

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

ในปัจจุบันระบบตรวจสอบลายนิ้วมือได้ถูกนำมาใช้งานกันอย่างแพร่หลาย การนำระบบ
 ตรวจสอบลายนิ้วมือไปประยุกต์ใช้งานร่วมกับสมาร์ทการ์ด โดยออกแบบให้สมาร์ทการ์ดทำการ
 ประมวลผลขั้นตอนการเปรียบเทียบลายนิ้วมือเอง จะทำให้ระบบโดยรวมมีความปลอดภัยสูง
 เนื่องจากในการตรวจสอบลายนิ้วมือ จะทำโดยส่งข้อมูลลายนิ้วมือที่ต้องการตรวจสอบไป
 ตรวจสอบภายในสมาร์ทการ์ด ทำให้ไม่มีการจัดส่งแม่แบบลายนิ้วมือที่เก็บไว้ในหน่วยความจำ
 ของสมาร์ทการ์ดออกมาภายนอก จึงทำให้ปลอดภัยต่อการถูกดักจับหรือการปลอมแปลงได้

วิทยานิพนธ์นี้นำเสนอการพัฒนาขั้นตอนการเปรียบเทียบลายนิ้วมือ (Fingerprint
 Matching) เพื่อให้สามารถประมวลผลบนสมาร์ทการ์ดแบบ 8 บิต ที่มีขนาดหน่วยความจำ
 ชั่วคราวเล็กกว่าข้อมูลลายนิ้วมือทั้งหมดได้ และลดเวลาที่ใช้ในการประมวลผลลง โดยเมื่อ
 ข้อมูลภาพลายนิ้วมือที่ต้องการตรวจสอบได้ผ่านขั้นตอนการทำ Feature Extraction แล้ว จะถูก
 แบ่งออกเป็น 3 ส่วนเท่าๆ กัน เพื่อส่งไปเปรียบเทียบกับแม่แบบลายนิ้วมือที่เก็บไว้ในสมาร์ท-
 การ์ด โดยจะเริ่มต้นเปรียบเทียบจากส่วนที่มีจำนวนจุดสำคัญบนเส้นลายนิ้วมือ (Minutiae) มาก
 ที่สุด ไปยังน้อยที่สุด และได้ออกแบบให้มีค่าขีดแบ่ง (Threshold) ย่อยๆ ตามแต่ละขั้นตอนการ
 ทำงาน โดยในขั้นตอนแรก และขั้นตอนที่สอง จะมีการใช้ค่าขีดแบ่งระดับบน (Upper Threshold)
 และค่าขีดแบ่งระดับล่าง (Lower Threshold) เพื่อพิจารณาว่าลายนิ้วมือว่าเป็นของบุคคลเดียวกัน
 หรือต่างบุคคล หรือควรจะนำข้อมูลภาพลายนิ้วมือส่วนอื่นมาประมวลผลเพิ่มเติมต่อไป โดยที่ค่า
 ขีดแบ่งระดับบน จะช่วยลดเวลาในบางกรณีของภาพลายนิ้วมือที่รับเข้ามาเป็นบุคคลเดียวกัน
 และค่าขีดแบ่งระดับล่าง จะช่วยลดเวลาในกรณีของภาพลายนิ้วมือที่รับเข้ามาต่างบุคคลกันมี
 ตำแหน่ง และชนิดของจุดสำคัญบนเส้นลายนิ้วมือ ที่แตกต่างกันระหว่างภาพที่รับเข้ามา กับ
 แม่แบบลายนิ้วมือ

4570282721 : MAJOR Computer Engineering

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

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

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

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