



แบบจำลองการควบคุมเข้าใช้งานระบบโดยการพิสูจน์ลายพิมพ์นิ้วมือ

สุจิตรา อุดลย์เกษม* จิตดำรง ปรีชาสุข* เจนจิรา รงค์รัตน์* และ วรกต ตั้งศิริมงคล*

บทคัดย่อ

งานวิจัยนี้นำเสนอแบบจำลองการควบคุมเข้าใช้งานระบบ โดยการใช้การพิสูจน์ลายพิมพ์นิ้วมือ (System Access Control Model using Fingerprint Verification) โดยแบบจำลองทำงานในลักษณะไคลเอนต์-เซิร์ฟเวอร์ แบบจำลองสามารถทำการยืนยันบุคคลที่มีสิทธิ์เข้าใช้พื้นที่/ระบบ และสามารถพิสูจน์บุคคลด้วยลายนิ้วมือ เปอร์เซนต์ความถูกต้องในการพิสูจน์บุคคลด้วยลายนิ้วมือเป็น 80.56 % และแบบจำลองสามารถตรวจสอบการเข้าใช้ระบบ โดยมีเปอร์เซนต์ความถูกต้อง 98.12 %

คำสำคัญ: การควบคุมการเข้าใช้ระบบ, การพิสูจน์ลายพิมพ์นิ้วมือ, การรู้จำไบโอเมตริกซ์

1. บทนำ

ระบบรักษาความปลอดภัยที่ใช้กันในปัจจุบันนั้น เป็นการรักษาความปลอดภัยโดยการตรวจบัตรประจำตัวหรือรหัสผ่าน ซึ่งพบว่าเกิดปัญหาคือ ระดับความปลอดภัยไม่สูงมาก และเกิดความไม่สะดวก เนื่องจากบัตรหรือรหัสผ่านเป็นสิ่งที่สามารถใช้แทนกันได้ ปลอมแปลงได้ง่าย และผู้ใช้อาจลืมรหัสผ่านหรือลืมพกพาบัตรประจำตัว จึงได้มีการนำเอาเทคโนโลยีการรู้จำไบโอเมตริกซ์ (Biometrics Recognition) เข้ามาช่วยในระบบรักษาความปลอดภัยหรือพิสูจน์บุคคล ตัวอย่างของไบโอเมตริกซ์ เช่น ใบหน้า, ลักษณะฝ่ามือ, ลายพิมพ์นิ้วมือ และอื่นๆ เป็นที่ยอมรับกันทั่วไปว่า ลายพิมพ์นิ้วมือให้ความปลอดภัยสูงสำหรับที่จะนำมาใช้ในการพิสูจน์บุคคล [1] งานวิจัยนี้ได้นำเสนอแบบจำลองการควบคุมเข้าใช้งานระบบ โดยใช้ลายพิมพ์นิ้วมือสำหรับการยืนยันตัวบุคคล เพื่อให้เกิดความมั่นใจได้ว่าบุคคลที่มีสิทธิ์เท่านั้น (Authorized) สามารถเข้าไปใช้งานระบบได้ ทำให้การเข้าใช้งานระบบมีระดับความปลอดภัยที่สูงมากขึ้น โดยที่งานวิจัยได้มีการ

- นำเสนอแบบจำลองการเข้าใช้งานระบบใหม่ โดยการใช้การพิสูจน์ลายพิมพ์นิ้วมือ

- พัฒนาแบบจำลองการเข้าใช้งานระบบโดยการใช้การพิสูจน์ลายพิมพ์นิ้วมือ

2. วารณกรรมที่เกี่ยวข้อง

ในส่วนนี้จะอธิบายเกี่ยวกับ ทฤษฎีการรู้จำไบโอเมตริกซ์ (Biometric Recognition) ตลอดจนความรู้เกี่ยวกับการพิสูจน์ลายพิมพ์นิ้วมือ (Fingerprint Verification) โดยสรุป จากนั้นเป็นการสรุปงานวิจัยที่เกี่ยวข้องกับการลายพิมพ์นิ้วมือ และสรุปงานวิจัยที่เกี่ยวข้องกับการเข้าใช้งานระบบ (System Access Control)

2.1 ทฤษฎีการรู้จำไบโอเมตริกซ์ (Biometrics Recognition)

ไบโอเมตริกซ์ (Biometrics) มาจากภาษากรีก 2 คำ คือ “Bios” (life) หมายถึงชีวิตหรือความมีชีวิต และ “Metro” (Measure) หมายถึงการวัดหรือมาตรวัด ดังนั้น Biometrics จึงหมายความว่า วิธีการหรือเทคนิคในการตรวจสอบ, แยกแยะสิ่งมีชีวิต โดยวัดจากคุณลักษณะของสิ่งมีชีวิตนั้นๆ แล้วนำมาเปรียบเทียบกับคุณลักษณะอื่นๆ ที่ได้มีการบันทึกไว้ก่อนหน้านี้ในฐานข้อมูล เพื่อวัตถุประสงค์ในการแยกแยะ (Recognize)

ไบโอเมตริกซ์สามารถแบ่งออกได้เป็น 2 ประเภทใหญ่ๆ คือ

- ไบโอเมตริกซ์ทางกายภาพ (Physiology Biometrics) เช่น ลายพิมพ์นิ้วมือ (Fingerprint) โครงหน้า (Face) รูม่านตา (Iris) ฯลฯ

- ไบโอเมตริกซ์ทางพฤติกรรม (Behavioral Biometrics) เช่น เสียง (Voice) ลายเซ็นต์ (Signature) ฯลฯ

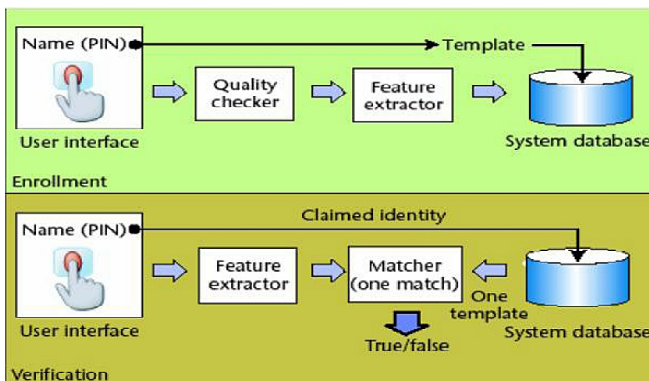
การใช้งานไบโอเมตริกซ์ แบ่งออกเป็น 2 ประเภทใหญ่ คือ

* ภาควิชาคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

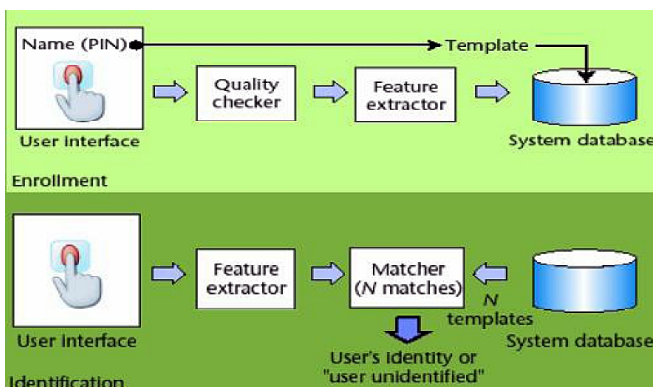


• เพื่อยืนยันตัวบุคคล (Verification) การใช้งานในกรณีนี้ จะมีการเปรียบเทียบข้อมูลไบโอเมตริกซ์ที่เก็บได้ใหม่ ณ จุดใช้งาน กับข้อมูลของบุคคลนั้นที่ได้เคยลงทะเบียนไว้เพื่อพิสูจน์ว่าบุคคลนั้น ๆ เป็นตัวจริง เป็นการเปรียบเทียบแบบหนึ่งต่อหนึ่ง ขั้นตอนการทำงานแสดงในภาพที่ 1

• เพื่อระบุตัวบุคคล (Identification) กรณีนี้จะต้องเทียบข้อมูลไบโอเมตริกซ์ที่เก็บใหม่ ณ จุดใช้งาน กับข้อมูลไบโอเมตริกซ์ทั้งหมดที่มีอยู่ในฐานข้อมูล เพื่อพิสูจน์ว่าบุคคลที่เป็นเจ้าของข้อมูลที่เก็บ ณ จุดใช้งานนั้นเป็นใครในฐานข้อมูล ถือว่าเป็นการเปรียบเทียบหนึ่งต่อหลายๆ ต้นแบบ ขั้นตอนการทำงานแสดงในภาพที่ 2



ภาพที่ 1 ขั้นตอนการทำงานแบบยืนยันตัวบุคคล [1]



ภาพที่ 2 ขั้นตอนการทำงานแบบระบุตัวบุคคล [1]

2.2 การรู้จำลายนิ้วมือ (Fingerprint Recognition)

ลายนิ้วมือ (Fingerprint) ในแต่ละบุคคลนั้นจะมีรูปแบบเฉพาะตัว และไม่มีการเปลี่ยนแปลงรูปแบบตามกาลเวลา (แต่อาจเปลี่ยนขนาดได้) ซึ่งปลอมแปลงได้ยาก จึงมีความน่าเชื่อถือสูง ตารางที่ 1 แสดงคุณลักษณะต่าง ๆ ของลายพิมพ์นิ้วมือ จะเห็นได้ว่าลายพิมพ์นิ้วมือมีลักษณะของการเป็น Distinc-

tiveness คือ ลักษณะที่แสดงความเป็นหนึ่งเดียว เฉพาะสูง ซึ่งเหมาะสมอย่างยิ่งในการที่จะนำไปใช้ในการพิสูจน์บุคคล

ตารางที่ 1 คุณลักษณะของลายพิมพ์นิ้วมือ [1]

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	H	M	M

H = High, M = Medium, L = Low

2.3 งานวิจัยที่เกี่ยวข้องกับการพิสูจน์ลายนิ้วมือ (Related work of Fingerprint Verification)

ลายนิ้วมือของแต่ละคน ประกอบด้วยสันและร่อง ซึ่งลักษณะนี้มีคุณลักษณะที่สำคัญ 2 ประการ คือ ไม่มีการเปลี่ยนแปลงรูปแบบตามกาลเวลา และมีรูปแบบเฉพาะในแต่ละบุคคล จุดลักษณะสำคัญบนลายนิ้วมือหรือที่เรียกว่า “ไมนูเทีย” (Minutia) ดังแสดงในภาพที่ 3



ending bifurcation

ภาพที่ 3 ไมนูเทีย: จุดหยุด (Ending) และ จุดแตก Bifurcation) [2]

ไมนูเทียในลายพิมพ์นิ้วมือเป็นสิ่งที่สำคัญ ที่จะนำไปใช้ในการพิสูจน์ว่าเป็นลายพิมพ์นิ้วมือของบุคคลใด โดยที่ระบบการพิสูจน์ลายพิมพ์นิ้วมือประกอบด้วยส่วนที่สำคัญดังนี้ [2]

- Image Capture ในส่วนนี้จะเป็นส่วนของการรับลายพิมพ์นิ้วมือจากเครื่องสแกนลายนิ้วมือ
 - Image Enhancement ในส่วนนี้จะเป็นการปรับปรุงคุณภาพของลายพิมพ์นิ้วมือให้มีความชัดเจนมากขึ้น
 - Feature Extraction ในส่วนนี้จะเป็นการหาไมนูเทีย
 - Verification ในส่วนนี้เป็นส่วนของการพิสูจน์ว่าลายพิมพ์นิ้วมือนี้เป็นลายพิมพ์นิ้วมือเป็นลายพิมพ์เดียวกันกับลายพิมพ์นิ้วมือที่ต้องการพิสูจน์หรือไม่
- ระบบการพิสูจน์ลายพิมพ์นิ้วมือได้ถูกพัฒนาและวิจัยใน

ทุกส่วน เพื่อปรับปรุงการทำงานในทุกขั้นตอนข้างต้น ดังปรากฏในงานวิจัยที่เกี่ยวข้องกับการพิสูจน์ลายพิมพ์นิ้วมือ ที่ได้ทำการปรับปรุงคุณภาพของการพิสูจน์ลายพิมพ์นิ้วมือ โดยใช้เทคนิคของการประมวลผลภาพช่วยในการทำให้การพิสูจน์ลายพิมพ์นิ้วมือมีผลการพิสูจน์ที่ดีขึ้น [3] นอกจากนี้ยังมีการปรับปรุงคุณภาพของการพิสูจน์ลายพิมพ์นิ้วมือด้วยการจัดจำแนกประเภทของลายพิมพ์นิ้วมือก่อนที่จะทำการพิสูจน์โดยใช้ directional field [4] และการพิสูจน์ลายพิมพ์นิ้วมือนั้น จำเป็นต้องทำการหาจุดไม่เหมือน ซึ่งก่อนที่จะทำการหาจุดไม่เหมือน ต้องทำการหา singular point ซึ่งจะทำให้การพิสูจน์ลายพิมพ์นิ้วมือเป็นผลให้การพิสูจน์ได้ด้วยความแม่นยำ [5]

2.4 งานวิจัยที่เกี่ยวข้องกับการเข้าใช้ระบบ (Related work on System Access Control)

เทคโนโลยีไบโอเมตริกซ์ ได้ถูกนำไปประยุกต์ใช้ในงานหลายด้าน ไม่ว่าจะเป็นด้านธุรกิจ ด้านการปกครอง และด้านกฎหมาย [1] โดยที่การประยุกต์ใช้ในแต่ละด้านนั้น มีวัตถุประสงค์สำคัญคือ การรักษาความปลอดภัย ด้วยการควบคุมการเข้าใช้ระบบ หรือควบคุมการผ่านเข้า-ออก อาคารสถานที่ โดยกำหนดให้ มีการตรวจสอบบุคคลที่ต้องการเข้าไปใช้ระบบ ด้วยการตรวจสอบรูม่านตา (Iris) ซึ่งให้ความถูกต้องในการระบุตัวบุคคล และมีความปลอดภัยในการเข้าใช้งานระบบสูง แต่มีค่าใช้จ่ายที่สูงมาก [6] นอกจากนี้ได้มีการนำเอา Smart Card ที่บรรจุข้อมูลลายพิมพ์นิ้วมือ เข้ามาใช้สำหรับควบคุมการเข้าถึงระบบการจ่ายเงิน (Payment System) ทำให้เกิดความปลอดภัยของระบบในระดับที่สูง [7]

3. แบบจำลองการเข้าใช้งานระบบโดยใช้การพิสูจน์ลายพิมพ์นิ้วมือ (System Access Control Model by Fingerprint Verification)

แบบจำลองการเข้าใช้งานระบบ โดยใช้การพิสูจน์ลายพิมพ์นิ้วมือ มีการทำงานใน 2 ส่วนคือ การลงทะเบียนบุคคล และการยืนยันบุคคล (ภาพที่ 4)

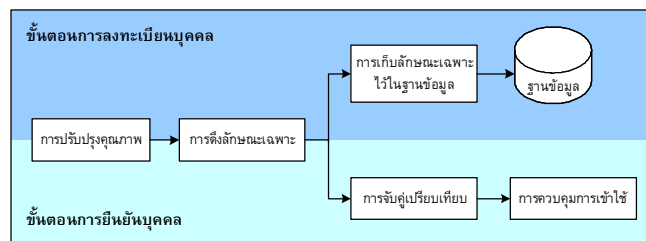
- การลงทะเบียนบุคคล (Enrollment Part)

เป็นส่วนที่รับข้อมูลของบุคคล และลายพิมพ์นิ้วมือ 3 นิ้ว เก็บไว้ในฐานข้อมูลของระบบเพื่อใช้ในการยืนยันบุคคลต่อไป

- การยืนยันบุคคล (Verification Part)

เป็นส่วนที่รับรหัสบุคคล หรือ ชื่อ-นามสกุลของบุคคลและ

รับลายพิมพ์นิ้วมือ เพื่อยืนยันบุคคล และตรวจสอบสิทธิ์การเข้าใช้ระบบ



ภาพที่ 4 แบบจำลองโดยรวมของระบบการเข้าใช้งานระบบโดยการพิสูจน์ลายพิมพ์นิ้วมือ

โดยที่การทำงานของทั้ง 2 ส่วน มีขั้นตอนการทำงานที่สำคัญ คือ

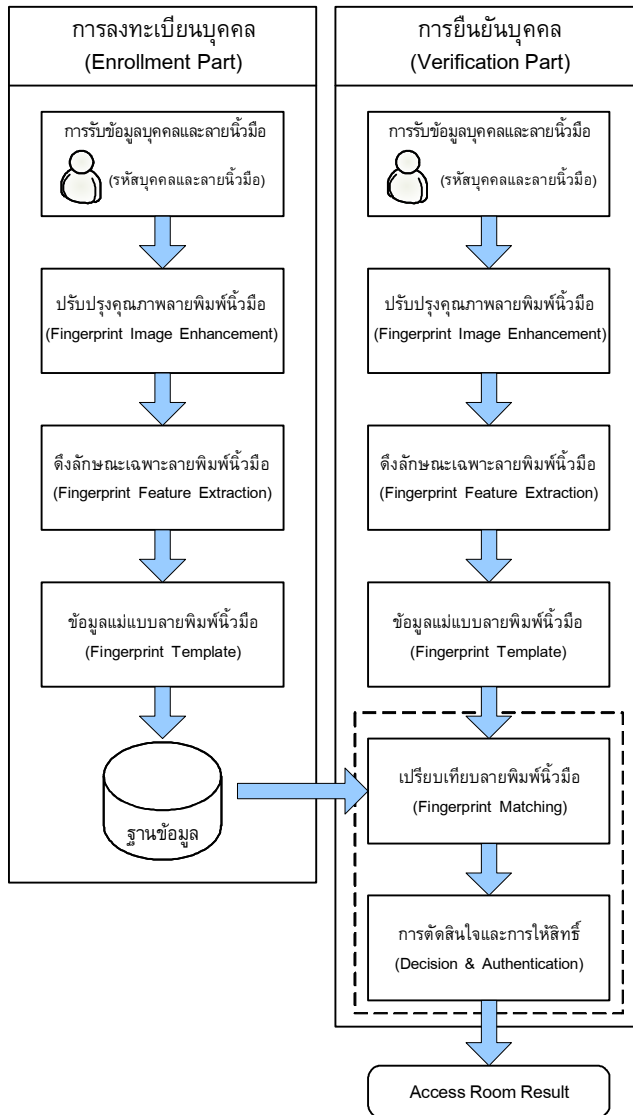
- การปรับปรุงคุณภาพลายพิมพ์นิ้วมือ (Fingerprint Image Enhancement) เพื่อให้ได้ภาพลายพิมพ์นิ้วมือที่มีคุณภาพอันเป็นผลให้ทำการประมวลผลได้ง่ายขึ้นและใกล้เคียงกับความเป็นจริงมากที่สุด

- การดึงลักษณะเฉพาะลายพิมพ์นิ้วมือ (Fingerprint Feature Extraction) เป็นการหาไม่เหมือนบนเส้นสัน จากภาพลายพิมพ์นิ้วมือที่ผ่านกระบวนการปรับปรุงภาพจากขั้นตอนก่อนหน้านี้

- การจับคู่เปรียบเทียบ (Fingerprint Matching) เป็นการจับคู่เปรียบเทียบลายพิมพ์นิ้วมือของบุคคลที่ต้องการเข้าใช้ระบบกับลายพิมพ์นิ้วมือของบุคคลนั้นที่เก็บไว้ในฐานข้อมูลว่าเป็นลายพิมพ์นิ้วมือเดียวกันหรือไม่

- การควบคุมการเข้าใช้ (Access Control) เป็นการตรวจสอบสถานะของบุคคล (สามารถเข้าใช้ระบบได้ ไม่สามารถเข้าใช้ระบบได้) และตรวจสอบสถานะของระบบ (สามารถเข้าใช้ได้ตามปกติ งดการเข้าใช้ชั่วคราว) เพื่อพิจารณาอนุญาตให้บุคคลเข้าใช้ระบบ ดังแสดงในตารางที่ 2 รายละเอียดในแต่ละส่วนสามารถแสดงได้ดังภาพที่ 5

แบบจำลองการเข้าใช้งานระบบ ได้ถูกออกแบบให้มีการทำงานแบบไคลเอนต์-เซิร์ฟเวอร์ (ภาพที่ 6) โดยคอมพิวเตอร์ที่ทำหน้าที่เซิร์ฟเวอร์ (server) จะเก็บข้อมูลทั้งหมดของระบบ ส่วนคอมพิวเตอร์ที่ทำหน้าที่ไคลเอนต์ (client) ทำหน้าที่รองรับข้อมูลบุคคลที่ต้องการตรวจสอบ และส่งไปให้เครื่องคอมพิวเตอร์ที่ทำหน้าที่เซิร์ฟเวอร์ต่อไป



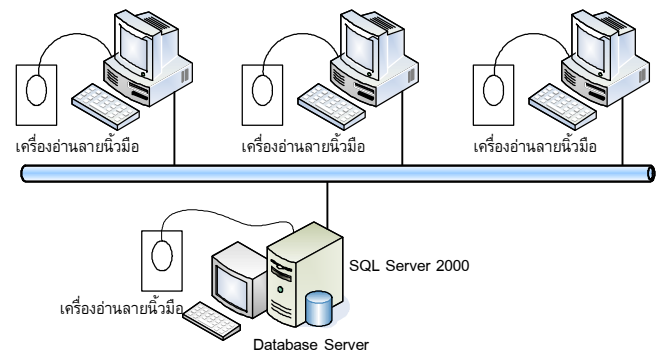
ภาพที่ 5 แสดงขั้นตอนของการทำงานในส่วนของการลงทะเบียนและยืนยันบุคคล

ตารางที่ 2 การอนุญาตในการเข้าใช้ระบบ

สถานะบุคคล สถานะระบบ	สามารถเข้าใช้ ระบบได้	ไม่สามารถเข้าใช้ ระบบได้
สามารถเข้าใช้ได้ ตามปกติ	อนุญาตให้เข้าใช้ ระบบได้	ไม่อนุญาตให้ เข้าใช้ระบบ
งดการเข้าใช้ ชั่วคราว	ไม่อนุญาตให้ เข้าใช้ระบบ	ไม่อนุญาตให้ เข้าใช้ระบบ

4. ผลการทดลอง (Experimental Results)

แบบจำลองการเข้าใช้งานระบบโดยใช้การพิสูจน์ลายพิมพ์นิ้วมือได้ถูกพัฒนาขึ้นจากโปรแกรม Microsoft Visual Basic.NET, MATLAB 6.5 และการทำงานของแบบจำลอง



ภาพที่ 6 สถาปัตยกรรมของแบบจำลองการเข้าใช้งานระบบโดยการพิสูจน์ลายพิมพ์นิ้วมือ

ทำงานติดต่อกับระบบฐานข้อมูล Microsoft Access โดยแบบจำลองนี้ทำงานภายใต้ระบบปฏิบัติการ Microsoft WindowsXP Professional โดยที่แบบจำลองที่พัฒนาขึ้นนี้มีความสามารถบรรลุตามวัตถุประสงค์แล้วยังมีความสามารถดังนี้ คือ

- แบบจำลองสามารถทำงานแบบไคลเอนต์-เซิร์ฟเวอร์ และในส่วนของเครื่องคอมพิวเตอร์ที่ทำหน้าที่เซิร์ฟเวอร์สามารถแสดงข้อมูลการทำงานของเครื่องคอมพิวเตอร์ที่ทำหน้าที่ไคลเอนต์ได้
- แบบจำลองสามารถยืนยันตัวตนบุคคลโดยใช้ลายพิมพ์นิ้วมือ โดยรับข้อมูลจากแป้นพิมพ์และเครื่องอ่านลายนิ้วมือนำไปประมวลผล แล้วนำไปเปรียบเทียบกับข้อมูลในฐานข้อมูล
- แบบจำลองสามารถจัดการตรวจสอบสิทธิ์การเข้าถึงระบบ

- แบบจำลองสามารถจัดการฐานข้อมูลของแต่ละพื้นที่ของระบบ โดยสามารถเก็บ เพิ่ม ลบ และเปลี่ยนแปลงแก้ไขข้อมูลแต่ละพื้นที่ได้

สำหรับผลการทดลองแบบจำลองการเข้าใช้งานระบบโดยใช้การพิสูจน์ลายพิมพ์นิ้วมือได้ทำการทดลอง 2 ส่วน ดังนี้ ส่วนที่ 1 การตรวจสอบการอนุญาตในการใช้งานแบบจำลองการเข้าใช้งาน โดยทดสอบการลงชื่อเข้าใช้ระบบ 160 ครั้ง แบ่งเป็นกรณีที่ยอมรับ 20 ครั้ง กรณีปฏิเสธอีก 140 ครั้ง ดังนั้นแบบจำลองที่นำเสนอสามารถตรวจสอบการเข้าใช้งานระบบด้วยความถูกต้อง 98.12 % และมีความผิดพลาด 1.88 %

ส่วนที่ 2 การตรวจสอบการยืนยันตัวตนบุคคลด้วยลายพิมพ์นิ้วมือ ทดสอบกับลายนิ้วมือ 26 นิ้ว เป็นนิ้วที่ลงทะเบียนแล้ว 11 นิ้ว และนิ้วที่ไม่ได้ลงทะเบียน 15 นิ้ว ซึ่งสามารถเกิดผลได้

4 ลักษณะ คือ

1. ยอมรับ เมื่อลายนิ้วมือที่เปรียบเทียบเป็นของบุคคลเดียวกัน (Positive Accept)
 2. ปฏิเสธ แม้ลายนิ้วมือที่เปรียบเทียบของบุคคลเดียวกัน (Negative Accept)
 3. ปฏิเสธ เมื่อลายนิ้วมือที่เปรียบเทียบไม่ใช่ของบุคคลเดียวกัน (Positive Reject)
 4. ยอมรับ แม้ลายนิ้วมือที่เปรียบเทียบไม่ใช่ของบุคคลเดียวกัน (Positive Reject)
- โดยที่ผลลัพธ์ของการทดลองแสดงในตารางที่ 3

ตารางที่ 3 แสดงผลลัพธ์การยืนยันตัวบุคคลด้วยลายพิมพ์นิ้วมือ

การทดลอง	ผลทดลอง	เปอร์เซ็นต์
(Accept +) and (Reject +)	21	80.77
(Accept -) and (Reject -)	5	19.23

5. บทสรุป (Conclusion)

ในงานวิจัยนี้นำเสนอแนวคิด การนำเอาเทคโนโลยีการรู้จำไบโอเมตริกซ์ (Biometric Recognition) นำมาประยุกต์ใช้ ด้านการรักษาความปลอดภัยซึ่งทำให้เกิดการออกแบบ และการพัฒนาแบบจำลองการควบคุมการใช้งานระบบ (System Access Control Model) สำหรับงานวิจัยนี้ได้ใช้การรู้จำลายพิมพ์นิ้วมือ ซึ่งจากแบบจำลองที่พัฒนาและออกแบบ สามารถนำไปประยุกต์ใช้งานกับไบโอเมตริกซ์ชนิดอื่นได้ไม่ว่าจะเป็นเสียง ลายเซ็นต์ หรือไบโอเมตริกซ์ชนิดอื่นๆ

เอกสารอ้างอิง

[1] Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition," IEEE trans

on Circuits and System for Video Technology., vol. 14, no. 1, pp. 4-20, 2004.

[2] Lawrence O' Gorman, "An Overview of Fingerprint Verification Technologies," Information Security Technical Report, vol. 3, no. 1, pp. 21-32, 1998.

[3] M. Poulos, A. Evangelov, E. Magkos and S. Papavlasopoulos, "Fingerprint Verification based on Image Processing Using An Onion Algorithm of Computational Geometry," International Conference on Mathematics Methods in Scattering Theory and Biomedical Technology (BIOTECH'6), 2003.

[4] Sen Wang, Wei Wei Zhang, and Yang Sheng Wang, "Fingerprint Classification by Directional Fields," IEEE, Proceeding, Multimodal Interfaces (ICMI'02), 2002.

[5] Nannan Wu, and Jie Zhou, "Model Based Algorithm For Singular Point Detection From Fingerprint Images," International Conference on Image Processing (ICIP), 2004.

[6] Raul Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, "Improving Access Control Security Using Iris Identification," IEEE Proceeding, 34th Annual 2000 International Carnahan Conference on Security Tehchnology, pp. 23-25, 2000.

[7] Sanchez-Reillo, R., and Sanchez-Avila, C., "Fingerprint Verification Using Smart Cards for Access Control Systems," IEEE Aerospace and Electronic Systems, vol. 17, no. 9, pp. 12-15, 2002.