ้าหากที่ขา RS ได้ลอจิก "0" หมายความว่าข้อมูลที่ป้อนให้แก่โมดูล LCD ขณะนั้นเป็นคำสั่ง ในทางตรงกันข้าม หากขา RS ได้รับลอจิก "1" ข้อมูลที่ป้อนให้ขณะนั้นเป็นข้อมูลที่ใช้ในการแสดงผล

เมื่อต้องการเขียนหรืออ่านข้อมูลใน CGRAM และ DDRAM เริ่มต้นต้องกำหนดแอดเดรสที่ต้องการอ่านหรือเขียนก่อน โดยใช้คำสั่งเลือกแอดเดรส จากนั้นกำหนดให้ขา RS เป็น "1" เพื่อแจ้งให้ตัวควบคุมภายในโมดูล LCD ทราบว่าข้อมูลที่ปรากฏต่อไปนี้เป็นข้อมูลปกติไม่ใช่คำสั่ง

ในกรณีอ่านข้อมูล ต้องกำหนดให้ขา R/$\overline{W}$ เป็น "1" ข้อมูลขนาด 8 บิต(หรือ 4 บิต) ก็จะปรากฏบนบัสข้อมูล โดยข้อมูลที่อ่านออกมาได้จะเป็นข้อมูลจากแอดเดรสของ CGRAM หรือ DDRAM ตามที่ต้องการ

ในกรณีเขียนข้อมูล เมื่อกำหนดแอดเดรสและป้อนลอจิก "1" ให้ขา RS แล้ว ต้องกำหนดให้ขา R/$\overline{W}$ เป็น "0" ข้อมูลที่อยู่บนบัสข้อมูลจะถูกเขียนลงในรีจิสเตอร์ DR จากนั้นจึงถ่ายทอดลงใน DDRAM ต่อไป

2.20 จังหวะการทำงานของ LCD โมดูล

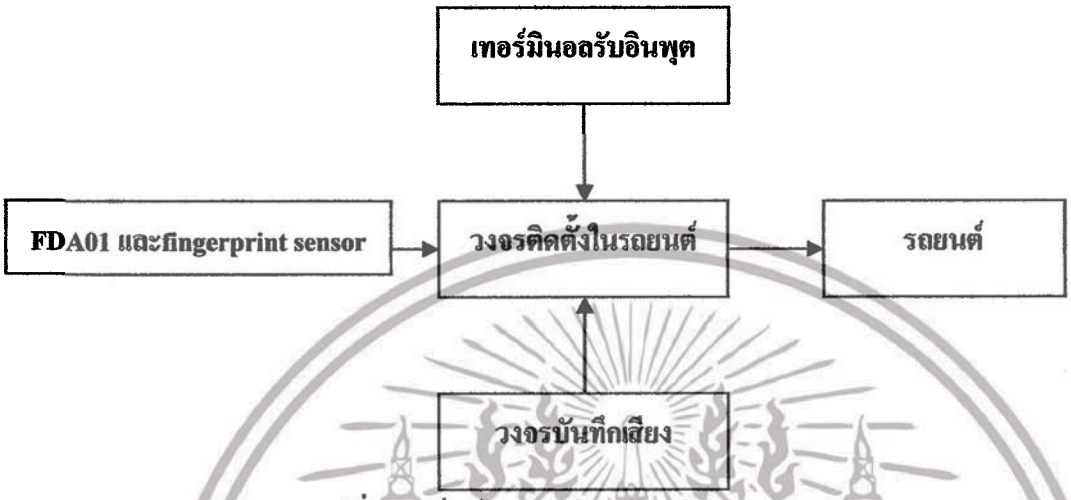
ในการติดต่อกับโมดูล LCD จะต้องมีการหน่วงเวลาหลังจากที่ทำการส่งรหัสคำสั่งหรือข้อมูล เนื่องจากต้องรอให้คอนโทรลเลอร์ภายใน LCD โมดูล แปลความหมายของรหัสคำสั่งและทำงานตามคำสั่งให้เรียบร้อยก่อน จากนั้นจึงจะรับข้อมูลหรือดำเนินการต่อไป

ดังนั้นในการใช้งานโมดูล LCD ผู้เขียนโปรแกรมต้องมีโปรแกรมเพื่อหน่วงเวลารอให้โมดูล LCD พร้อมทำงานด้วย โดยเมื่อเริ่มจ่ายไฟให้แก่โมดูล LCD ต้องรอประมาณ 10 มิลลิวินาที เพื่อให้โมดูล LCD ทำการเตรียมความพร้อมหรืออินิเชียล (Initial) หลังจากนั้นก็จะกำหนดลอจิกให้แก่ขา RS ของโมดูล LCD แล้วต้องหน่วงเวลาอีกประมาณ 2 มิลลิวินาทีเพื่อให้คอนโทรลเลอร์ในโมดูล LCD แปลความหมายของลอจิกที่ขา RS ว่าข้อมูลต่อไปที่จะได้รับนั้นเป็นรหัสคำสั่ง หรือเป็นข้อมูลที่ต้องการแสดงผล จากนั้นจะเป็นการส่งข้อมูลมารอที่บัสข้อมูล D0-D7 (กรณีทำงานในโหมด 8 บิต) ขั้นตอนต่อไปจะเป็นการส่งสัญญาณพัลส์ไปที่ขา E เพื่อเอ็นเอเบิลโมดูล LCD ให้รับข้อมูลจากบัสข้อมูลเข้าไป โดยพัลส์ที่ป้อนเข้าที่ขา E ของโมดูล LCD ต้องเป็นพัลส์ขอบขาขึ้น จากนั้นทำการหน่วงเวลา 2 มิลลิวินาที

ทั้งหมดที่กล่าวมาคือขั้นตอนและจังหวะในการทำงาน 1 รอบของโมดูล LCD จะเห็นได้ว่ามีโปรแกรมย่อยที่สำคัญอยู่ 3 โปรแกรมย่อยคือ โปรแกรมอินิเชียล LCD, โปรแกรมหน่วงเวลาและโปรแกรมย่อยการส่งพัลส์เพื่อเอ็นเอเบิลโมดูล LCD

บทที่3

การออกแบบและหลักการทำงาน



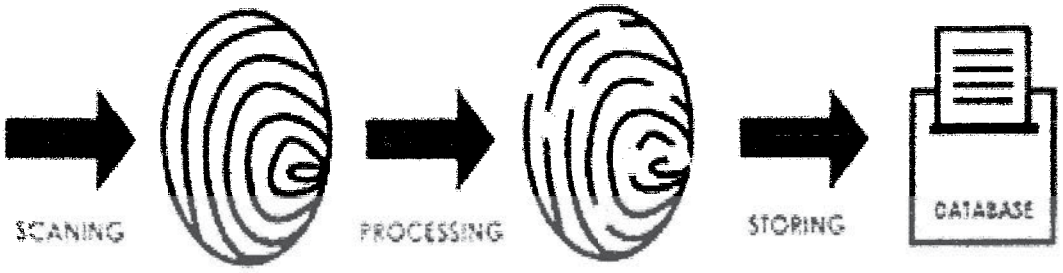
รูปที่ 3.1 บล็อกไดอะแกรมภาพรวมของระบบ

3.1 ส่วนการทำงานของเครื่องตรวจสอบลายนิ้วมือ

โดยทั่วไปนั้นเครื่องตรวจสอบลายนิ้วมือจะทำการวิเคราะห์โดยเริ่มจากการการนำลายนิ้วมือของแต่ละบุคคลแต่ละนิ้วมาหาจุดลักษณะที่สำคัญกระบวนการแรกเริ่มของการตรวจพิสูจน์ลายนิ้วมือคือการอ่านภาพลายนิ้วมือเข้ามาเก็บไว้ในหน่วยความจำถาวรซึ่งในส่วนนี้จะใช้EEPROMเป็นส่วนที่เก็บข้อมูลไว้ โดยข้อมูลที่อ่านหรือสแกน เข้ามานั้นจะนำมาผ่านการประมวลผล(Processing)ก่อนแล้วจัดเก็บข้อมูลนั้นไว้ซึ่งข้อมูลนี้จะถูกเก็บไว้เป็นต้นแบบ หรือรหัสของผู้ใช้แต่ละคน

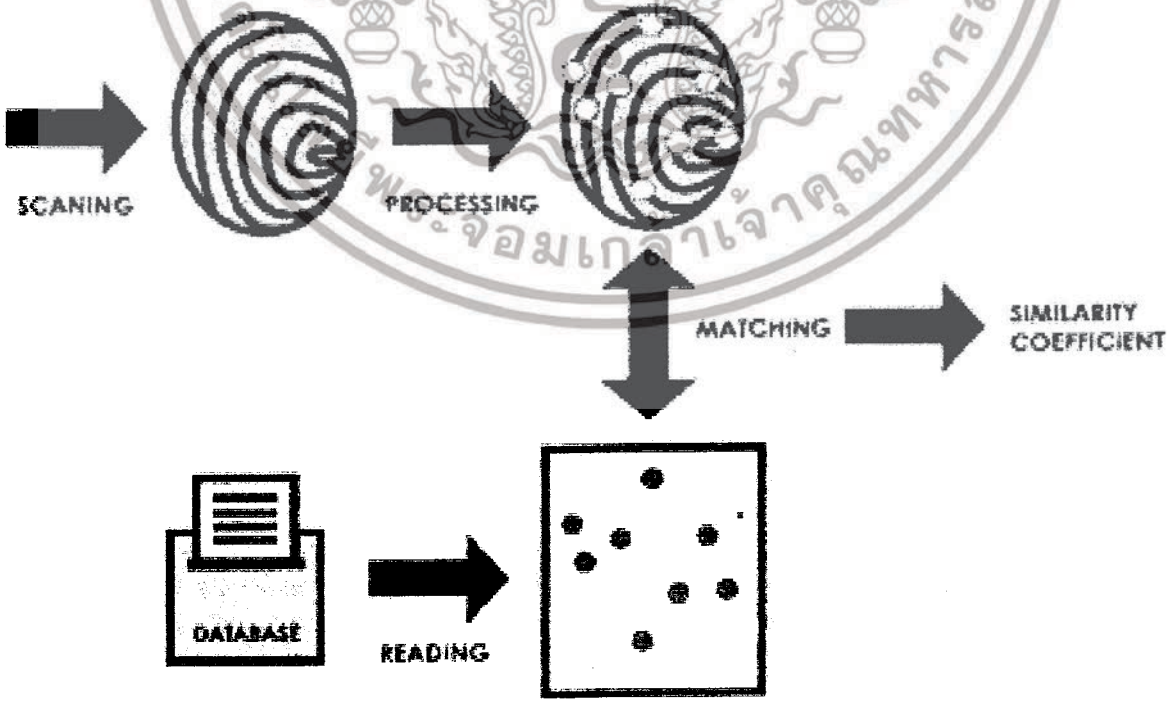
ในขั้นตอนก่อนที่จะนำลายนิ้วมือเข้าไปเก็บนั้นจะต้องผ่านขั้นตอนของการประมวลผลก่อนในกระบวนการนี้จะทำให้ภาพที่ได้รับการสแกนเข้ามาเกิดความสมบูรณ์มากขึ้นเพราะเมื่อเครื่องได้รับ การสแกนเข้ามาแล้ว ภาพที่อ่านได้อาจไม่ชัดเจน พร่าเลือน ก็จะทำให้การประมวลผลในขั้นตอนถัดไปทำได้ด้วยความยากลำบากหรือ ทำไม่ได้ ซึ่งจะทำให้ ผลที่ได้ก็อาจไม่ถูกต้องตามที่ควรจะเป็น เมื่อเกิดปัญหาเช่นนี้ในกระบวนการนี้จึงได้มีการกระทำหลายกระบวนการด้วยกันคือกระบวนการกำจัดสัญญาณรบกวนการปรับความมืด-สว่างและความแตกต่างของภาพและฉากของภาพ การแปลงเป็น ภาพ2ระดับ(binary) การทำให้เส้นลายนิ้วมือบาง(Thinning) การปรับภาพ หลังจากแปลงภาพเป็นสองระดับ การหาค่า Threshold ของการปรับภาพเป็นภาพ2ระดับและอื่นๆอีกมากมายซึ่งกระบวนการจะมากหรือน้อยขึ้นอยู่กับว่าตัวอุปกรณ์นั้นมีการอ่านค่าลายนิ้วมือที่ได้ภาพละเอียดและสมบูรณ์แค่ไหน เมื่อได้ลายนิ้วมือที่ผ่านการประมวลผลแล้ว ก็จะนำข้อมูลหรือภาพนี้ไปจัดเก็บในหน่วยความจำถาวร (EEPROM) ซึ่งสามารถลบข้อมูลได้ด้วยไฟฟ้า โดยภาพที่ถูกจัดเก็บไว้นี้จะถูกเก็บไว้เพื่อใช้ในการเปรียบเทียบ กับลายนิ้วมือที่ได้รับการสแกนเข้ามาเมื่อนำตัวอุปกรณ์นี้ไปใช้งาน ดังรูปที่3.2 แสดงกระบวนการทำงานของ การเริ่มใช้งาน

จากรูปที่3.2 เริ่มด้วยการสแกนลายนิ้วมือเข้ามาแล้วนำภาพที่ได้ผ่านการประมวลผลซึ่งจะได้ภาพที่มีประสิทธิภาพมากขึ้นแล้วจึงเก็บภาพนั้นไว้



รูปที่ 3.2 กระบวนการทำงานของการสแกนลายนิ้วมือ

จากรูปที่ 3.2 เริ่มด้วยการสแกนลายนิ้วมือเข้ามาแล้วนำภาพที่ได้ผ่านการประมวลผล ซึ่งจะได้ภาพที่มีประสิทธิภาพมากขึ้น แล้วจึงเก็บภาพนั้นไว้ หลังจากเก็บภาพไว้แล้วนั้นก็มาถึงขั้นตอนการนำไปใช้งาน เมื่อตัวอุปกรณ์ได้ถูกบันทึกหรือเก็บลายนิ้วมือของผู้ที่จะนำไปใช้แล้ว ขั้นตอนการใช้ก็จะคล้ายกับตอนอ่านลายนิ้วมือเข้ามาเก็บไว้เพียงแต่การอ่านเข้ามาครั้งนี้ ข้อมูลที่ได้จะถูกนำไปเก็บไว้ที่หน่วยความจำชั่วคราว(RAM)ซึ่งหลังจากสแกนเข้ามา เมื่อประมวลผลแล้วก็จะทำการเก็บข้อมูลไว้ที่ส่วนของหน่วยความจำชั่วคราว ส่วนในขั้นตอนถัดไปก็จะนำข้อมูลที่เก็บอยู่ในส่วนของหน่วยความจำสามารถกับส่วนที่เก็บไว้ในหน่วยความจำชั่วคราวนั้นมาทำการเปรียบเทียบกัน(Matching) เมื่อ ได้ผลแล้วก็จะแจ้งผลให้ผู้ใช้ทราบว่ามีความเหมือนกันมากน้อยแค่ไหน



รูปที่ 3.3 กระบวนการเปรียบเทียบลายนิ้วมือ

การประมวลผลภาพลายนิ้วมือ

โดยโปรแกรมที่ใช้ในการจำแนกลายนิ้วมือจะประกอบด้วยขั้นตอนหลักๆคือ

1.การปรับคุณภาพของภาพ (Image Enchancement)

เนื่องจากภาพจากเครื่องสแกนได้ภาพที่ไม่คมชัด อาจทำให้การหาลักษณะเด่นเกิดข้อผิดพลาดได้ จึงต้องมีการประมวลผลภาพในเบื้องต้น(Pre-Processing) ก่อน จากรูปจะเป็นการปรับคุณภาพของภาพโดยวิธี Fast Furier Transform(FFT)

2.ในการปรับภาพให้เป็นภาพ 2 ระดับ (Binalization)

ทำได้โดยการหาระดับสีเทาของภาพ จากนั้นนำไปเป็นค่าที่ใช้เปรียบเทียบ โดยที่ระดับสีของจุดภาพใดๆมีค่ามากกว่าระดับสีเทาจะกำหนดให้เป็นสีดำ และระดับของจุดภาพใดๆมีค่าน้อยกว่าระดับสีเทาจะกำหนดให้เป็นสีขาว

3.การลดขนาดเส้นลายนิ้วมือ(Thining)

โดยการใช้ฟังก์ชั่นของโปรแกรม Matlabทำให้ภาพที่ผ่านกระบวนการนี้แล้วจะมีขนาดเส้นของลายนิ้วมือที่ลดลงและเส้นมีความสม่ำเสมอมากขึ้น

4.การหาลักษณะเด่นของลายนิ้วมือ (minutia Extraction)

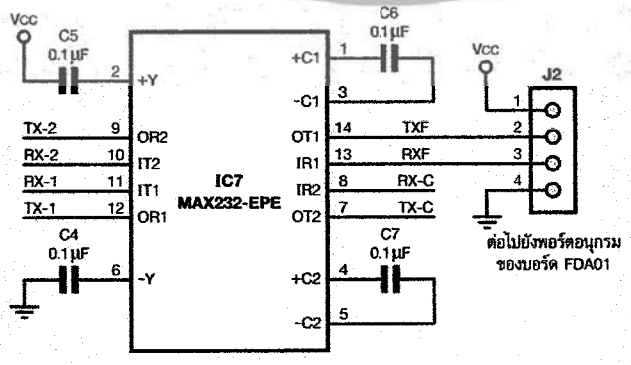
ในกระบวนการนี้จะทำการค้นหาพิกเซลที่เป็นจุดแยกและจุดปลาย ซึ่งเป็นเมตริกซ์ขนาด 3x3 ไปใช้ในการค้นหาตำแหน่งของจุดแยกและจุดปลาย โดยจะใช้การติดตามลายเส้นไปจนกระทั่งพบจุดแยกและจุดปลาย หลังจากนั้นจึงทำการเก็บตำแหน่งของจุดสำคัญไว้

5.การเปรียบเทียบลายนิ้วมือ

ในกระบวนการนี้จะใช้หลักการ Natural Network มาใช้ในการเปรียบเทียบและจำแนกว่าเป็นลายนิ้วมือของบุคคลใด

3.2 การเปลี่ยนระดับสัญญาณของพอร์ทอนุกรมเป็นระดับสัญญาณทีทีแอล

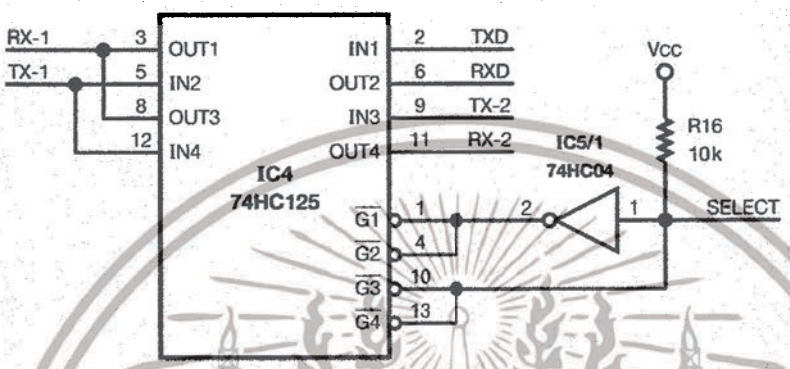
วงจรที่ใช้ในการเปลี่ยนระดับสัญญาณใช้ไอซีเบอร์ MAX232 โดยรับสัญญาณมาจากพอร์ทอนุกรมของเครื่องสแกนลายนิ้วมือ



รูปที่ 3.4 วงจรเปลี่ยนระดับสัญญาณของพอร์ทอนุกรมเป็นระดับสัญญาณทีทีแอล

3.3 การเลือกเส้นทางของข้อมูล

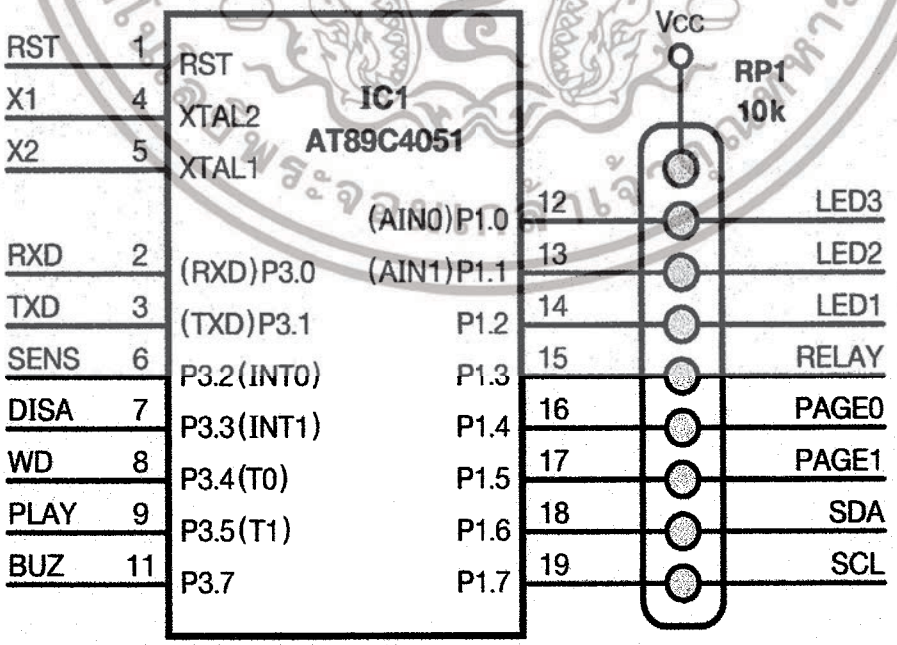
วงจรที่ใช้ในการเลือกเส้นทางของข้อมูลจะใช้ไอซีเบอร์ 74HC125 โดยที่เมื่อขา Select ถูกปล่อยลอยจะเป็น การเลือกเส้นทางของข้อมูล แต่ถ้าขา Select ถูกดึงลงกราวน์ เส้นทางที่เชื่อมจากบอร์ดควบคุม FDA 01 จะถูก ตัดขาดทำให้ข้อมูลจาก J4 จะถูกส่งไปยังพอร์ทอนุกรมของไมโครคอนโทรลเลอร์



รูปที่ 3.5 วงจรเลือกเส้นทางข้อมูล

3.4 ส่วนของการควบคุมการทำงาน

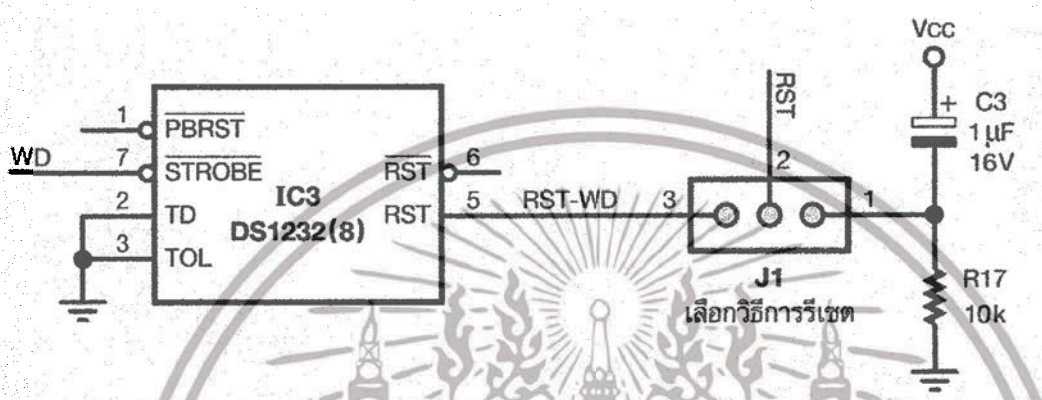
ในการควบคุมการทำงานของระบบจะใช้ เป็นไมโครคอนโทรลเลอร์ AT89C4051 ซึ่งโปรแกรมภายในไมโครคอนโทรลเลอร์ จะควบคุมการทำงานและการตัดสินใจจากข้อมูลที่ถูกส่งมา



รูปที่ 3.6 วงจรควบคุมการทำงานของระบบ

3.5 ส่วนของการตรวจสอบความผิดพลาด

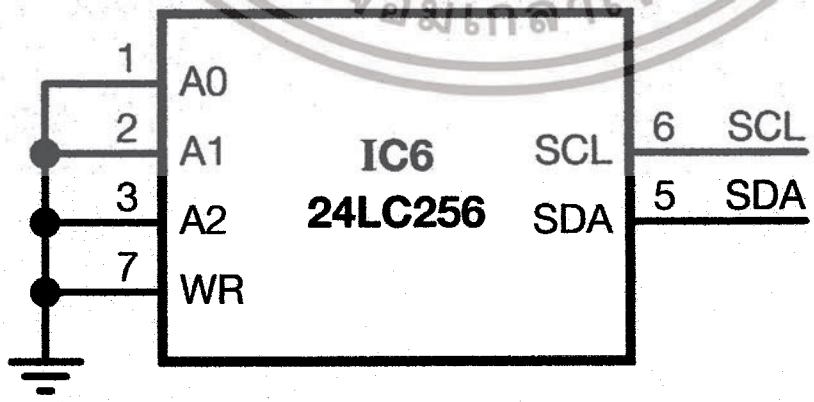
ในการตรวจสอบความผิดพลาดของระบบจะใช้ไอซีเบอร์ DS1232 โดยจะทำหน้าที่เป็นวอตช์ด็อก (Watchdog) คอยตรวจสอบความผิดพลาดที่อาจจะเกิดขึ้น โดยจะทำการรีเซ็ทค่าเมื่อเกิดความผิดพลาด



รูปที่ 3.7 วงจรตรวจความผิดพลาด

3.6 ส่วนของการบันทึกข้อมูล

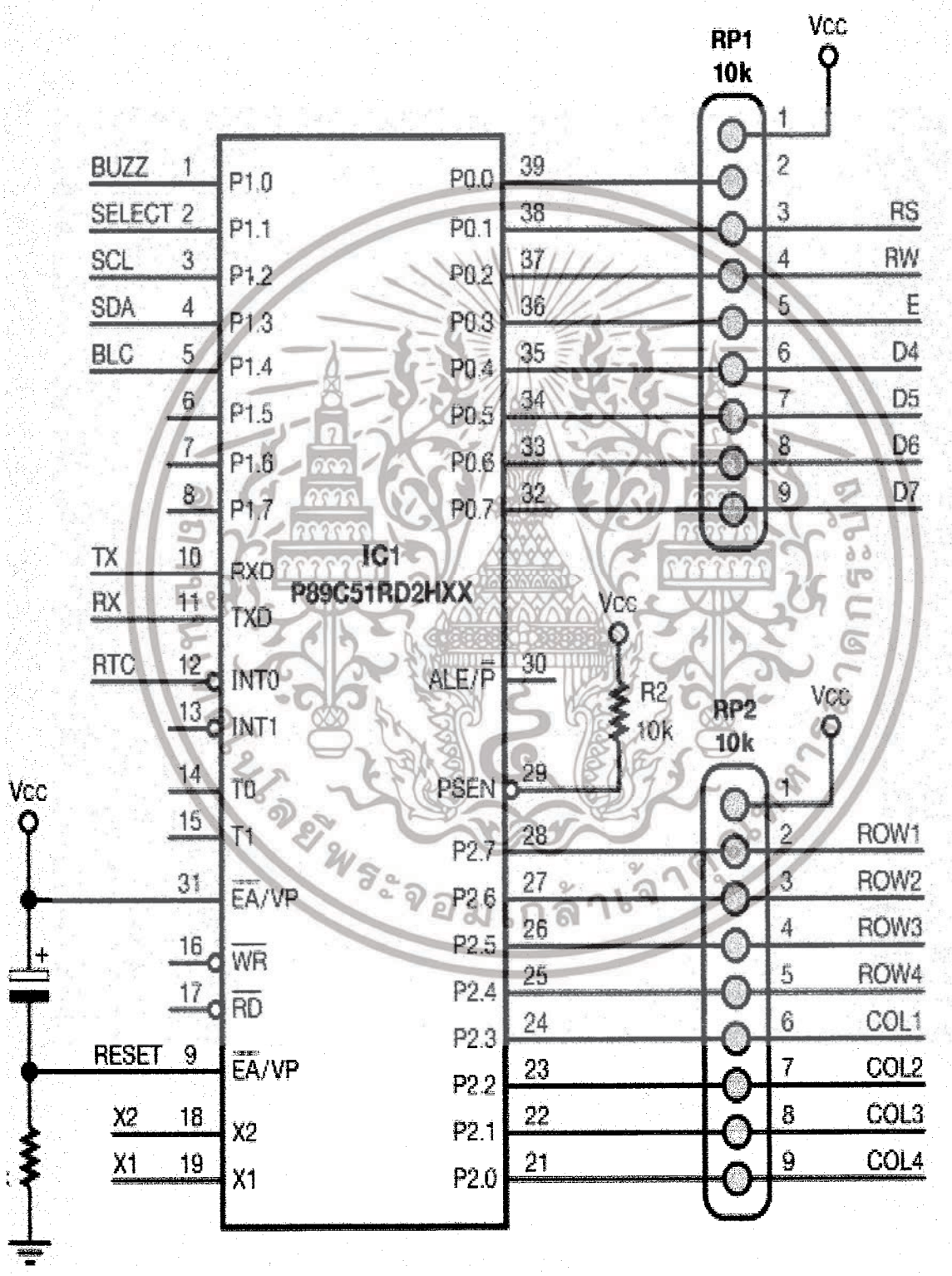
สำหรับในกรณีที่เกิดไฟดับจะมีการบันทึกข้อมูลโดยใช้ไอซีเบอร์24LC256 ซึ่งเป็นหน่วยความจำแบบ EEPROM โดยจะเชื่อมต่อกับไมโครคอนโทรลเลอร์โดยผ่านทางขา P1.6 และ P1.7



รูปที่ 3.8 วงจรบันทึกข้อมูล

3.7 วงจรของส่วนเทอร์มินอลรับข้อมูล

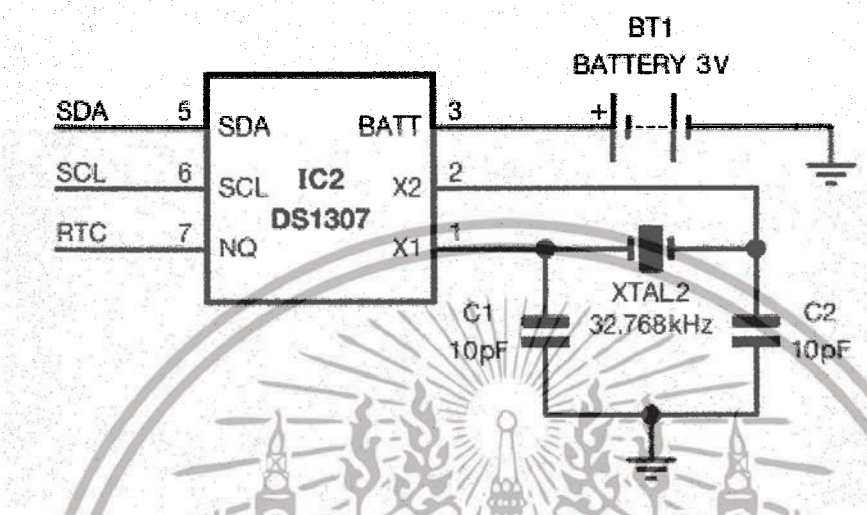
ใช้ไมโครคอนโทรลเลอร์ P89C51RD2 ในการควบคุมการทำงานของระบบโดยรวม



รูปที่ 3.9 วงจรควบคุมการทำงานของระบบ

3.8 ส่วนของการกำเนิดฐานเวลาจริง

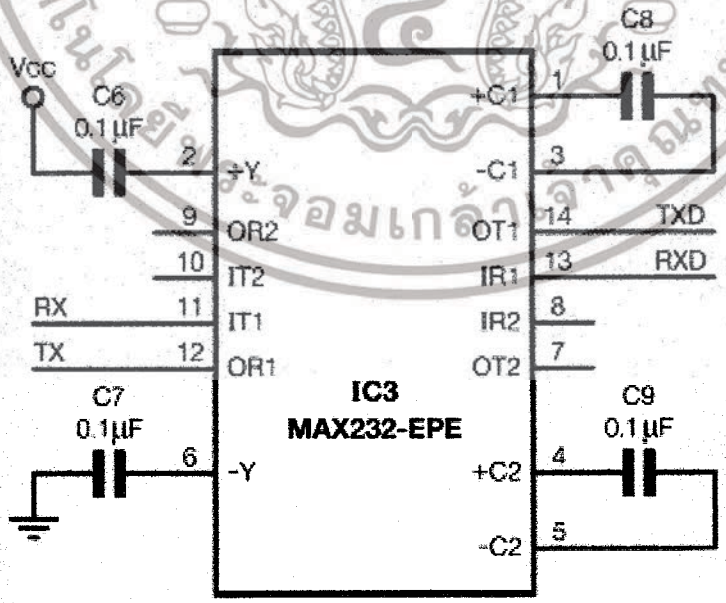
ในส่วนของการกำเนิดฐานเวลาจริง (RTC) จะใช้ ไอซีเบอร์ DS1307 ซึ่งจะทำงานโดยมี XTAL2 และ C1 และ C2 (10pF) เป็นส่วนกำเนิดความถี่ และมี BATTERY 3V เป็นแหล่งจ่ายไฟแบ็กอัพ



รูปที่ 3.10 วงจรกำเนิดฐานเวลาจริง

3.9 การเปลี่ยนระดับสัญญาณของพอร์ทอนุกรมเป็นระดับสัญญาณทีทีแอล

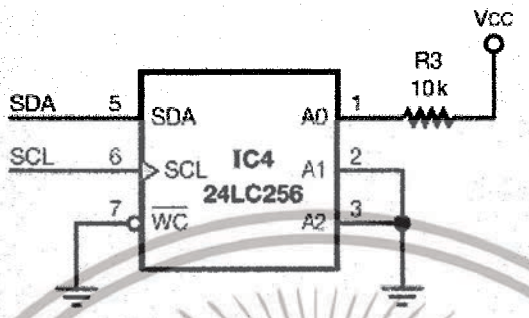
วงจรที่ใช้ในการเปลี่ยนระดับแรงดันใช้ไอซีเบอร์ MAX 232 เป็นไอซีปรับระดับแรงดันตามมาตรฐานการอินเตอร์เฟส RS-232



รูปที่ 3.11 วงจรเปลี่ยนระดับสัญญาณของพอร์ทอนุกรมเป็นระดับสัญญาณทีทีแอล

3.10 ส่วนของการสำรองข้อมูล

ในส่วนของการสำรองข้อมูลจะใช้ไอซีเบอร์ 24LC256 ซึ่งเป็นหน่วยความจำแบบ EEPROM สำหรับการสำรองข้อมูล โดยจะเชื่อมต่อกับไมโครคอนโทรลเลอร์โดยผ่านทางพอร์ท 1.2 และ 1.3

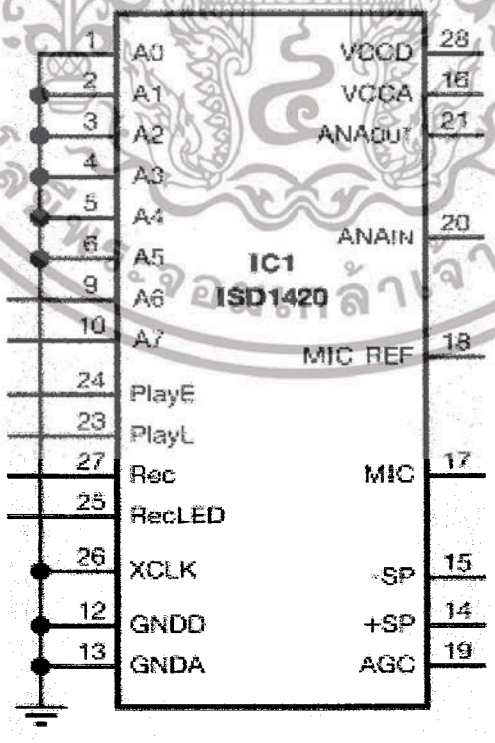


รูปที่ 3.12 วงจรสำรองข้อมูล

3.11 ส่วนของวงจรสำหรับบันทึกเสียงพูด

3.11.1ในส่วนของวงจรสำหรับบันทึกเสียงพูดจะใช้ไอซีเบอร์ ISD1420

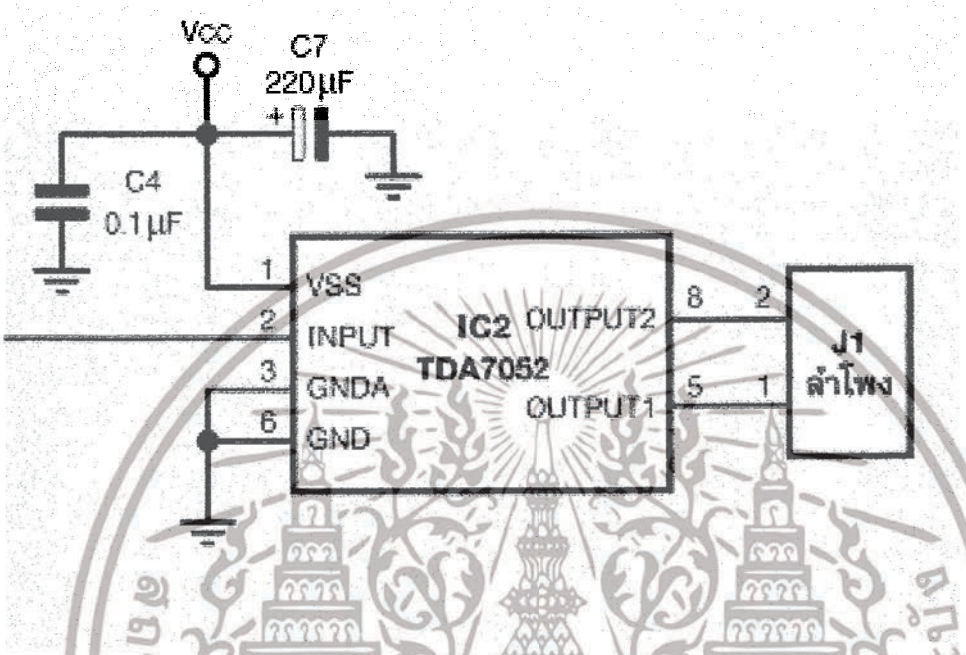
เป็นตัวที่ใช้เก็บข้อมูลของเสียงที่ได้บันทึกไว้จากไมโครโฟนผ่านเข้ามาเก็บไว้ยังหน่วยความจำภายในไอซี ซึ่งไอซีสามารถเก็บสัญญาณเสียงได้ประมาณ 20 วินาที



รูปที่ 3.13 วงจรบันทึกเสียง

3.11.2ในส่วนของวงจรขยายสัญญาณเสียง

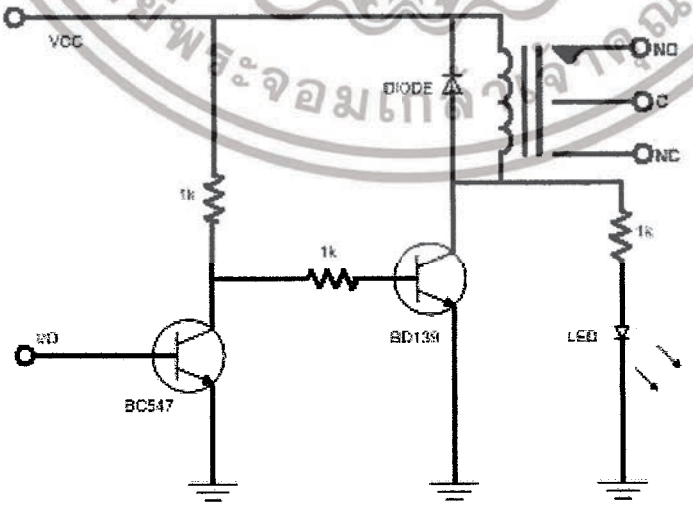
ในส่วนของวงจรขยายสัญญาณเสียงจะใช้ไอซีเบอร์ TDA7052 ในการขยายสัญญาณเสียงที่รับมาจากไอซีบันทึกเสียงก่อนที่จะส่งออกไปยังลำโพงต่อไป



รูปที่ 3.14 วงจรขยายสัญญาณเสียง

3.12 ส่วนของวงจรขับรีเลย์

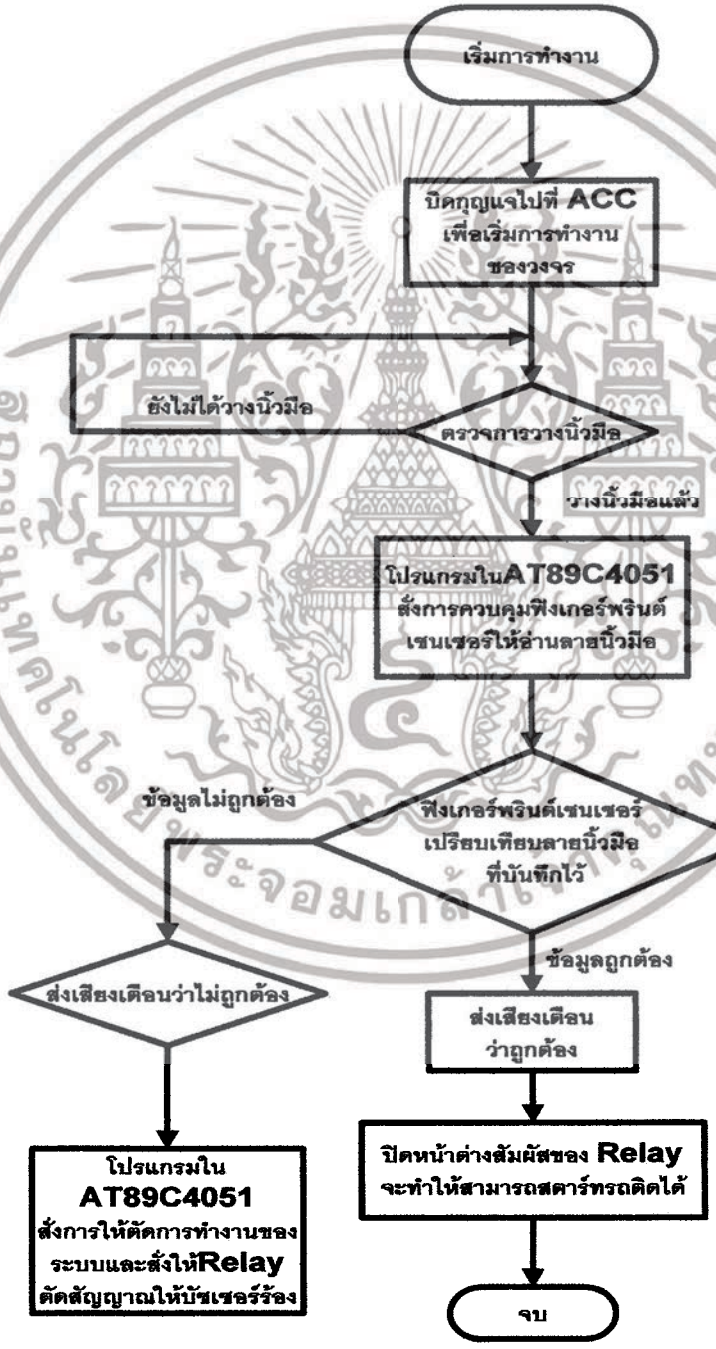
ในส่วนของวงจรขับรีเลย์จะใช้ทรานซิสเตอร์ BC547 และ BD139 ในการขับรีเลย์ทำให้บัซเซอร์ส่งสัญญาณเมื่อตรวจสอบไม่ผ่าน



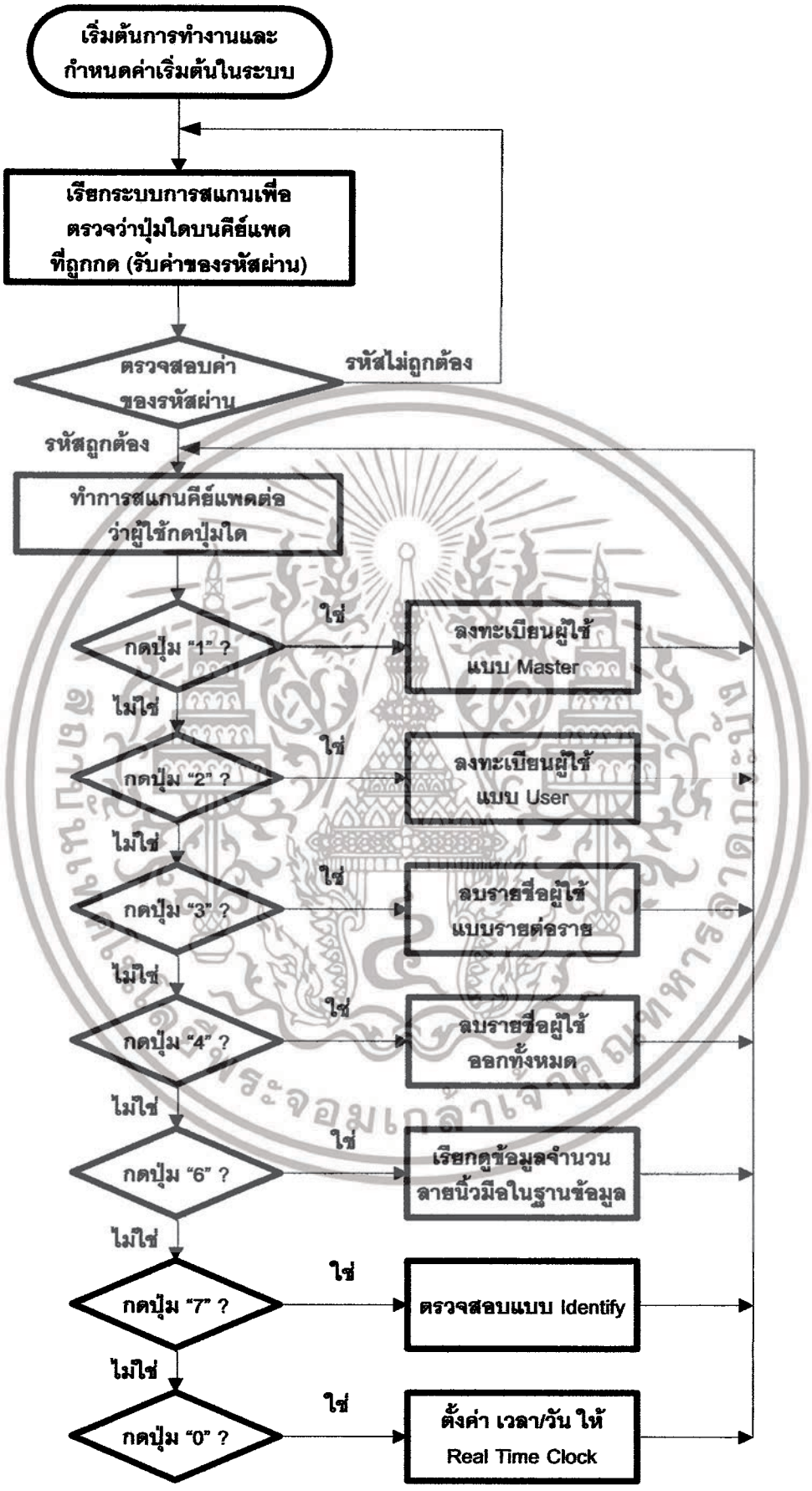
รูปที่ 3.15 วงจรขับรีเลย์

3.13 ส่วนของหลักการทำงานของซอฟต์แวร์

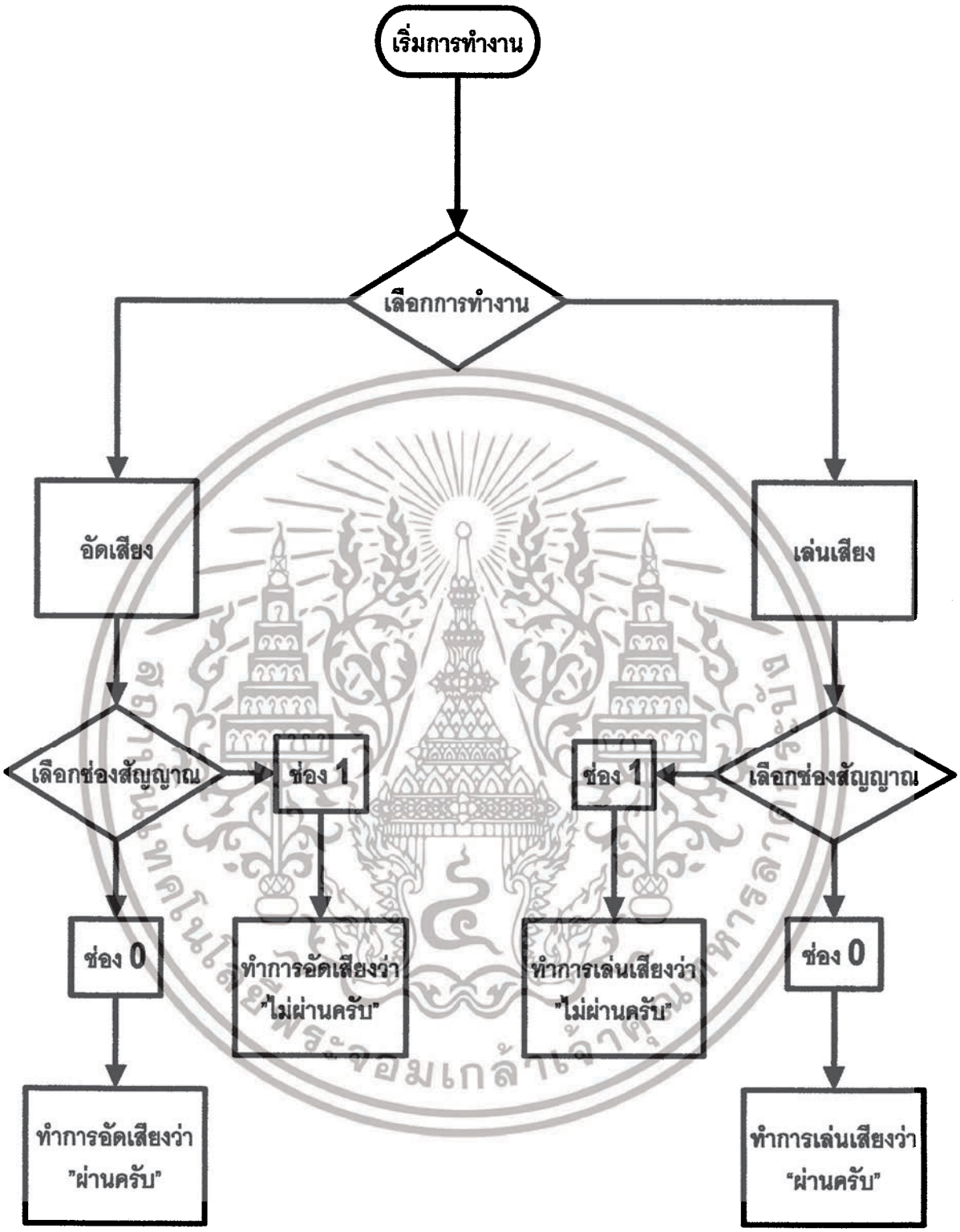
สำหรับซอฟต์แวร์ในโครงงานนี้จะประกอบด้วยซอฟต์แวร์ที่ไมโครคอนโทรลเลอร์AT89C4051 บนแผงวงจรซึ่งติดตั้งในรถยนต์และที่ไมโครคอนโทรลเลอร์P89C51RD2 บนเทอร์มินอลรับอินพุต ซึ่งการทำงานของทั้งคู่ต่างก็มีหน้าที่และกลไกที่แตกต่างกันซึ่งได้อธิบายอย่างคร่าวๆไว้ในโฟลวชาร์ตการทำงานของไมโครคอนโทรลเลอร์บนแผงวงจรควบคุมซึ่งติดตั้งในรถยนต์(รูปที่ 3.16) , โฟลวชาร์ตการทำงานของไมโครคอนโทรลเลอร์บนเทอร์มินอลรับข้อมูล(รูปที่ 3.17) และโฟลวชาร์ตการทำงานของวงจรบันทึกเสียง (รูปที่ 3.18)



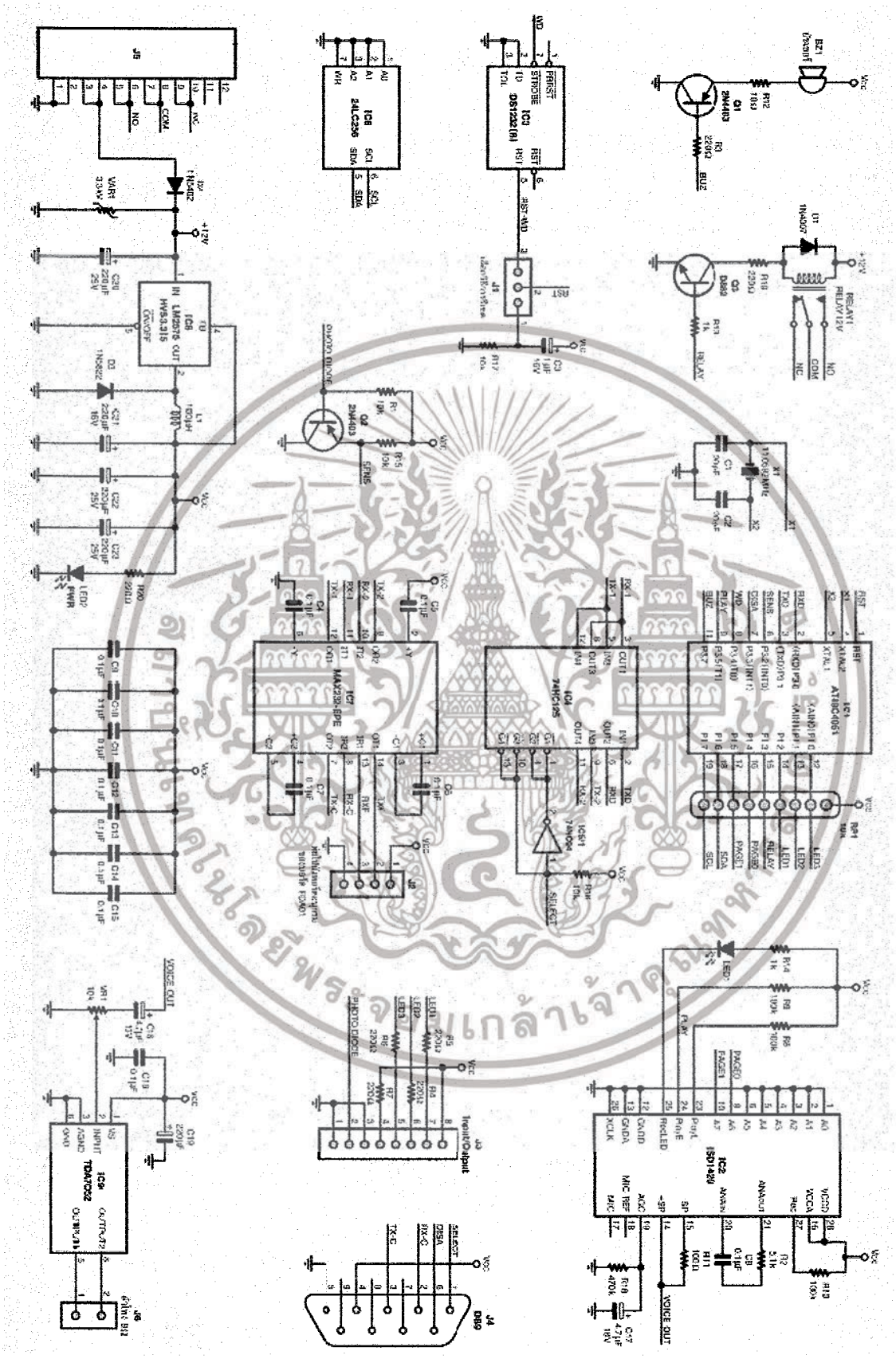
รูปที่ 3.16 โฟลวชาร์ตการทำงานของไมโครคอนโทรลเลอร์บนแผงวงจรควบคุมซึ่งติดตั้งในรถยนต์



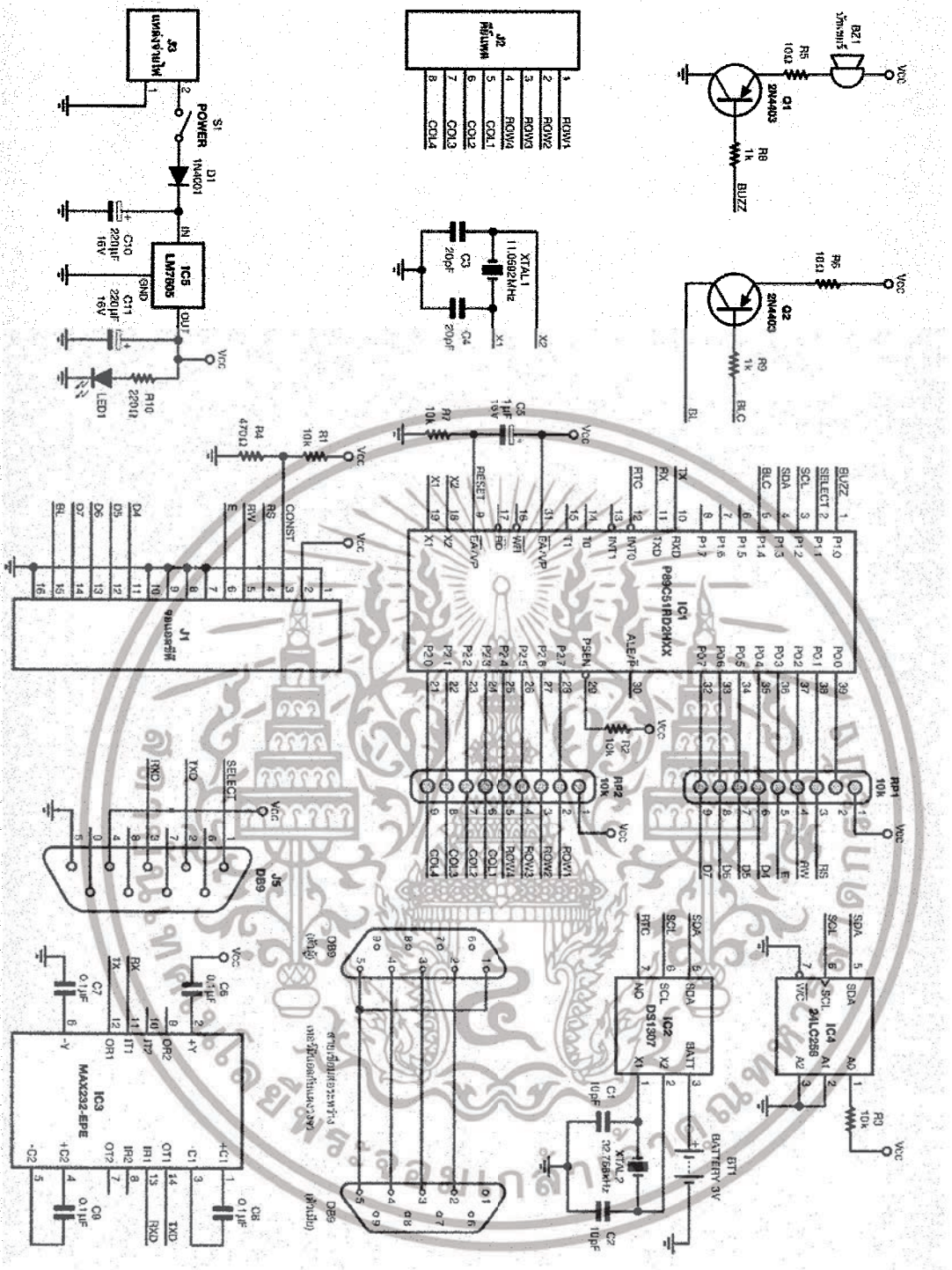
รูปที่ 3.17 โฟลวชาร์ตการทำงานของไมโครคอนโทรลเลอร์บนเทอร์มินอลรับข้อมูล



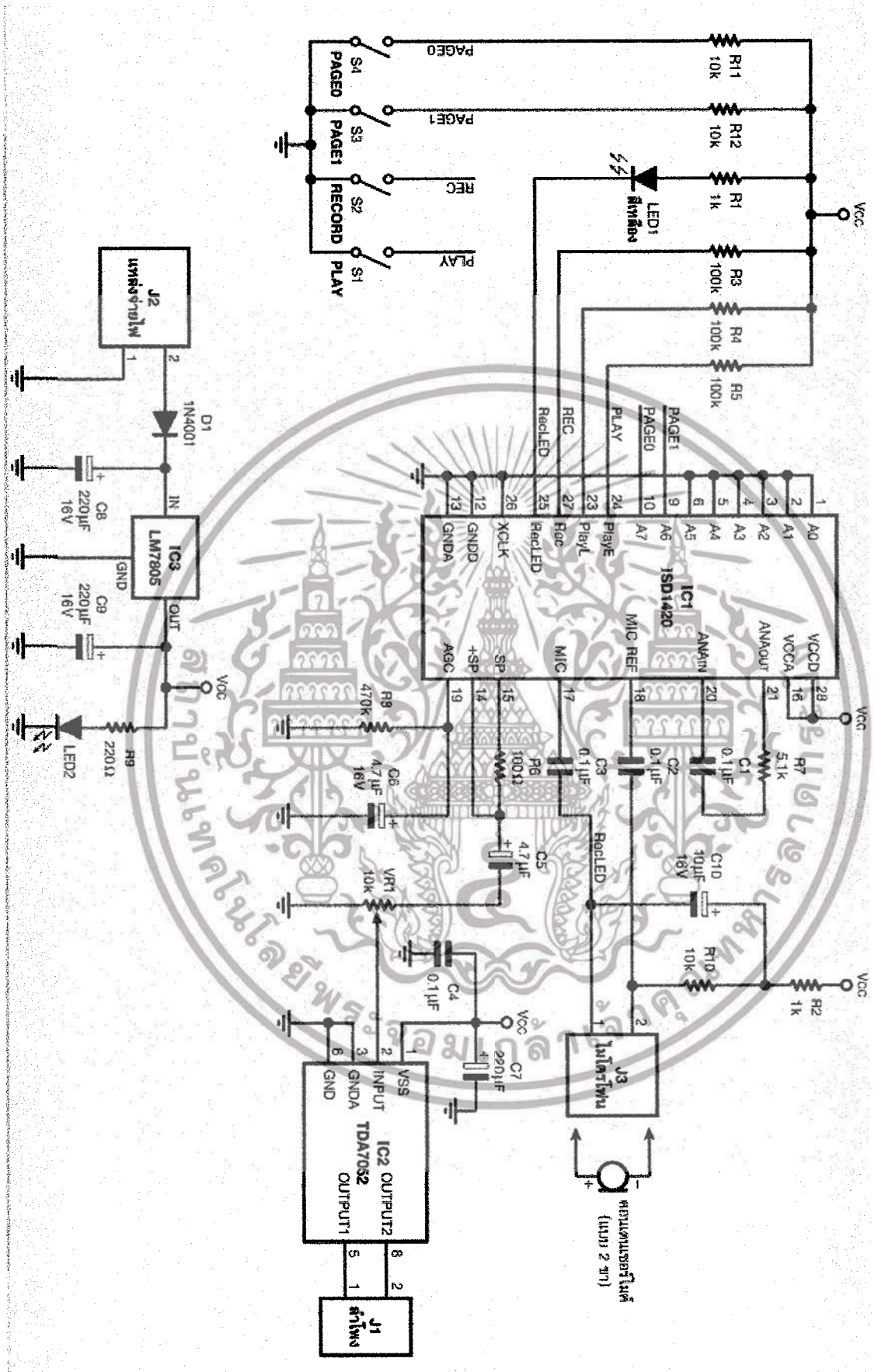
รูปที่ 3.18 โฟลวชาร์ตการทำงานของวงจรบันทึกเสียง



รูปที่ 3.19 รูปวงจรรวมของวงจรติดตั้งในรถยนต์



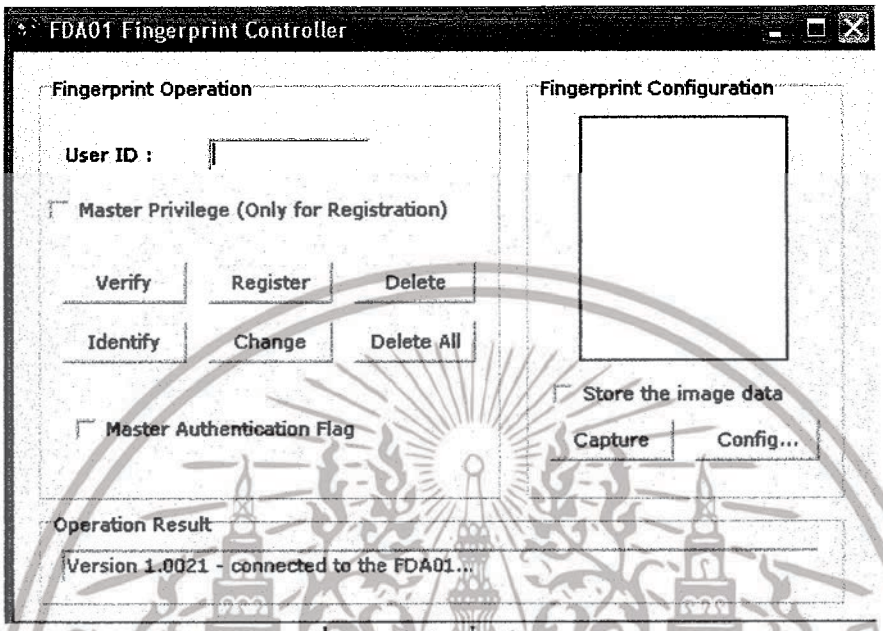
รูปที่ 3.20 รูปวงจรรวมของวงจรเทอร์มินอลรับข้อมูล



รูปที่ 3.21 รูปวงจรรวมของวงจรบันทึกเสียง

บทที่ 4
การทดลองและผลการทดลอง

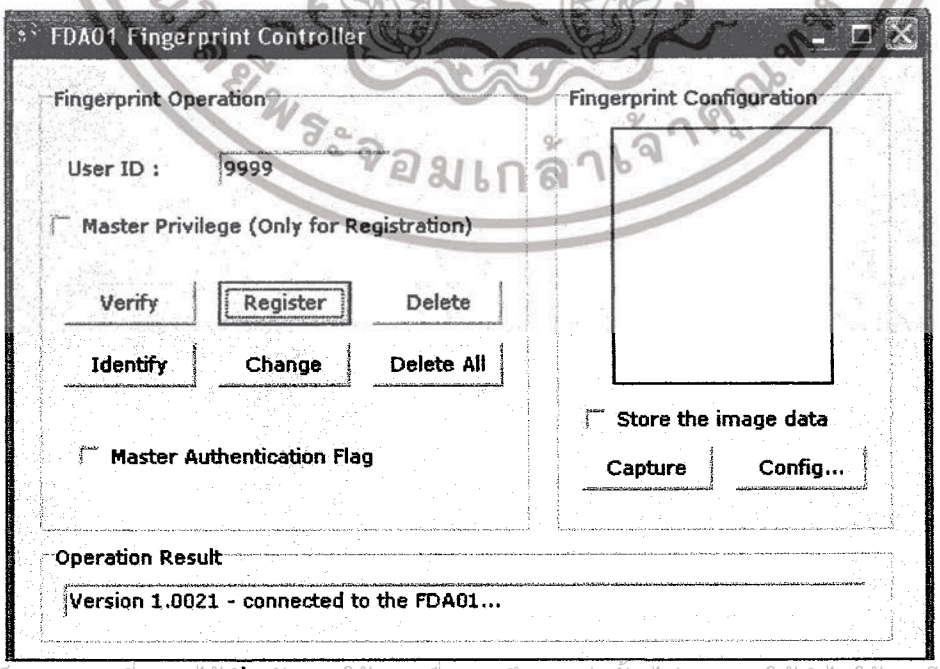
4.1 การทดลองของเครื่องสแกนลายนิ้วมือ โดยเชื่อมต่อเข้ากับคอมพิวเตอร์โดยตรง



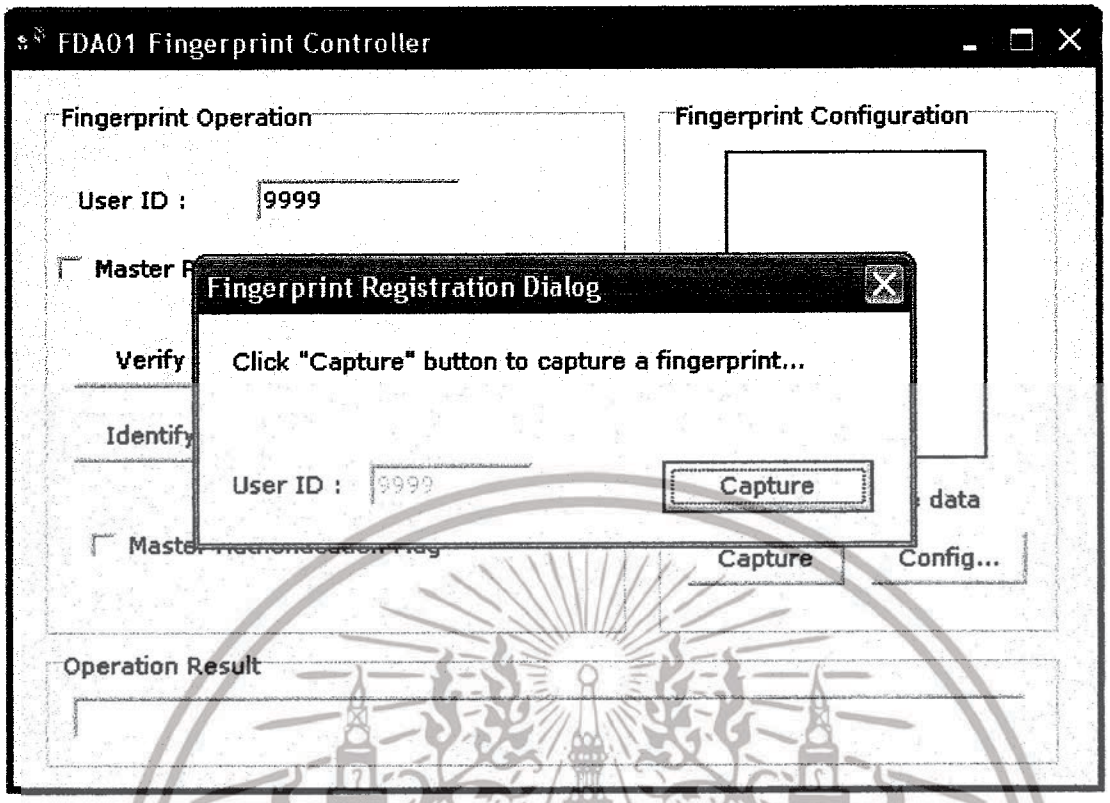
รูปที่ 4.1 หน้าต่างเมื่อเข้าสู่ระบบ

4.1.1 ขั้นตอนการลงทะเบียนข้อมูล

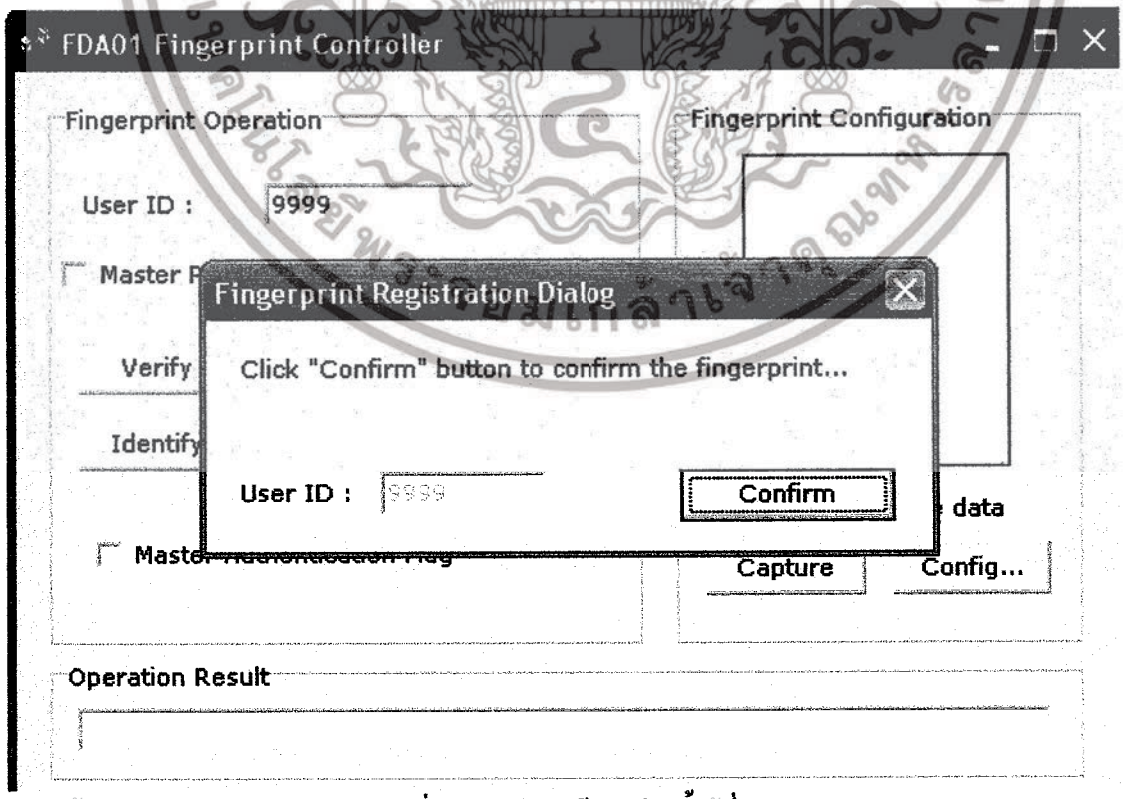
ทำการใส่ User ID ที่ต้องการ แล้วกดปุ่ม Register ทางโปรแกรมจะสั่งให้เราป้อนลายนิ้วมือเข้าดังรูปที่4.3 แล้วจากนั้นโปรแกรมจะสั่งให้เราป้อนลายนิ้วมือเพื่อยืนยันอีกครั้งหนึ่งดังรูปที่4.4 เมื่อเรายืนยันอีกครั้งหนึ่งแล้ว โปรแกรมก็จะทำการบันทึกข้อมูลของผู้ใช้ดังรูปที่4.5



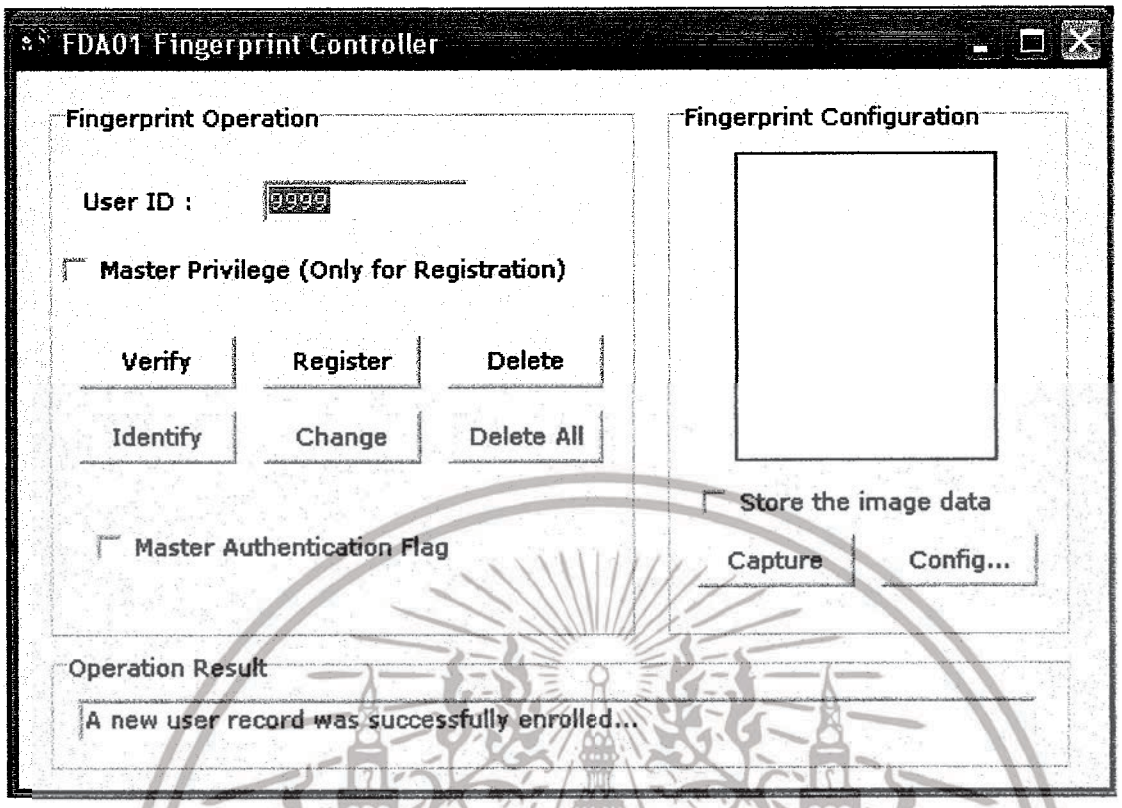
รูปที่ 4.2 การลงทะเบียนของผู้ใช้คนแรกด้วยรหัส 9999



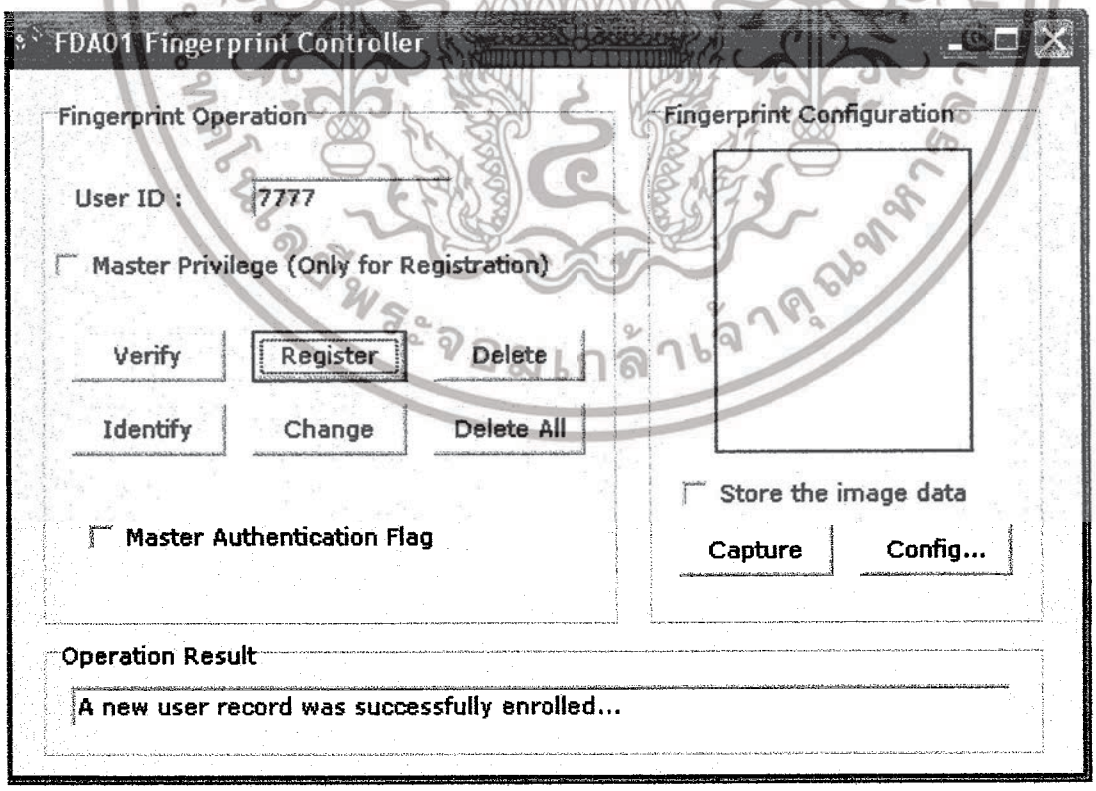
รูปที่ 4.3 การป้อนลายนิ้วมือเข้าสู่หน่วยความจำ



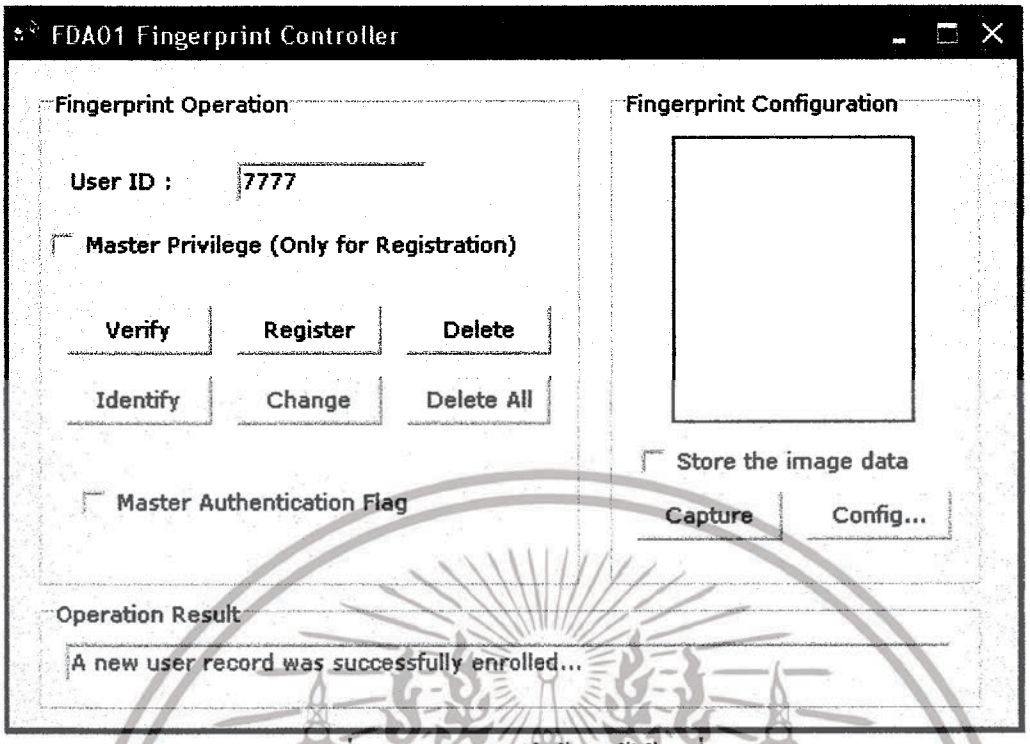
รูปที่ 4.4 การยืนยันข้อมูลอีกครั้งหนึ่ง



รูปที่ 4.5 แสดงการบันทึกข้อมูลผู้ใช้คนที่1



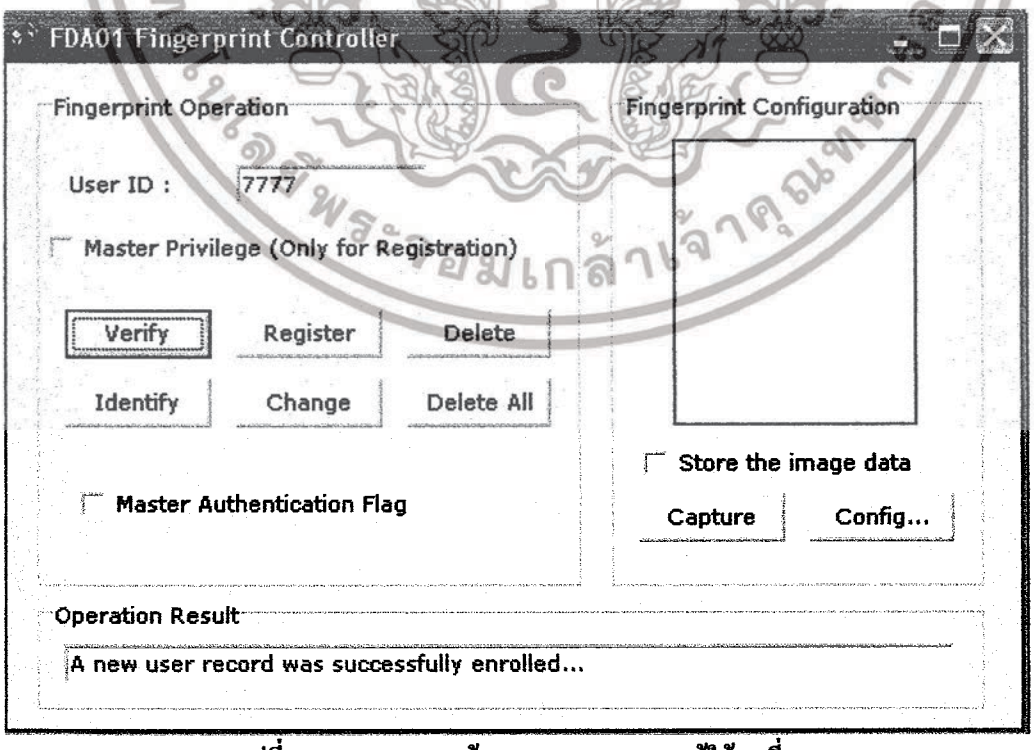
รูปที่4.6 การลงทะเบียนผู้ใช้คนที่สองด้วยรหัส 7777



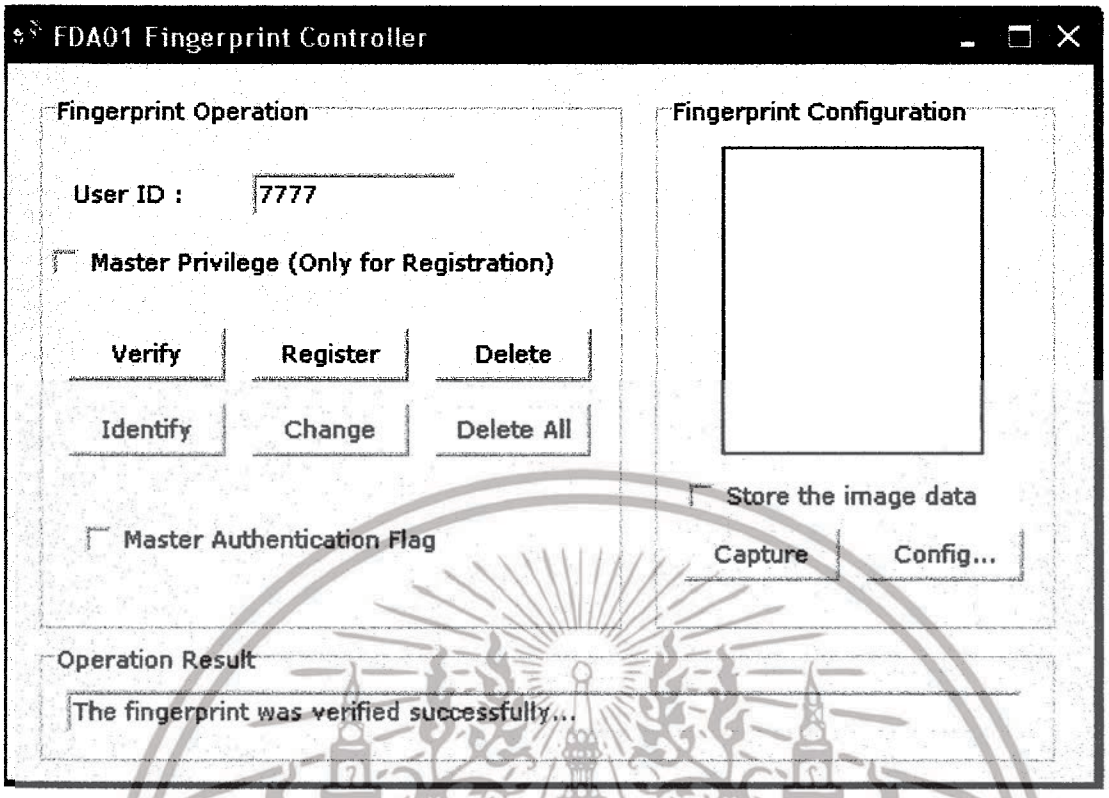
รูปที่4.7 แสดงการบันทึกข้อมูลผู้ใช้คนที่ 2

4.1.2 การตรวจสอบลายนิ้วมือแบบ 1:1(Verify)

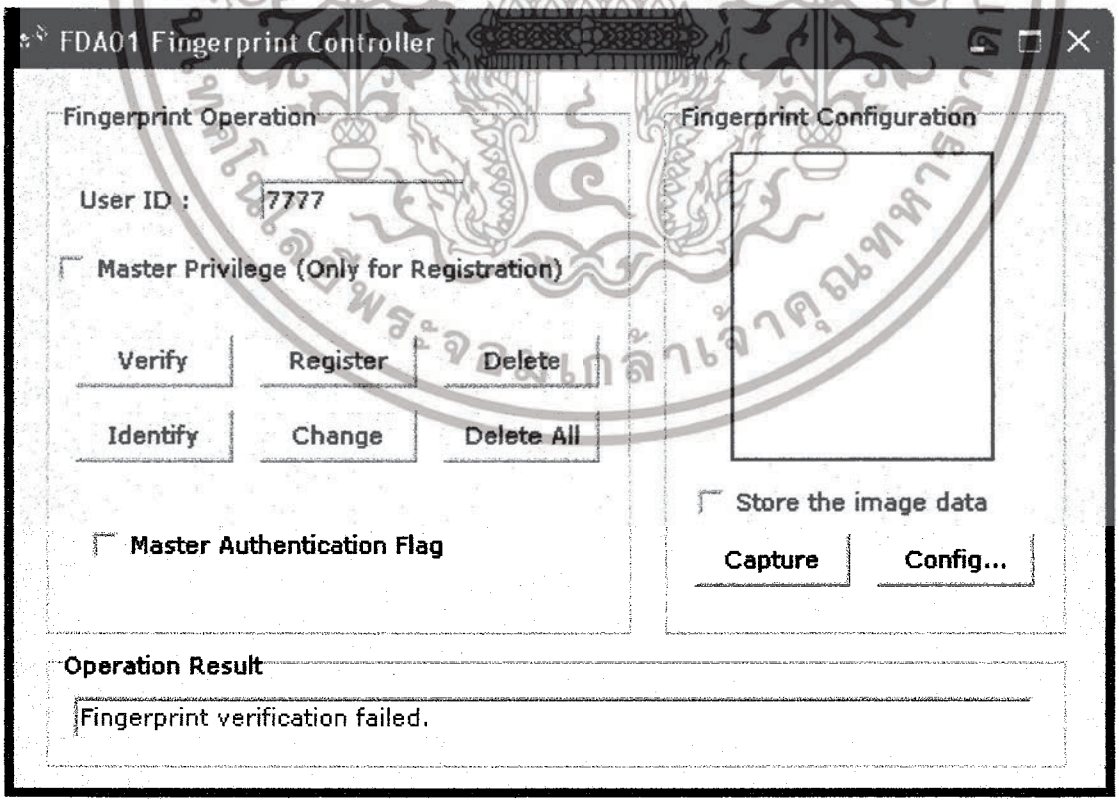
เป็นการตรวจสอบแบบ 1:1 โดยเปรียบเทียบลายนิ้วมือที่อ่านจากฟิงเกอร์พริ้นต์เซนเซอร์เปรียบเทียบกับเท็มเพลตลายนิ้วมือของผู้ใช้ลายนั้นๆ ที่ถูกเก็บไว้ในฐานข้อมูลก่อนว่าตรงกันหรือไม่ หากตรงกันก็จะอนุญาตให้ผู้ใช้สามารถใช้งานได้ แต่หากไม่ตรงกันก็จะไม่อนุญาตให้ผู้ใช้ใช้งาน



รูปที่4.8 การตรวจสอบข้อมูลแบบ Verify ของผู้ใช้คนที่ 2



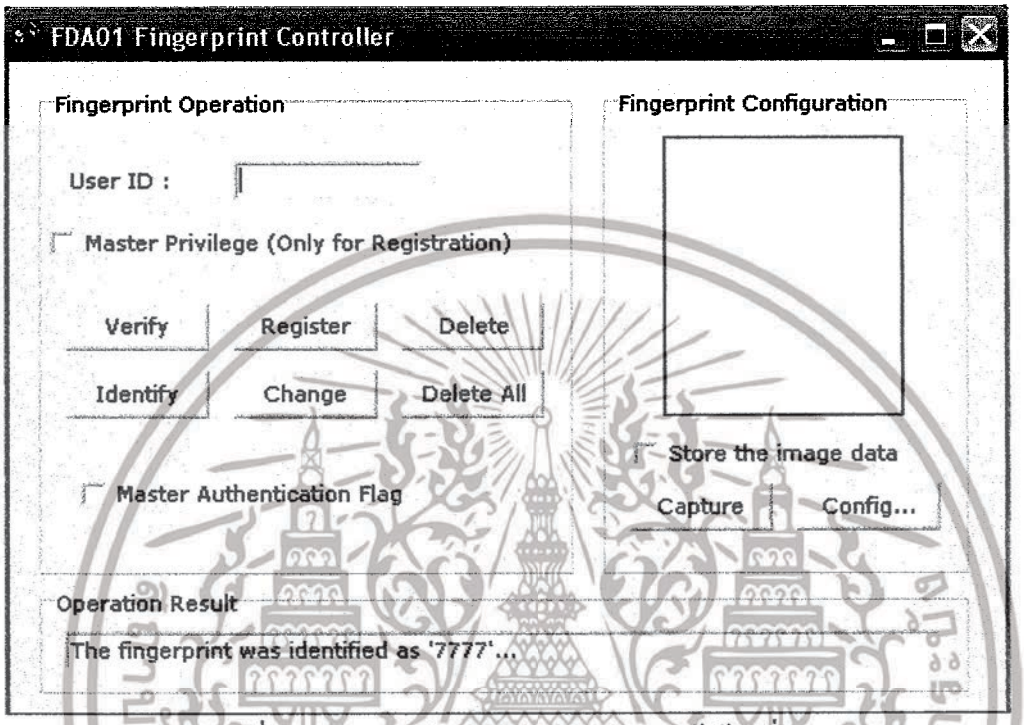
รูปที่ 4.9 การตรวจสอบแบบ Verify ที่รหัสข้อมูลตรงกับลายนิ้วมือของผู้ใช้



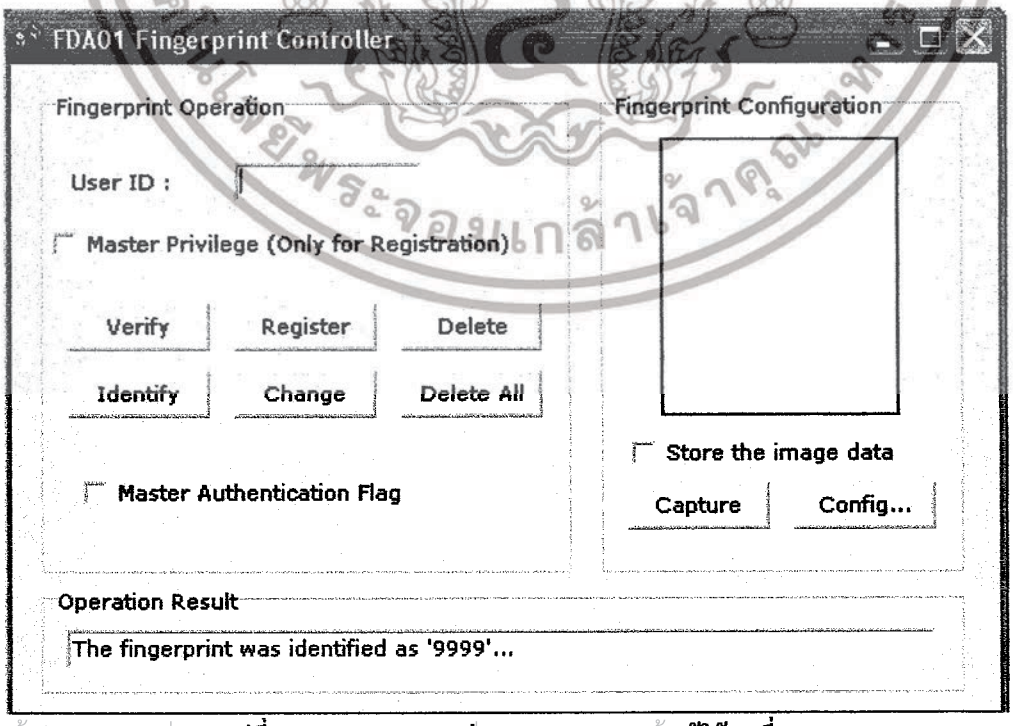
รูปที่ 4.10 การตรวจสอบแบบ Verify ที่รหัสข้อมูลไม่ตรงกับลายนิ้วมือของผู้ใช้

4.1.3 การตรวจสอบลายนิ้วมือแบบ 1:N (Identify)

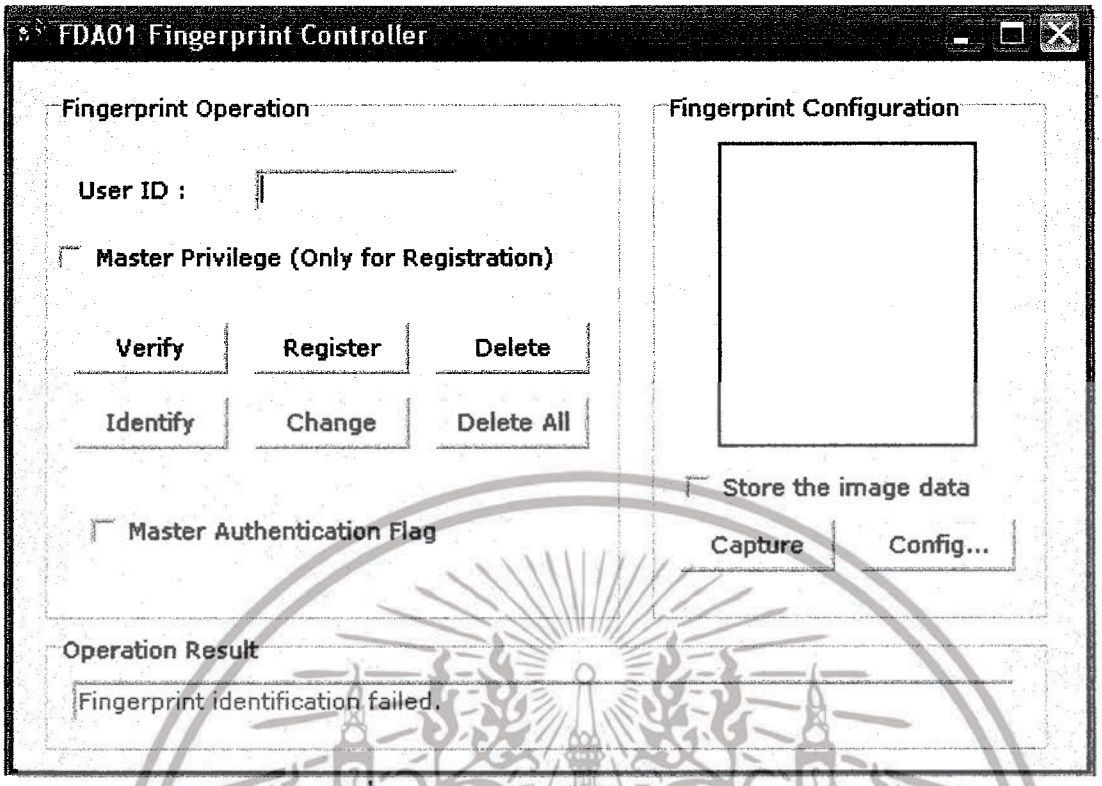
เป็นการตรวจลักษณะการจับคู่แบบหนึ่งต่อจำนวนมากกว่า คือการเปรียบเทียบเท็มเพลตของลายนิ้วมือที่อ่านได้จากฟิงเกอร์พริ้นต์เซนเซอร์กับเท็มเพลตของผู้ใช้จำนวนมากในฐานเพื่อดูข้อมูลตรงกับเท็มเพลตของผู้ใช้รายใด โดยการเปรียบข้อมูลทั้งหมดตั้งแต่เท็มเพลตแรกไปยังเท็มเพลตสุดท้าย หากมีข้อมูลอยู่ในเท็มเพลตก็จะอนุญาตให้ผู้ใช้งานใช้งานได้



รูปที่ 4.11 การตรวจผ่านสอบแบบ Identify ของผู้ใช้คนที่ 2

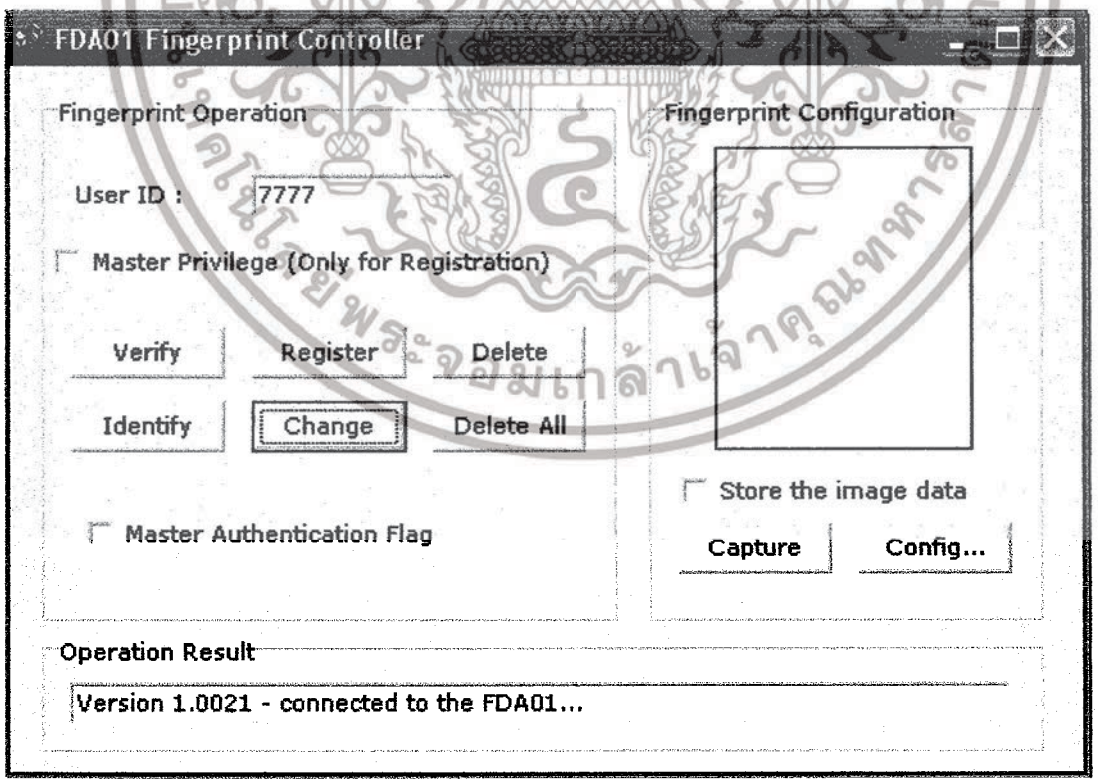


รูปที่4.12 การตรวจสอบผ่านแบบ Identify ของผู้ใช้คนที่ 1

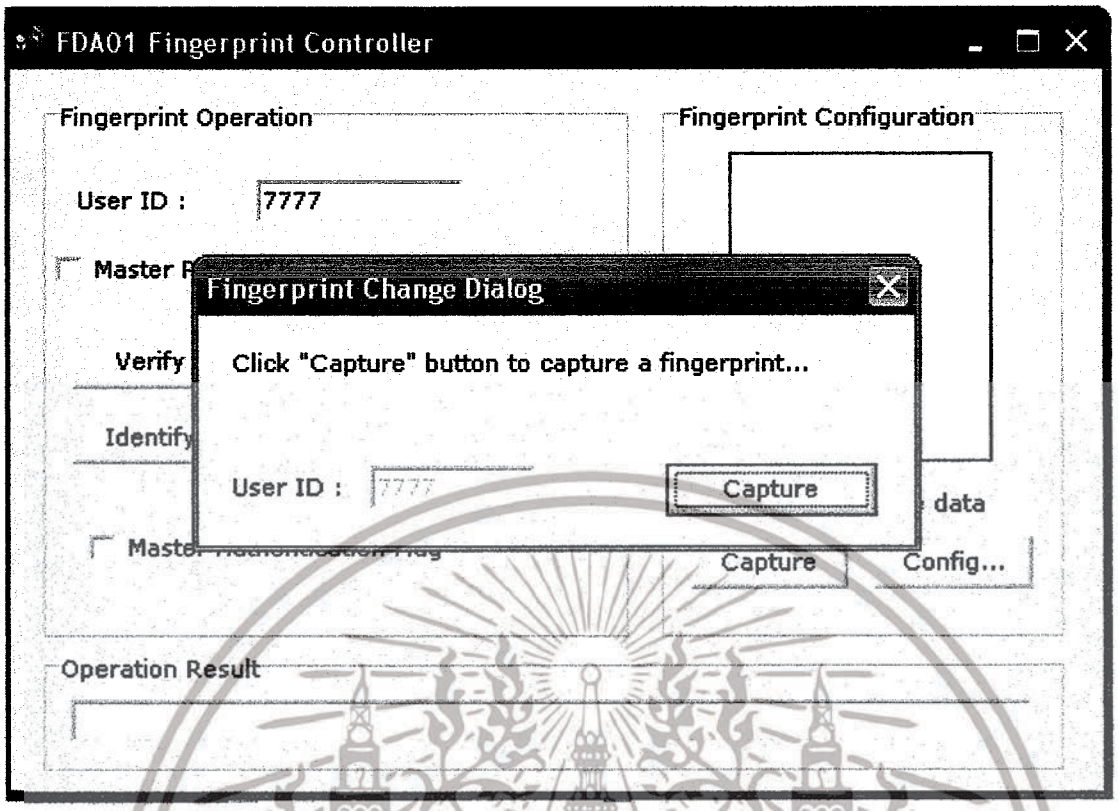


รูปที่ 4.13 การตรวจสอบไม่ผ่านแบบ Identify

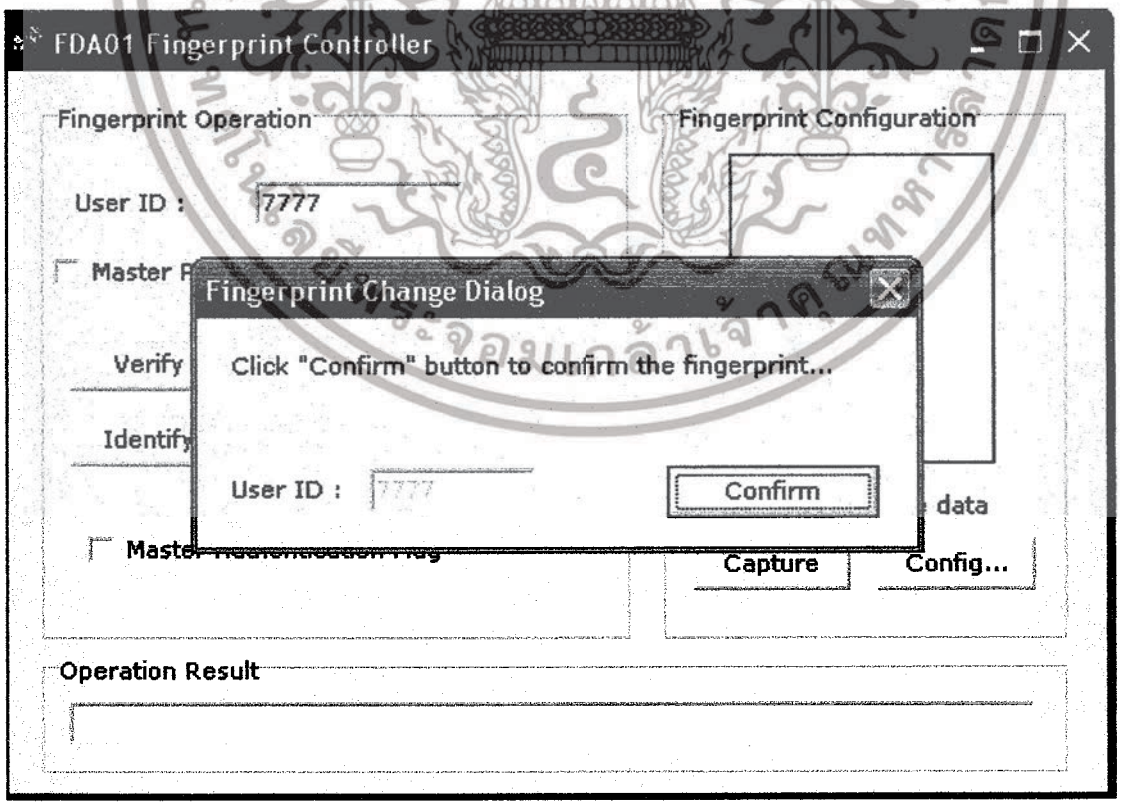
4.1.4 การเปลี่ยนผู้ใช้งานโดยใช้รหัสเดิม (Change)



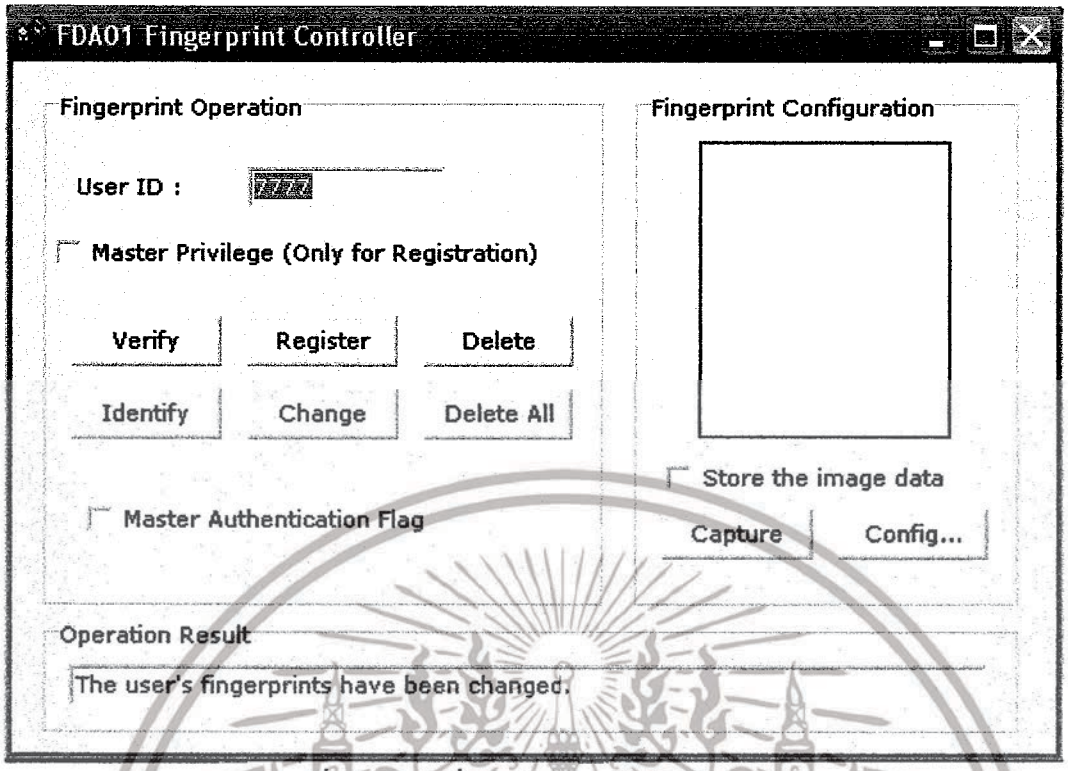
รูปที่ 4.14 การเปลี่ยนข้อมูลผู้ใช้เดิมที่ใช้รหัส 7777 เป็นผู้ใช้คนใหม่



รูปที่ 4.15 การป้อนลายนิ้วมือของผู้ใช้คนใหม่ที่ต้องการรหัส 7777

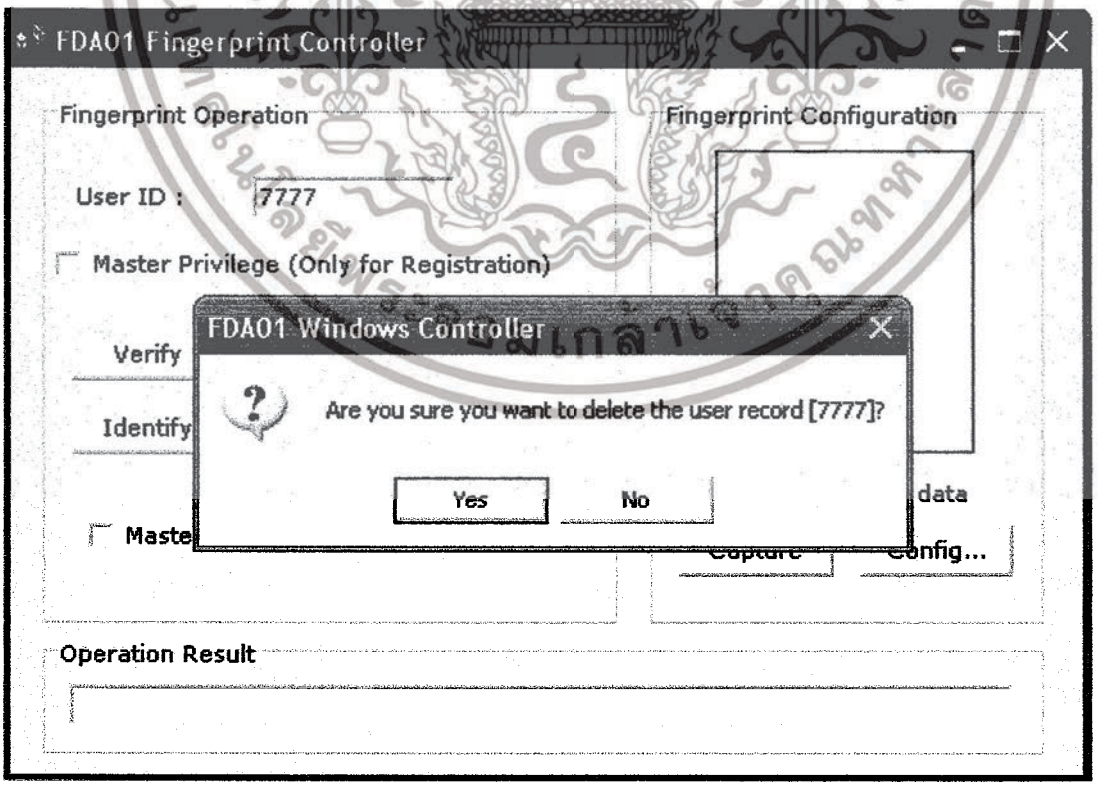


รูปที่ 4.16 การยืนยันลายนิ้วมือของผู้ใช้คนใหม่อีกครั้ง

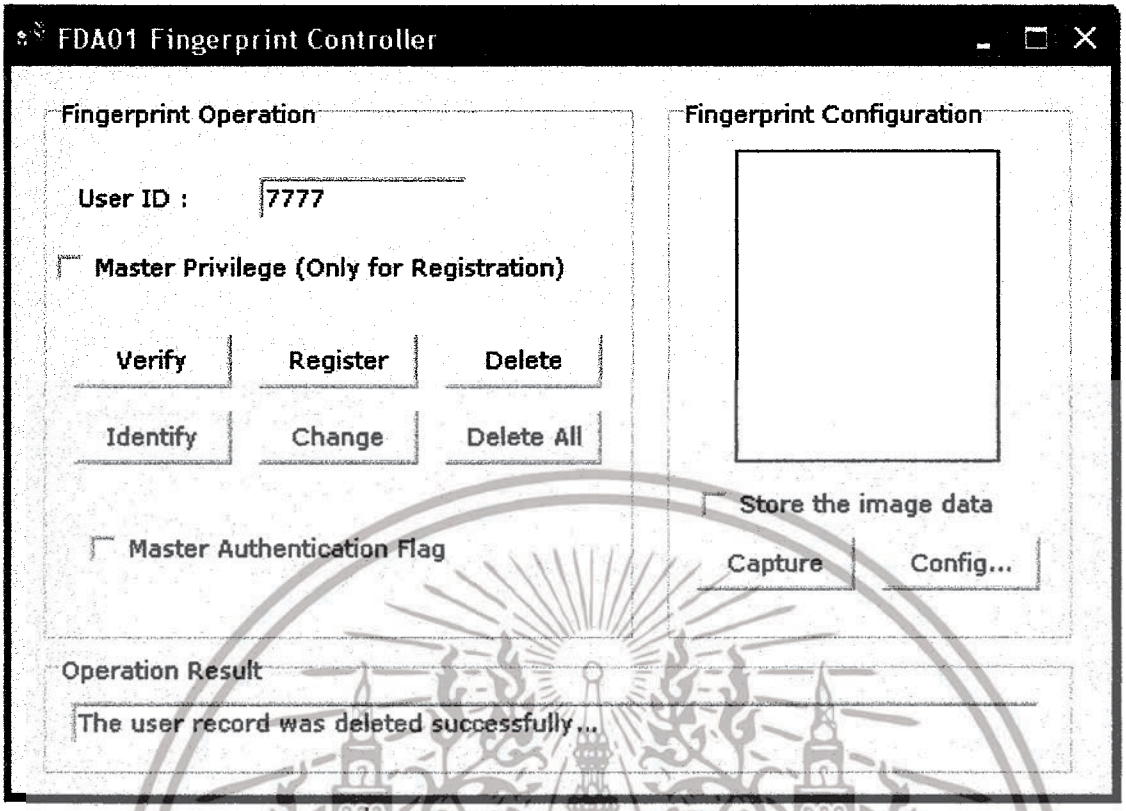


รูปที่ 4.17 การเปลี่ยนแปลงข้อมูลผู้ใช้เสร็จสมบูรณ์

4.1.5 การลบข้อมูลผู้ใช้ที่ละข้อมูล (Delete)

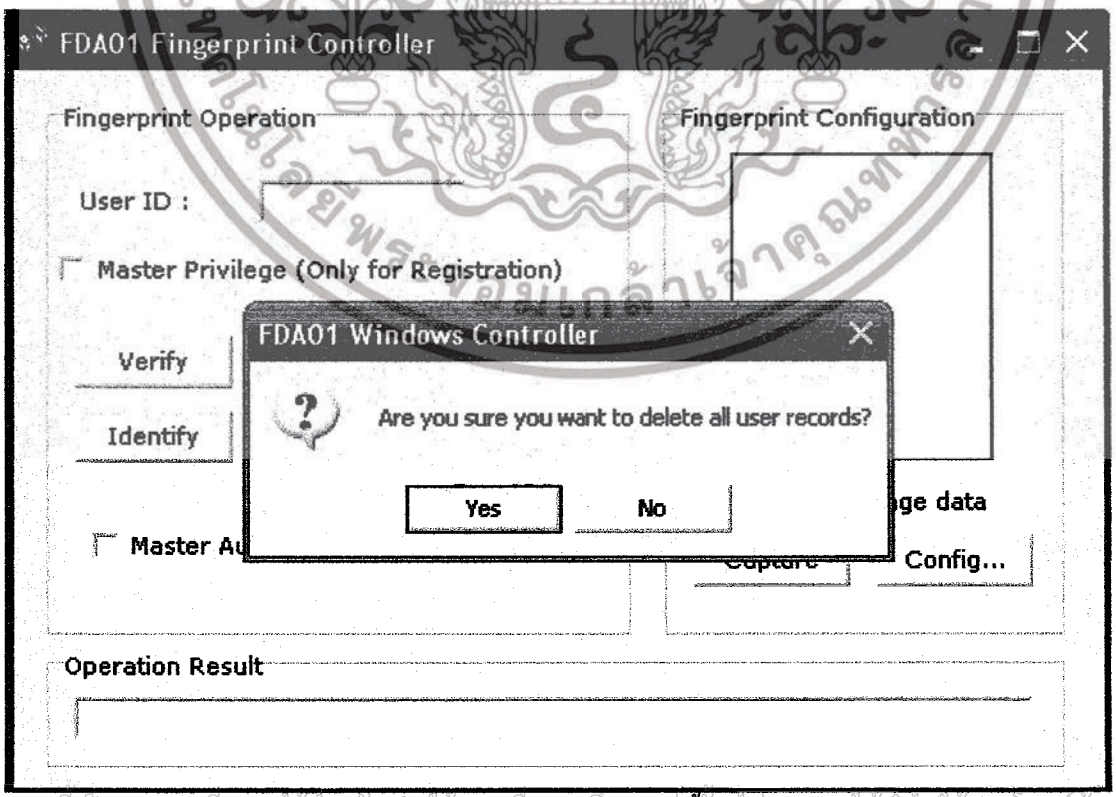


รูปที่ 4.18 การลบข้อมูลผู้ใช้ที่มีรหัส 7777

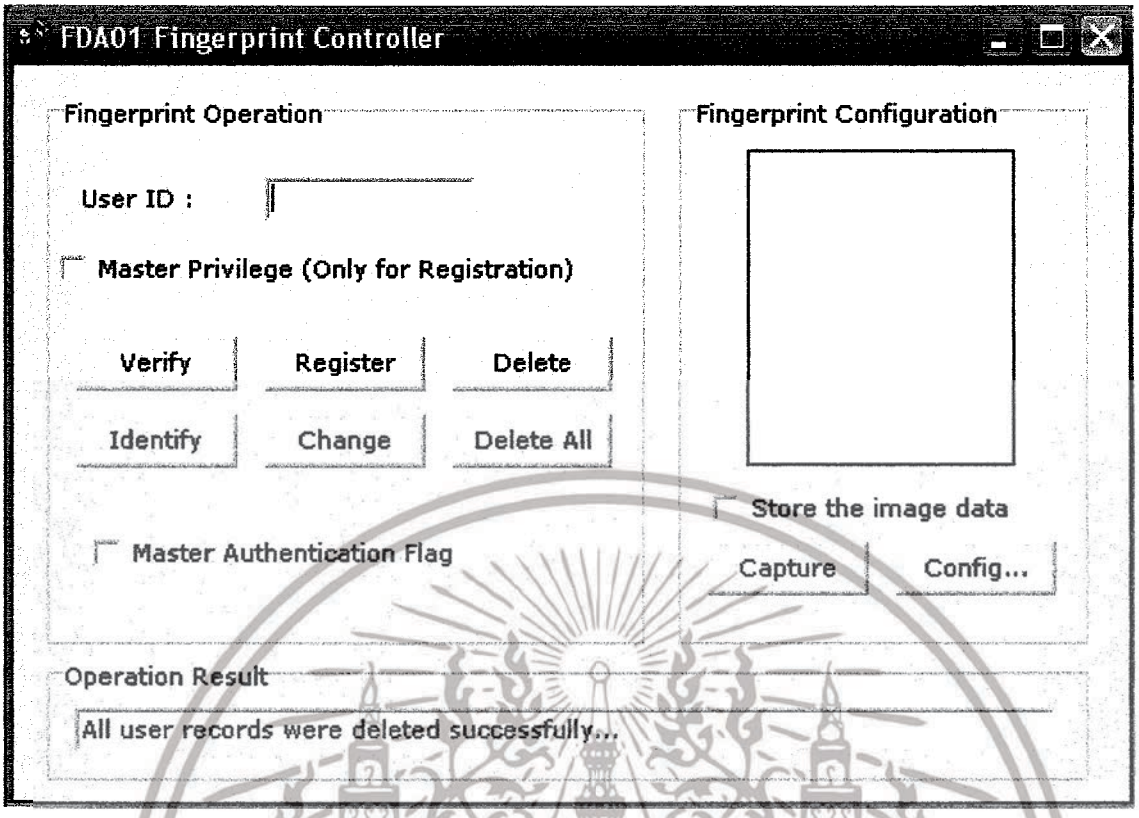


รูปที่ 4.19 ยืนยันการลบข้อมูลของผู้ใช้รหัส 7777

4.1.6 การลบข้อมูลของผู้ใช้ที่มีอยู่ในระบบทั้งหมด (Delete All)



รูปที่ 4.20 การลบข้อมูลของผู้ใช้ทั้งหมด



รูปที่ 4.21 ยืนยันการลบของมูลทั้งหมด

4.2 การทดลองของเครื่องสแกนลายนิ้วมือ

ครั้งที่	นิ้วที่รีจิสเตอร์ไว้ในฐานข้อมูลแล้ว		นิ้วที่ไม่ได้รีจิสเตอร์ไว้ในฐานข้อมูล	
	แสงสว่างปกติ	มีแสงรบกวนจากภายนอก	แสงสว่างปกติ	มีแสงรบกวนจากภายนอก
1	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
2	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
3	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
4	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
5	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
6	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
7	ผ่าน	ไม่ผ่าน	ไม่ผ่าน	ไม่ผ่าน
8	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
9	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
10	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน

ตารางที่ 4.1 การทดลองของเครื่องสแกนลายนิ้วมือ

4.3 การทดลองของเครื่องติดตั้งในรถยนต์

ขั้นตอนแรกเมื่อทำการเปิดระบบ บอร์ดจะรอคอยการป้อนรหัสผ่านคือลายนิ้วมือ เมื่อมีการวางนิ้วมือลงบนฟิงเกอร์พรินต์เซนเซอร์ นิ้วมือจะมาอยู่ในตำแหน่งสะท้อนลำแสงอินฟราเรด โดย AT89C4051 จะตรวจพบการเปลี่ยนแปลง แล้วระบบจะเริ่มทำงานและสั่งการให้บอร์ดควบคุม FDA01 อ่านลายนิ้วมือจากฟิงเกอร์พรินต์เซนเซอร์ เพื่อใช้เป็นอินพุตสำหรับนำมาเปรียบเทียบกับข้อมูลลายนิ้วมือที่ได้เก็บบันทึกไว้ในฐานข้อมูล โดยตรวจสอบแบบ 1:N ถ้าตรวจสอบแล้วพบว่าลายนิ้วมือที่นำมาตรวจสอบตรงกับฐานข้อมูลที่มีอยู่ หลอดไฟจะติดและเครื่องจะส่งเสียงบอกว่า "ผ่าน" รถก็จะสามารถสตาร์ทได้ แต่ถ้าตรวจสอบแล้วพบว่าลายนิ้วมือที่นำมาตรวจสอบไม่ตรงกับฐานข้อมูลที่มีอยู่ เครื่องจะส่งเสียงบอกว่า "ไม่ผ่าน" และบัซเซอร์จะส่งเสียงดังเตือนพร้อมทั้งทำให้รถไม่สามารถสตาร์ทได้

บทที่ 5
บทสรุปและแนวทางในการพัฒนาต่อ

5.1 สรุปผลการทดลอง

โครงงานนี้เป็นการทดลองเกี่ยวกับระบบรักษาความปลอดภัยโดยใช้เครื่องสแกนลายนิ้วมือในการตรวจสอบความถูกต้อง เพื่อระบุตัวบุคคลว่าตรงกับที่บันทึกไว้หรือไม่ จากการทดสอบความถูกต้องของการสแกนลายนิ้วมือพบว่าการตรวจสอบมีความแม่นยำมาก ทำให้เราสามารถมั่นใจได้ว่าจะไม่มีบุคคลใดที่ไม่ได้ระบุตัวตนลงในฐานข้อมูลจะสามารถผ่านระบบรักษาความปลอดภัยมาได้ โดยจะมีบัซเซอร์ดังขึ้นมาแจ้งเตือนเมื่อบุคคลที่ไม่ได้ระบุตัวตนลงในฐานข้อมูลมาทำการสแกนลายนิ้วมือ จึงนับได้ว่าเป็นทางเลือกที่ดีมากอีกทางหนึ่งสำหรับคนที่ต้องการความมั่นใจในความปลอดภัย

5.2 บทวิจารณ์

- เครื่องสแกนลายนิ้วมือมีโอกาสผิดพลาดมากขึ้นเนื่องจากผลกระทบจากแสงภายนอก
- โปรแกรมสั่งให้ระบบแจ้งเตือนโดยการให้บัซเซอร์ดังขึ้นเมื่อสแกนลายนิ้วมือไม่ผ่าน ปกติแล้วถ้าสแกนไม่ผ่านครั้งเดียวระบบจะแจ้งเตือนทันที ดังนั้นจึงควรเพิ่มจำนวนครั้งให้มากขึ้นถึงจะส่งเสียงเตือนเพื่อให้ผู้ตรวจสอบมีโอกาสมากขึ้นเพราะผู้ตรวจสอบอาจวางนิ้วช้าหรือวางนิ้วไม่ถูกวิธีได้

เอกสารอ้างอิง

1. การประยุกต์ใช้งานไมโครคอนโทรลเลอร์ ตระกูล MCS-51 โดย รศ. สมยศ จุณณะปิยะ, ภาควิชาวิศวกรรมโทรคมนาคม, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2546

2.ระบบการทำงานของอุปกร์ต่างๆจาก www.jnutthailand.com