กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA

White Paper

การพิสูจน์ และยืนยันตัวตนด้วยระบบไบโอเมตริก

PERSONAL VERIFICATION USING BIOMETRIC SYSTEMS

โดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สารบัญ	

หน้า

บทสรุปผู้บริหาร

เทคโนโลยีไบโอเมตริก (Biometrics) ถือเป็นสิ่งที่ใช้เพื่อการพิสูจน์และยืนยันตัวบุคคลรูปแบบหนึ่งที่ถือเป็นลักษณะเฉพาะทางสรีรวิทยา หรือ Physiological Characteristics และลักษณะเฉพาะทางพฤติกรรม หรือ Behavioral Characteristics ที่เน้นการใช้งานเพื่อบริการประชาชน ซึ่งในรายงานฉบับนี้ได้มีการรวบรวมและนำเสนอเทคโนโลยีไบโอเมตริก โดยแบ่งออกเป็น 6 ลักษณะเฉพาะที่เป็นที่นิยมในปัจจุบัน คือ ใบหน้า ลายนิ้วมือ ลายม่านตา ลายเส้นเลือด ลายเซ็น และเสียงพูด ซึ่งแต่ละแบบจะมีข้อดีและข้อด้อยที่แตกต่างกันไป ซึ่งคุณลักษณะที่สำคัญ เช่น ความเป็นเอกลักษณ์เฉพาะ ความคงทนถาวรในการใช้งาน การมีในมนุษย์ทุกคน การตรวจวัดได้ ประสิทธิภาพในการใช้งาน การยอมรับของผู้ใช้งาน และความยากในการปลอมแปลง

โดยในรายงานฉบับนี้ จะแบ่งออกเป็น 5 บท เริ่มตั้งแต่บทที่ 1 ที่จะนำเสนอการศึกษาและวิเคราะห์ลักษณะเฉพาะของไบโอเมตริกในแต่ละแบบ ที่จะช่วยตอบข้อสงสัยของหลายคนเกี่ยวกับหลักการทำงานเพื่อการรู้จำและแยกแยะลักษณะของบุคคลในแต่ละแบบ จะช่วยเพิ่มความเข้าใจลักษณะในแต่ละแบบได้อย่างเด่นชัดมากขึ้น โดยมีอัลกอริทึมที่ได้รับความนิยมในลักษณะเฉพาะแต่ละแบบ เช่น การรู้จำใบหน้า จะเป็นอัลกอริทึมการเรียนรู้เชิงลึก (Deep Learning) ที่ทำให้คอมพิวเตอร์มีความสามารถในการพัฒนาตนเองได้ โดยการเรียนรู้ข้อผิดพลาดที่สอนโดยข้อมูลที่มนุษย์กำหนดให้ ซึ่งจะเห็นได้ว่าในปัจจุบันมีหลายองค์กรที่นำเทคโนโลยีนี้ไปใช้ เนื่องจากมีความแม่นยำ ราคาไม่แพง ผู้ใช้ยอมรับ และปลอดภัย เพราะมีระยะห่างระหว่างบุคคล และอุปกรณ์ เป็นต้น

ในบทที่ 2 จะมีการยกตัวอย่างหรือ Used Cases เพื่อให้เห็นการนำเอาไบโอเมตริกไปใช้งานในรูปแบบการให้บริการประชาชนอย่างเป็นรูปธรรมในโครงการต่าง ๆ ที่โครงการส่วนใหญ่เกิดขึ้นเพื่อช่วยแก้ปัญหาของประเทศในมิติต่าง ๆ และความสำเร็จส่วนหนึ่งมาจากความร่วมมือกันระหว่างหน่วยงานสำคัญที่เกี่ยวข้อง เช่น โครงการ Aadhaar ในประเทศอินเดีย ที่ถือเป็นโครงการที่รวบรวมข้อมูลไบโอเมตริกของประชาชนที่มีขนาดใหญ่ที่สุดของโลก โดยโครงการนี้ใช้การตรวจสอบด้วยการระบุตัวตนทั้งลายนิ้วมือ 10 นิ้ว และลายม่านตาสองข้าง เพื่อป้องกันการลงทะเบียนที่ซ้ำซ้อน ในขณะที่โครงการ National ID ในประเทศออสเตรเลีย ได้ใช้แอปพลิเคชัน myGov ID ที่ประสานความร่วมมือกับ Australian Post Digital ID โดยกำหนดว่าผู้ใช้บริการต้องมีอายุ 15 ปีขึ้นไป และ โครงการ Schengen ในกลุ่มประเทศสหภาพยุโรป หรือ EU ที่มีการใช้ Schengen Information System หรือ SIS ซึ่งเป็นระบบข้อมูลที่ใช้อย่างแพร่หลายและใหญ่ที่สุดในกลุ่มประเทศ EU ที่ใช้การแบ่งปันข้อมูลแบบ Real Time ให้แก่หน่วยงานด้านความปลอดภัยระดับชาติที่มีอำนาจควบคุม โดยมีการกำหนดช่วงเวลาในการจัดเก็บข้อมูลไว้อย่างชัดเจน (ระยะเวลา 5 ปี) หรือขึ้นอยู่กับประเทศสมาชิกที่มีสิทธิ์ทบทวนถึงความจำเป็นในการจัดเก็บมากกว่าที่กำหนดได้ โดยมีการกำหนดโครงสร้างของฐานข้อมูลในการจัดเก็บที่ชัดเจน เช่น ภาพใบหน้า ทั้งหน้าตรง ใบหน้าอื่น ๆ ผลกระทบจากกลุ่มอายุ เพื่อเพิ่มความแม่นยำ และการคำนึงถึงปัญหาด้านความปลอดภัยด้านการโจมตีระบบในแบบต่าง ๆ เป็นต้น

สำหรับในบทที่ 3 จะเน้นประเด็นที่เกี่ยวข้องกับการใช้งานไบโอเมตริกกับข้อมูลส่วนบุคคล ซึ่งได้มีการอ้างอิงถึงกฎหมายในประเทศไทย 2 ฉบับ คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 รวมถึงประเด็นเทคโนโลยีไบโอเมตริกที่เกี่ยวข้องกับสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลในต่างประเทศ เช่น ประเด็นการถูกฟ้องจากการละเมิดข้อมูลส่วนบุคคลของ Facebook และ Google เป็นต้น ที่จะรวมไปถึงประเด็นการใช้งานในกลุ่มผู้สูงอายุ และเด็ก พร้อมทั้งประเด็นทางด้านจริยธรรม ซึ่งในบทนี้จะทำให้เห็นว่าประเทศไทยมีกฎหมายรองรับการคุ้มครองสิทธิส่วนบุคคลที่เป็นแนวทางเดียวกับสากล แต่ยังไม่มีในมุมของการคุ้มครองสิทธิข้อมูลไบโอเมตริก

ลำดับต่อไปในบทที่ 4 จะกล่าวถึง ภูมิทัศน์ของมาตรฐานไบโอเมตริกโดยรวม ซึ่งจะอธิบายถึงมาตรฐานสากล ISO/IEC JTC 1/SC37 ซึ่งเป็นมาตรฐานหลักที่เกี่ยวข้องกับไบโอเมตริกที่ใช้ในการบริการประชาชน และมาตรฐาน ANSI/NIST ITL ซึ่งเป็นมาตรฐานไบโอเมตริกที่ใช้กับงานทางด้านนิติวิทยาศาสตร์ ที่จะทำให้ผู้สนใจเข้าใจถึงวัตถุประสงค์และเป้าหมายของแต่ละมาตรฐานได้อย่างชัดเจนมากขึ้น

และในบทสุดท้าย บทที่ 5 จะเป็นการนำเสนอแนวทางการวัดสมรรถนะของระบบไบโอเมตริกเพื่อเปรียบเทียบประสิทธิภาพของระบบในการนำไปใช้งาน ซึ่งแบ่งเป็นการวัดประสิทธิภาพระบบยืนยันตัวบุคคล การวัดประสิทธิภาพระบบค้นหาตัวบุคคล การวัดประสิทธิภาพการนำเข้าข้อมูล รวมถึงหน่วยงานอิสระต่าง ๆ ที่เปรียบเทียบประสิทธิภาพของระบบไบโอเมตริกในปัจจุบัน พร้อมการแสดงให้เห็นถึงความแตกต่างของการประเมินสมรรถนะของระบบไบโอเมตริกในแต่ละระดับ ทั้งการประเมินในระดับเทคโนโลยี ระดับการจำลองประยุกต์ใช้งาน และระดับปฏิบัติการ

บทที่ 1

การศึกษาและวิเคราะห์ลักษณะเฉพาะของไบโอเมตริก

บทที่ 1. การศึกษาและวิเคราะห์ลักษณะเฉพาะของไบโอเมตริก

ไบโอเมตริก (Biometric) คือ การวัดลักษณะเฉพาะที่มีความแตกต่างกันระหว่างบุคคล หรือการวัดอัตลักษณ์ของบุคคล โดยอัตลักษณ์นี้ มาจากคำว่า อัตตา ที่แปลว่าตัวตน กับ ลักษณ์ ที่แปลว่ารูปร่างลักษณะ เมื่อคำว่า ไบโอเมตริก ถูกแปลเป็นไทย ได้ถูกเรียกในชื่ออื่น ๆ อาทิเช่น ข้อมูลชีวภาพ ชีวมิติ หรือ ชีวมาตร แต่สำหรับรายงานฉบับนี้ จะใช้ทับศัพท์โดยใช้คำว่า “ไบโอเมตริก” ในรายงานฉบับนี้ทั้งเล่ม เพื่อจะได้สื่อความหมายได้ชัดเจนและสากลต่อไป

ลักษณะเฉพาะไบโอเมตริก (Biometric Characteristics)

ลักษณะเฉพาะไบโอเมตริก (Biometric Characteristics) สามารถแบ่งออกเป็นสองรูปแบบ คือ ลักษณะเฉพาะทางสรีรวิทยา (Physiological Characteristics) และ ลักษณะเฉพาะทางพฤติกรรม (Behavioral Characteristics) ดังแสดงในภาพที่ 1 ซึ่งมีรายละเอียด ดังต่อไปนี้

1) **ลักษณะเฉพาะทางสรีรวิทยา (Physiological Characteristics)**

   ลักษณะเฉพาะทางสรีรวิทยา เป็นสิ่งที่สามารถวัดได้โดยตรงจากส่วนต่าง ๆ ทั้งภายในและภายนอกของร่างกายของมนุษย์ อาทิ ใบหน้า ม่านตา ลายนิ้วมือ ลักษณะฝ่ามือ เส้นเลือดในนิ้วหรือในมือ เรตินาหรือลักษณะเส้นเลือดในลูกตา ใบหู ลักษณะรูปแบบอุณหภูมิของใบหน้า ฟัน และ ดีเอ็นเอ (DNA)

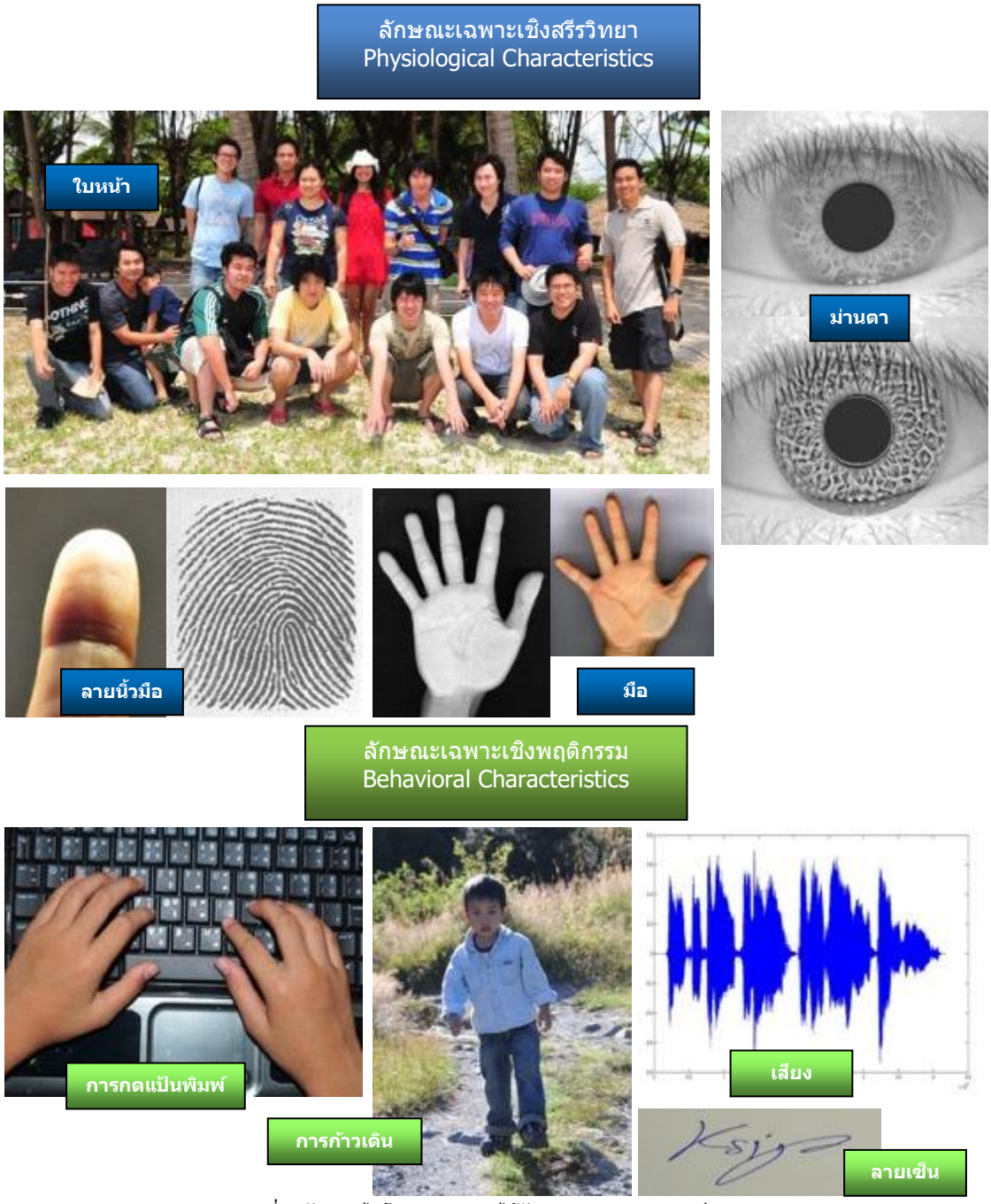
2) **ลักษณะเฉพาะทางพฤติกรรม (Behavioral Characteristics)**

   ลักษณะเฉพาะทางพฤติกรรม เป็นสิ่งที่สามารถวัดได้จากลักษณะทางพฤติกรรมหรือการกระทำของแต่ละบุคคล อาทิ เสียงพูด ลายเซ็น รูปแบบการกดแป้นพิมพ์ หรือ ลักษณะการเดิน เป็นต้น

คุณสมบัติของลักษณะเฉพาะไบโอเมตริก (Properties of Biometric Characteristics)

คุณสมบัติของลักษณะเฉพาะไบโอเมตริก ควรต้องมีคุณสมบัติ 7 ประการดังต่อไปนี้ [Jain2007]

1) **ความเป็นเอกลักษณ์ (Uniqueness)** ซึ่งทุกคนต้องมีลักษณะเฉพาะที่ไม่มีใครเหมือนและไม่เหมือนใคร คุณสมบัตินี้จะต้องแตกต่างกันในแต่ละบุคคลที่จะทำให้สามารถแยกแยะแต่ละบุคคลออกจากกันได้
2) **ความคงทนถาวร (Permanence)** ลักษณะเฉพาะไบโอเมตริกนี้ จะต้องมีความคงทนไม่เปลี่ยนแปลงไปในระยะเวลายาวนาน หรือในเวลาที่จำกัด หรือในระหว่างการใช้งาน
3) **ความเป็นลักษณะเฉพาะทั่วไปของมนุษย์ (Universality)** ลักษณะเฉพาะไบโอเมตริกนี้ จะต้องมีในมนุษย์ทุกคนโดยทั่วไปที่มีลักษณะภายนอกเป็นปกติของมนุษย์ หรือที่เรียกว่ามีอวัยวะครบสามสิบสอง
4) **ความสามารถในการตรวจวัดได้ (Collectability)** ลักษณะเฉพาะไบโอเมตริกนี้ จะสามารถเก็บข้อมูลได้ในรูปแบบดิจิทัลโดยใช้อุปกรณ์เฉพาะได้โดยไม่สร้างความลำบากให้แก่ผู้ใช้ นอกจากนี้ข้อมูลที่ได้ต้องเพียงพอที่จะนำไปใช้วัดความแตกต่างระหว่างบุคคลได้
5) **สมรรถนะ (Performance)** เทคโนโลยีไบโอเมตริกที่นำมาใช้กับลักษณะเฉพาะไบโอเมตริกนี้ต้องมีประสิทธิภาพ ความเร็วในการทำงาน ความแม่นยำที่ต้องการ และราคาที่เหมาะสม เหมาะกับความต้องการของงานที่นำไปประยุกต์ใช้
6) **ความเป็นที่ยอมรับของผู้ใช้ (Acceptability)** ลักษณะเฉพาะไบโอเมตริกนี้ต้องเป็นที่ยอมรับโดยให้ความร่วมมือยินดี หรือได้ประโยชน์จากการใช้งานของผู้ใช้ โดยไม่ควรเป็นแหล่งแพร่เชื้อโรค หรือทำให้ติดต่อ โดยเฉพาะการสัมผัสกับอวัยวะต่าง ๆ ของมนุษย์ที่สามารถส่งผ่านเชื้อโรคได้
7) **การปลอมแปลงได้ยาก (Circumvention)** ลักษณะเฉพาะไบโอเมตริกนี้ ควรปลอมแปลงได้ยาก และทำลายหรือเปลี่ยนแปลงได้ยาก



ภาพที่ 1 ตัวอย่างไบโอเมตริก (ภาพได้รับอนุญาตจาก [วุฒิพงศ์2557])

ตัวอย่างลักษณะเฉพาะไบโอเมตริกแบบต่าง ๆ ดังแสดงในภาพที่ 1 รายงานฉบับนี้จะครอบคลุมลักษณะเฉพาะไบโอเมตริกที่นิยมใช้ในการยืนยันตัวบุคคลที่สำคัญ 6 รูปแบบ คือ การรู้จำใบหน้า การรู้จำลายนิ้วมือ การรู้จำลายม่านตา การรู้จำลายเส้นเลือด การรู้จำลายเซ็น และการรู้จำเสียงพูด ซึ่งจะเรียบเรียงรายละเอียดตามบทย่อยดังต่อไปนี้

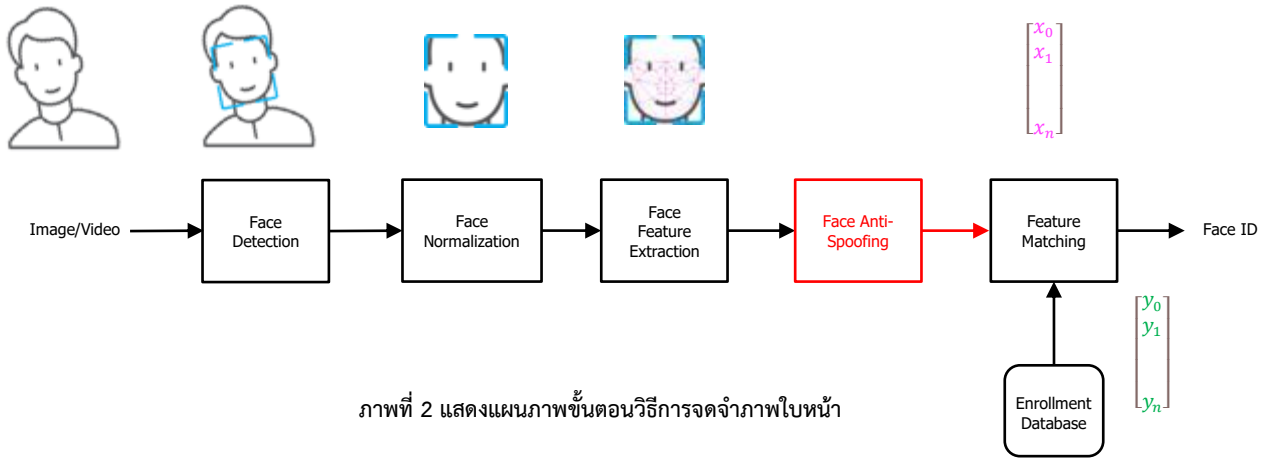
1.1. การรู้จำใบหน้า (Face Recognition)

ความแตกต่างของมนุษย์เราโดยทั่วไปสามารถจำแนกได้หลายลักษณะทั้งทางกายภาพและพฤติกรรม ในที่นี้จะเป็นการกล่าวถึงการจำแนกทางกายภาพ คือ ใบหน้าก่อนเป็นอย่างแรก ซึ่งถือเป็นลักษณะทางกายภาพที่แสดงความเป็นเอกลักษณ์เฉพาะแต่ละคนรูปแบบหนึ่ง โดยในปัจจุบันได้มีการพัฒนาให้เทคโนโลยีสามารถจำแนกลักษณะของคนได้ ซึ่งนำไปสู่การประยุกต์ใช้กับงานในแบบต่าง ๆ ได้อย่างกว้างขวางเพื่อใช้ในการยืนยันตัวบุคคล เช่น การให้เทคโนโลยีทางคอมพิวเตอร์มีการจดจำใบหน้าของคน โดยการวิเคราะห์จากโครงสร้างบนใบหน้า ทั้งจากลักษณะของดวงตา คิ้ว จมูก ปาก ริมฝีปาก คาง ขากรรไกร โหนกแก้ม หน้าผาก และตำแหน่งที่มีความสัมพันธ์กันของอวัยวะต่าง ๆ เป็นต้น สิ่งนี้เรียกว่า “การรู้จำใบหน้า” หรือ Face Recognition

1.1.1. หลักการทำงานของการรู้จำใบหน้า

การทำงานของระบบรู้จำใบหน้า (Face Recognition System) จะประกอบไปด้วย 5 ขั้นตอน ซึ่งแสดงได้ตามแผนภาพที่ 2 โดยมีรายละเอียด ดังต่อไปนี้

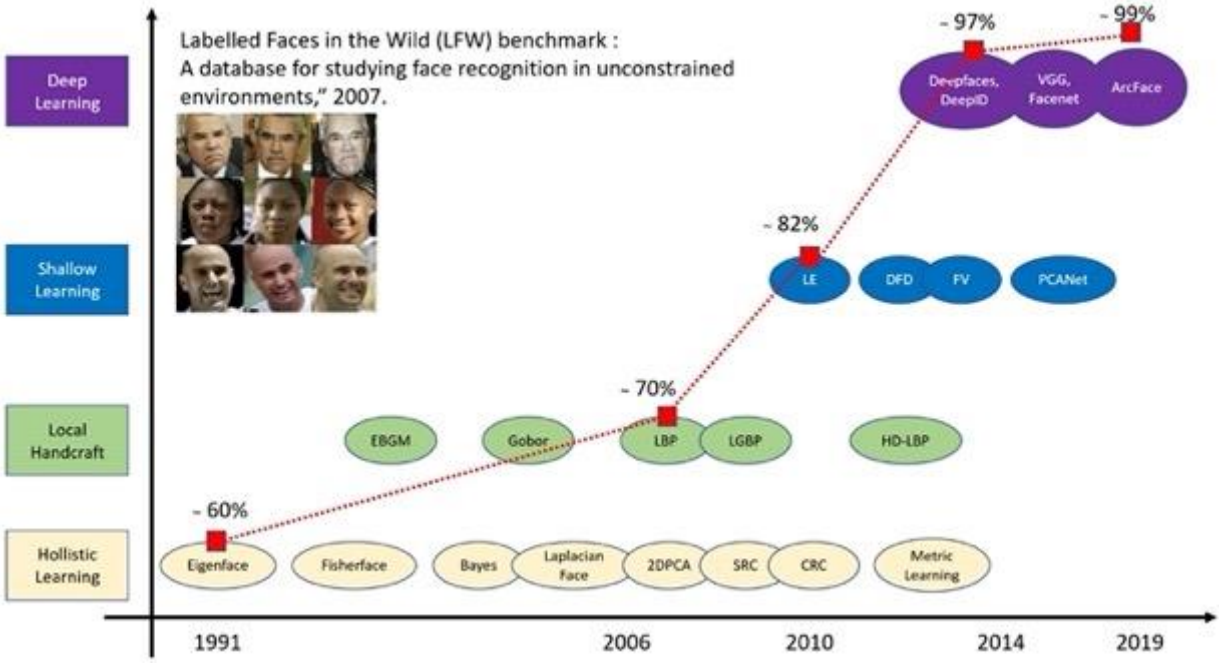
1) **การตรวจจับใบหน้า (Face Detection)** โดยจะทำการตัดเฉพาะส่วนที่เป็นใบหน้าจากภาพหรือวีดิทัศน์ เพื่อแยกภาพออกจากพื้นหลัง และหาจุดสำคัญต่าง ๆ บนใบหน้าเพื่อใช้เป็นจุดอ้างอิง (Face Landmark)
2) **การทำให้เป็นบรรทัดฐาน (Normalization)** เป็นการปรับความเอียง แสงเงา ให้ภาพใบหน้ากลับมาเป็นรูปแบบบรรทัดฐาน
3) **การสกัดลักษณะเด่น (Feature Extraction)** ดำเนินการสกัดลักษณะเด่นและลักษณะเฉพาะที่สำคัญของแต่ละใบหน้าที่สามารถใช้ในการพิสูจน์ตัวตนได้
4) **การป้องกันปลอมแปลง (Anti-spoofing)** ขั้นตอนนี้จะเป็นขั้นตอนเสริมในการป้องกันการปลอมแปลง เช่น ตรวจสอบลักษณะเด่นที่ได้ว่ามีการปลอมแปลงภาพนำเข้าหรือไม่ เป็นต้น
5) **การจับคู่ลักษณะเด่น (Feature Matching)** เป็นขั้นตอนของการเปรียบเทียบลักษณะเด่นของภาพใบหน้าที่นำเข้าผ่านระบบหรือที่ตรวจจับได้ กับข้อมูลลักษณะเด่นจากภาพใบหน้าที่มีอยู่ในฐานข้อมูลที่ลงทะเบียนไว้ก่อนหน้าแล้ว



ภาพที่ 2 แสดงแผนภาพขั้นตอนวิธีการจดจำภาพใบหน้า

1.1.2. อัลกอริทึมการรู้จำใบหน้า

การพัฒนาอัลกอริทึมการรู้จำของ Face Recognition หรือกระบวนการรู้จำใบหน้า สามารถแบ่งออกเป็น 4 กลุ่ม ประกอบด้วยวิธีการเรียนรู้แบบองค์รวม วิธีการกำหนดลักษณะเฉพาะที่ด้วยมนุษย์ วิธีการเรียนรู้เชิงตื้น และวิธีการเรียนรู้เชิงลึก (แสดงตามแผนภาพที่ 3) โดยวิวัฒนาการของอัลกอริทึมการรู้จำใบหน้าในแต่ละวิธี จะมีแนวทางในรายละเอียด ดังนี้



ภาพที่ 3 แผนภาพแสดงวิวัฒนาการการรู้จำใบหน้าด้วยเทคนิคทั้ง 4 กลุ่ม (ภาพดัดแปลงจาก [Galbally2019])

1) **วิธีการเรียนรู้แบบองค์รวม (Holistic Learning Methods)** เป็นงานวิจัยในช่วงแรกเริ่ม ซึ่งใช้วิธีการสกัดลักษณะเฉพาะของภาพใบหน้าทั้งภาพด้วยสมการทางคณิตศาสตร์เพื่อดึงลักษณะเด่นและลดขนาดข้อมูลที่ใช้ในการอ้างอิงภาพใบหน้า อัลกอริทึมที่เป็นวิธีการในกลุ่มนี้มีในรูปแบบต่าง ๆ ได้แก่ Eigenfaces [Turk1991], Fisherface [Belhumeur1997], Bayes [Moghaddam2000], Laplacianface [He2005], 2-dimensional Principal Component Analysis (2DPCA) [Xu2006], Sparse Representation-Based Classifier (SRC) [Deng2012], Collaborative Representation-Based Classifier (CRC) [Deng2018], metric learning [Guillaumin2009] แต่เนื่องจากสมการคณิตศาสตร์ที่ใช้เพื่อสกัดลักษณะเฉพาะจะได้มาจากการคำนวณทางคณิตศาสตร์ ที่ต้องพึ่งชุดข้อมูลที่นำไปทำการสอน (Training set) ซึ่งมีอยู่อย่างจำกัด ทำให้วิธีนี้มีข้อจำกัดหลายเรื่อง เช่น การรองรับความหลากหลายต่าง ๆ ที่ไม่ได้มีการควบคุม เช่น การเปลี่ยนแปลงสภาพแสงหรือการทนต่อรูปแบบใบหน้าที่มีความเอียง อีกทั้ง เทคนิคนี้ไม่สามารถนำไปใช้แยกแยะบุคคลในฐานข้อมูลที่มีปริมาณมากได้
2) **วิธีการกำหนดลักษณะเฉพาะที่ด้วยมนุษย์ (Local Handcraft Methods)** เป็นวิธีที่แบ่งภาพใบหน้าตามองค์ประกอบหลักของใบหน้า (Face landmark) เช่น ดวงตา จมูก ปาก เพื่อสกัดลักษณะเฉพาะชั้นแรก (1-Layer feature) ขององค์ประกอบนั้น ๆ เช่น ขนาด รูปทรง ลักษณะผิว และลักษณะเฉพาะชั้นสอง (2-Layer feature) โดยใช้ความสัมพันธ์ระหว่างกันและกันของแต่ละองค์ประกอบ เช่น ระยะห่างและองศาระหว่างตาซ้ายและจมูก ตาขวาและปาก เป็นต้น อัลกอริทึมที่เป็นวิธีการในกลุ่มนี้มีในรูปแบบต่าง ๆ ได้แก่ Elastic Bunch Graph Matching (EBGM) [Wiskott1997], Local Binary Pattern (LBP) [Ahonen2006], Local Gabor Binary Pattern Histogram Sequence (LGBPHS) [Zhang2005], และ High-Dimensional Local Binary Pattern (HD-LBP) [Chen2013] ดังนั้น อัลกอริทึมในกลุ่มนี้จะมีประสิทธิภาพที่ดีกว่าวิธีแรก (วิธีแรก คือ วิธีการเรียนรู้แบบองค์รวม) โดยจะสามารถรองรับปัญหาได้ดีขึ้น เนื่องจากใช้การวิเคราะห์องค์ประกอบใบหน้าหลายส่วนเข้าผนวกกัน แต่ก็มีข้อเสียของอัลกอริทึมในกลุ่มนี้ คือ ข้อมูลลักษณะเฉพาะที่ได้จะมีขนาดใหญ่ และยังไม่สามารถจำแนกบุคคลได้ดีเท่าที่ควร
3) **วิธีการเรียนรู้เชิงตื้น (Shallow Learning Method)** เป็นวิธีที่พัฒนาการสกัดลักษณะเฉพาะของใบหน้าโดยการเรียนรู้ที่ใช้ตัวกรองเฉพาะที่ เพื่อที่จะแยกความแตกต่างได้ดีขึ้นกว่าแบบเดิม สามารถเข้ารหัสข้อมูลใบหน้าได้ดีกว่า เมื่อเทียบกับ 2 วิธีก่อนหน้านี้ (วิธีการเรียนรู้แบบองค์รวม และวิธีการกำหนดลักษณะเฉพาะที่ด้วยมนุษย์) อัลกอริทึมที่เป็นวิธีการในกลุ่มนี้มีในรูปแบบต่าง ๆ ได้แก่ Learning-Based descriptors (LE) [Cao2010],

Discriminant Face Descriptor (DFD) [Lei2014], Fischer Vector (FV) [Simonyan2013], และ PCAnet [Chen2015] แต่อัลกอริทึมในกลุ่มนี้ก็ยังมีปัญหาในด้านความหลากหลายของภาพใบหน้าอยู่

4) **วิธีการเรียนรู้เชิงลึก (Deep Learning Method)** จากอัลกอริทึมรู้จำใบหน้าในวิธีต่าง ๆ ที่กล่าวมาแล้ว จะใช้แนวทางการแก้ปัญหาในการแยกองค์ประกอบของลักษณะเฉพาะเป็นสองส่วน คือ ลักษณะเฉพาะชั้นแรก (1-Layer feature) และลักษณะเฉพาะชั้นสอง (2-Layer feature) แต่การจำแนกภาพใบหน้าถือเป็นเรื่องที่มีความซับซ้อนมาก และเป็นเรื่องยากที่จะแก้ปัญหาด้วยรูปแบบเรขาคณิตเท่านั้น เช่น ความแตกต่างระหว่างภาพบุคคลคนเดียวกัน แต่ถ่ายในสภาพแสงหรือท่าทางที่แตกต่าง รวมถึงความคล้ายคลึงของภาพบุคคลสองคนที่ถ่ายในท่าทางและสิ่งแวดล้อมที่คล้ายกัน ดังนั้น ในปี พ.ศ. 2557 (ค.ศ. 2014) Facebook จึงได้พัฒนาโมเดลที่เรียกว่า “DeepFace” ที่ใช้ การเรียนรู้เชิงลึก (Deep learning) ซึ่งเป็นเทคนิคที่ชนะการแข่งขันในงาน ImageNet เมื่อปี พ.ศ. 2555 (ค.ศ. 2012) โดยหลักการเรียนรู้เชิงลึกจะเป็นการรวมของกระบวนการต่าง ๆ ในการสกัดลักษณะเฉพาะภาพใบหน้าด้วยลักษณะเฉพาะแบบหลายชั้น (Multiple-layer feature) ซึ่งสามารถใช้งานได้จริงแม้ในสภาพแวดล้อมที่ไม่มีการควบคุม โดยจากผลการทดสอบประสิทธิภาพความถูกต้องแม่นยำของ DeepFace สามารถทำได้ถึง 97.35% ซึ่งเหนือกว่าการจำแนกด้วยมนุษย์เป็นครั้งแรก นับแต่นั้นเป็นต้นมา การเรียนรู้เชิงลึกจึงเป็นที่นิยมและมีการพัฒนาอย่างต่อเนื่องในรูปแบบต่าง ๆ เช่น Deepfaces [Taigman2014], DeepID [Sun2014], Visual Geometry Group Network (VGG) [Parkhi2015], Facenet [Schroff2015] และอีกหลาย ๆ โมเดลจนมาถึง ArcFace [Deng2019a] ในปี พ.ศ. 2564

จะเห็นได้ว่า จากวิธีการ 4 วิธีที่กล่าวถึงก่อนหน้านี้ อัลกอริทึมที่นิยมที่สุดในปัจจุบัน ได้แก่ อัลกอริทึมการเรียนรู้เชิงลึก (Deep learning) ซึ่งใช้ระบบโครงข่ายประสาทเทียม (Artificial Neural Network) ถือเป็นศาสตร์แขนงหนึ่งของปัญญาประดิษฐ์หรือ AI (Artificial Intelligence) ที่หลายคนอาจจะคุ้นกับคำนี้ โดยมีหลักการทำงาน คือ การทำให้คอมพิวเตอร์มีความสามารถในการพัฒนาตัวเองได้ โดยการเรียนรู้จากข้อผิดพลาด ซึ่งสอนโดยข้อมูลที่มนุษย์กำหนดให้ ตัวอย่างอัลกอริทึมการรู้จำใบหน้าโดยใช้เทคนิคการเรียนรู้เชิงลึก มีสองส่วนที่สำคัญ คือ ส่วนการตรวจจับใบหน้า และส่วนการรู้จำใบหน้า มีรายละเอียดดังนี้

1) **อัลกอริทึมเปิดเผยชุดคำสั่งสำหรับส่วนการตรวจจับใบหน้า**

อัลกอริทึมที่มีความนิยมในปัจจุบันมีชื่อว่า RetinaFace [Deng2019b] เป็นอัลกอริทึมที่ตีพิมพ์ในงาน CVPR 2020 (Computer Vision and Pattern Recognition Conference) และติด 1 ใน 10 เทคนิคที่มีความถูกต้องสูง โดยอัลกอริทึมนี้สามารถทำงานได้ แม้มีการบดบังใบหน้าบางส่วน เช่น การสวมหน้ากากอนามัย หรือการใส่แว่นตากันแดด อีกทั้งยังจะสามารถตรวจหาภาพใบหน้าที่มีขนาดเล็กได้ดีอีกด้วย

2) **อัลกอริทึมเปิดเผยชุดคำสั่งสำหรับส่วนการรู้จำใบหน้า**

อัลกอริทึมที่มีความนิยมในปัจจุบันมีชื่อว่า ArcFace หรือ Additive Angular Margin Loss [Deng2019a] ซึ่งเป็นหนึ่งในโมเดลจดจำใบหน้า (Face recognition model) ที่ดีที่สุดในปัจจุบัน และยังเป็นซอฟต์แวร์ที่เปิดเผยหรือที่เรียกว่า Open Source อีกด้วย อัลกอริทึมการเรียนรู้เชิงลึก ArcFace จะถูกนำมาใช้ในกระบวนการสกัดลักษณะเฉพาะ (Feature extraction) ของใบหน้าแต่ละบุคคล โดยผลลัพธ์การสกัดลักษณะเฉพาะของใบหน้าจะอยู่ในรูปแบบเวกเตอร์ลักษณะเฉพาะ (Feature vector) หรือเรียกอีกอย่างว่า เวกเตอร์ฝังตัว (Embedding vector) ซึ่งจะถูกใช้ในระบบจดจำใบหน้า ทั้ง 2 ขั้นตอน คือ

- ขั้นตอนการลงทะเบียน (Enrollment) เป็นขั้นตอนที่ภาพใบหน้าที่ลงทะเบียนจะถูกสกัดลักษณะเฉพาะ Embedding vectors และเก็บลงในฐานข้อมูล
- ขั้นตอนระบุตัวตน (Authentication) เป็นขั้นตอนที่ภาพใบหน้าที่ต้องการตรวจสอบจะถูกนำมาสกัดลักษณะเฉพาะ Embedding vectors และเปรียบเทียบความเหมือนกับลักษณะเฉพาะ Embedding vectors ที่มีอยู่ในฐานข้อมูลเพื่อระบุตัวตน

โดยการวัดความเหมือนระหว่างเวกเตอร์ลักษณะเฉพาะ (Similarity scoring) จะอยู่ในรูปแบบสมการ Cosine distance ซึ่งจะให้ค่าผลลัพธ์อยู่ในช่วงระหว่าง 0 ถึง 1 ภาพใบหน้าทั้ง 2 ภาพที่เป็นบุคคลเดียวกัน ค่าผลลัพธ์ระยะห่างระหว่าง 2 เวกเตอร์จะมีค่าน้อยหรือมีค่าเข้าใกล้ 0 และในทางกลับกันสำหรับภาพของบุคคลคนละคน

ค่าผลลัพธ์ระยะห่างระหว่าง 2 เวกเตอร์จะมีค่ามากหรือมีค่าเข้าใกล้ 1 ซึ่งผลลัพธ์ค่าความเหมือนนี้สามารถนำมาใช้ได้ทั้งระบบการยืนยันตัวบุคคลด้วยใบหน้า (Face Verification) และการระบุตัวบุคคลด้วยใบหน้า (Face Identification)

การใช้งานอัลกอริทึม ArcFace สามารถดาวน์โหลดได้จาก InsightFace (รายละเอียดตามตารางที่ 1) ซึ่งเป็นผู้พัฒนา Open source ทางด้านการวิเคราะห์ใบหน้า ทั้งภาพใบหน้า 2 มิติ และ 3 มิติ ภายใต้ MIT License โดย InsightFace ได้มีการพัฒนาอัลกอริทึม ArcFace ไว้โดยใช้ Framework ที่เป็นที่นิยมอย่าง Pytorch

ตารางที่ 1 รายชื่ออัลกอริทึมที่เปิดเผยชุดคำสั่งสำหรับการรู้จำใบหน้า

รูปแบบการทำงานของอัลกอริทึม	ชื่ออัลกอริทึม [Ref]	แหล่งดาวน์โหลด
การตรวจจับใบหน้า (Face Detection)	**RetinaFace** [Deng2019b]	https://github.com/serengil/retinaface
การรู้จำใบหน้า (Face Recognition)	**ArcFace** [Deng2019a]	https://github.com/deepinsight/insightface

1.1.3. การนำเทคโนโลยีการรู้จำใบหน้าไปประยุกต์ใช้งาน

ปัจจุบันเทคโนโลยีการรู้จำใบหน้าถูกนำไปประยุกต์ใช้งานในรูปแบบต่าง ๆ อย่างแพร่หลาย ดังต่อไปนี้

1) การควบคุมการเข้าถึง (Access Control)

การประยุกต์ใช้เทคโนโลยีการรู้จำใบหน้าในการควบคุมการเข้าถึง มีตั้งแต่อุปกรณ์ส่วนบุคคล สถานที่รักษาความปลอดภัย ใบอนุญาตให้ผ่านขึ้นเครื่องบินหรือรถไฟ และการใช้ควบคู่กับบัตรเข้าชมกีฬา โดยมีตัวอย่างดังนี้ [1]

- การเข้าถึงอุปกรณ์ส่วนบุคคล สมาร์ทโฟน หรือเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งบริษัทยักษ์ใหญ่ เช่น Apple, Google, Microsoft และ Alibaba ต่างได้มีการพัฒนาการรู้จำใบหน้าเพื่อประยุกต์ใช้งานแล้ว
- การควบคุมการเข้าถึงใบอนุญาตให้ผ่านขึ้นเครื่องบิน (Boarding Pass) โดยใช้สำหรับ check-in ที่สนามบินในประเทศสหรัฐอเมริกา โดยมีมาตั้งแต่ปี พ.ศ. 2561 (ค.ศ. 2018) โดยตรวจสอบหน้ากับภาพ ID ที่เก็บไว้ในฐานข้อมูลของหน่วยงานศุลกากร หรือ U.S. Customs and Border Protection นอกจากนี้ยังใช้งานในอีกหลายประเทศเช่น สหรัฐอาหรับเอมิเรตส์ อังกฤษ [2] และสิงคโปร์ เป็นต้น
- การควบคุมการเข้าถึงใบอนุญาตให้ผ่านขึ้นรถไฟในประเทศจีน ได้ติดตั้งระบบรู้จำใบหน้าไว้ตามสถานีรถไฟ สนามบิน แหล่งท่องเที่ยว งานมหกรรม และอาคารสำนักงาน
- การควบคุมการเข้าถึงสนามกีฬาหรือสวนสนุก (Ticket Pass) มีตัวอย่างต่อไปนี้
  - ในปี ค.ศ. 2008 ใช้ในมหกรรมกีฬาโอลิมปิค (Olympics) ที่ปักกิ่ง ประเทศจีน โดยใช้ระบบรู้จำใบหน้าเพื่อยืนยันตัวบุคคลของผู้ถือตั๋วที่เข้าชมมหกรรมกีฬาในครั้งนั้น
  - ในปี ค.ศ. 2020 สนามอเมริกันฟุตบอลที่ New York และ Los Angeles ได้ติดตั้งระบบรู้จำใบหน้าสำหรับแฟนบอลเพื่อการเข้าสนามฟุตบอล ซึ่งได้ช่วยให้แฟนบอลไม่ต้องสัมผัสอุปกรณ์เท่าที่เป็นไปได้
  - ในช่วงฤดูร้อนปี ค.ศ. 2021 สวนสนุก Disney's Magic Kingdom รัฐ Florida ได้ทดสอบระบบรู้จำใบหน้าเพื่อใช้คู่กับตั๋วรายปี เพื่อให้คนเข้าสวนสนุกไม่ต้องสัมผัสอุปกรณ์ต่าง ๆ ในช่วงการระบาดใหญ่ของ COVID-19 ที่ปกติเคยใช้ระบบรู้จำลายนิ้วมือ

2) การยืนยันตัวบุคคล (Identity Verification)

การประยุกต์ใช้การรู้จำใบหน้าในการยืนยันตัวบุคคล โดยใช้กับบัตรประจำตัวประชาชน หรือ หนังสือเดินทาง มีตัวอย่างดังต่อไปนี้

- ประเทศอินเดีย มีระบบ “Aadhaar” ซึ่งเป็นระบบยืนยันตัวบุคคลในประเทศอินเดีย โดยใช้เลขบัตรประชาชน 12 หลักควบคู่กับการใช้ไบโอเมตริก ซึ่งประกอบด้วย ใบหน้า ลายนิ้วมือ และม่านตา ซึ่งในปี พ.ศ. 2563 (ค.ศ. 2020) ได้มีผู้ลงทะเบียนมากกว่า 1,250 ล้านคนในระบบแล้ว (อ้างอิงจากรายงานประจำปี โดย Unique Identification Authority of India, 2019-2020 [Aadhaar2020][3])

[1] https://en.wikipedia.org/wiki/Facial_recognition_system

[2] https://edition.cnn.com/travel/article/airports-facial-recognition/index.html

[3] https://uidai.gov.in/images/AADHAR_AR_2019_20_ENG_approved.pdf

- ประเทศออสเตรเลีย นิวซีแลนด์ และแคนาดา มีระบบ Automated Border Processing System ที่ได้มีการเปรียบเทียบใบหน้าผู้เดินทางกับภาพที่เก็บไว้ในหนังสือเดินทางอิเล็กทรอนิกส์ (Electronic Passport หรือ e-Passport) เช่น “SmartGate” ที่ใช้ในประเทศออสเตรเลียและนิวซีแลนด์ นอกจากนี้ยังใช้ในสนามบินนานาชาติในประเทศแคนาดาอีกด้วย

3) การรักษาความปลอดภัยและนิติวิทยาศาสตร์ (Security and Forensic)

การประยุกต์ใช้การรู้จำใบหน้าในการรักษาความปลอดภัยและนิติวิทยาศาสตร์ มีการใช้งานในหน่วยงานของภาครัฐหลายประเทศ เช่น ประเทศสหรัฐอเมริกา สาธารณรัฐประชาชนจีน สหภาพยุโรป มีตัวอย่างดังต่อไปนี้

- FBI (สำนักงานสืบสวนของสหรัฐอเมริกา) ได้ติดตั้งระบบ Next Generation Identification program ซึ่งรวมระบบรู้จำใบหน้าที่สามารถค้นหาใบหน้าจากฐานข้อมูลอาชญากรหรือฐานข้อมูลประชาชนได้
- Skynet Project เป็นโครงการที่ริเริ่มโดยรัฐบาลจีน เพื่อสร้างระบบรักษาความปลอดภัย โดยใช้กล้อง CCTV ที่มีกล้อง 20 ล้านตัว ที่มีระบบรู้จำใบหน้าแบบเวลาจริง (Real time) ติดตั้งทั่วประเทศ โดยอ้างว่า ระบบ Skynet จะสามารถตรวจหาใบหน้าของคนทั้งประเทศได้ในเวลาเพียงหนึ่งวินาทีเท่านั้น
- ตำรวจอย่างน้อย 21 ประเทศในสหภาพยุโรป (European Union) ได้มีการวางแผนว่าจะใช้ รวมถึงมีการใช้ระบบรู้จำใบหน้าแล้ว ทั้งในงานบริหารจัดการ หรือใช้ในงานทางด้านอาชญากรรมหรือนิติวิทยาศาสตร์

4) สื่อสังคม (Social Media)

แนวโน้มการประยุกต์ใช้การรู้จำใบหน้าในสื่อสังคมทางออนไลน์เริ่มมีปริมาณเพิ่มขึ้นอย่างรวดเร็ว ดังตัวอย่างต่อไปนี้

- Facebook ใช้ DeepFace เพื่อระบุตัวบุคคลด้วยใบหน้ามนุษย์ในภาพถ่ายดิจิทัลในสังคมออนไลน์ (Social Network) ที่ปัจจุบันมีปัญหาเรื่องการละเมิดสิทธิส่วนบุคคล จึงได้ยกเลิกการใช้งานไปแล้ว
- Tiktok ใช้การรู้จำใบหน้า กับวีดิทัศน์ของผู้ใช้งาน โดยมีอัลกอริทึมเพื่อจะระบุอายุ เพศ และเผ่าพันธุ์
- PimEyes เป็นระบบค้นหารู้จำใบหน้า (Facial-Recognition Search Engine) ซึ่งหากผู้ใช้งานอัปโหลดภาพใบหน้าไปที่เว็บไซต์ PimEyes ระบบจะแสดงภาพของเจ้าของใบหน้าที่สามารถหาได้ในอินเทอร์เน็ต
- ห้าง Westfield Centers ในประเทศออสเตรเลีย และ นิวซีแลนด์ เมื่อลูกค้าไปซื้อของจะถูกสแกนใบหน้าโดยกล้องที่ซ่อนไว้ในป้ายโฆษณาดิจิทัล และระบบจะทำการวิเคราะห์ เพศ อารมณ์ (แบ่งระดับของอารมณ์ (ความสุข) ออกเป็น 5 ระดับ) รวมถึงการวิเคราะห์อายุของลูกค้า เพื่อนำไปใช้วิเคราะห์สำหรับการโฆษณาสินค้าต่อไป
- ป้ายโฆษณาดิจิทัลในเมืองลอนดอน ประเทศอังกฤษ ใช้เทคโนโลยีการรู้จำยี่ห้อรถที่ผ่านไปมา หรือทำการรู้จำใบหน้าโดยสามารถวิเคราะห์เพื่อแยกอายุและเพศของคนเดินในสถานที่สาธารณะ เพื่อนำเสนอการโฆษณาให้เหมาะสมกับกลุ่มเป้าหมาย

1.1.4. จุดเด่นของการรู้จำใบหน้า

เทคโนโลยีการรู้จำใบหน้า มีจุดเด่นของเทคโนโลยีดังต่อไปนี้

1) **ความแม่นยำ** ได้ถูกพัฒนาเพิ่มขึ้นเทียบเคียงกับไบโอเมตริกอื่นที่ใช้งานอยู่ เช่น ลายนิ้วมือ และม่านตา จนสามารถนำไปประยุกต์ใช้งานได้อย่างแพร่หลาย
2) **ระบบมีราคาไม่แพง** ทำให้สามารถใช้งานร่วมกับระบบกล้องวงจรปิดเพื่อรักษาความปลอดภัยได้เป็นอย่างดี โดยระบบสามารถขยายขนาดและรองรับผู้ใช้งานจำนวนมากได้
3) **ผู้ใช้ยอมรับ** ไม่ต่อต้านและมีความสะดวกใจในการใช้งาน
4) **สามารถรู้จำใบหน้าได้ในระยะห่าง** การใช้งานสามารถใช้ได้แม้จะมีระยะห่างระหว่างบุคคลกับอุปกรณ์กล้องหลายเมตร ทำให้ปลอดภัยต่อการใช้งานในช่วงที่มีภาวะโรคระบาด เมื่อเทียบกับระบบที่ต้องมีการสัมผัสระหว่างบุคคลกับอุปกรณ์อย่างเช่นลายนิ้วมือ

1.1.5. ข้อจำกัดหรืออุปสรรคของการใช้งานการรู้จำใบหน้า

การใช้งานเทคโนโลยีล้วนมีข้อจำกัด หรืออุปสรรคที่อาจเกิดขึ้นจากการใช้งาน โดยเทคโนโลยีการรู้จำใบหน้ามีปัจจัยที่อาจทำให้ความแม่นยำของระบบรู้จำใบหน้ามีความผิดพลาดหรือมีความแม่นยำลดลง โดยแบ่งออกเป็น 3 ปัจจัยหลัก ดังต่อไปนี้

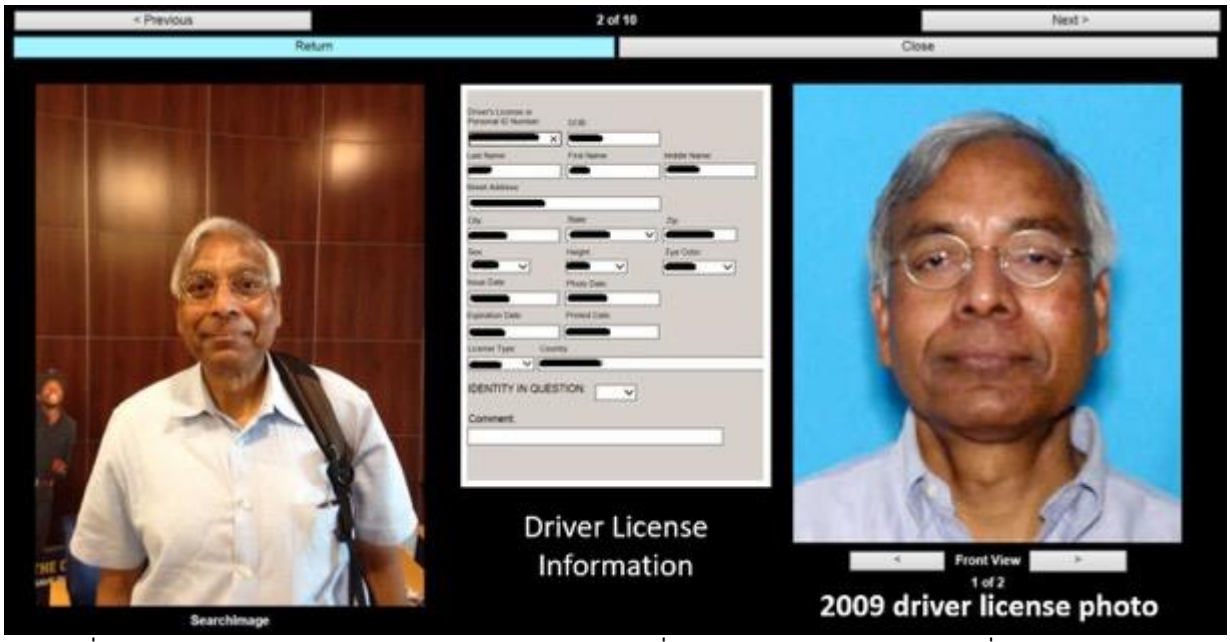
1) **ปัจจัยทางคุณภาพของภาพถ่ายและสภาพแวดล้อม (Image Quality & Environment Factors)** มีเหตุปัจจัยในหลายมิติที่อาจทำให้ระบบรู้จำใบหน้ามีความผิดพลาดเกิดขึ้นได้ เนื่องจากแสงและสภาพแวดล้อมในการถ่ายภาพหรือคุณภาพของภาพใบหน้าที่ไม่เพียงพอ หรือมีการเปลี่ยนแปลง ได้แก่
   - **แสงสว่าง (illumination)** โดยปกติใบหน้าจะมีการเปลี่ยนแปลงไปตามทิศทางที่แสงเข้ามากระทบและเงาที่เกิดขึ้น ซึ่งมีผลต่อระบบรู้จำใบหน้า การถ่ายภาพใบหน้าโดยใช้แสงอินฟราเรดช่วย จะทำให้ผลของแสงธรรมชาติที่เข้ามากระทบในทิศทางต่าง ๆ หายไป รวมทั้งเงาที่เกิดขึ้นด้วย ทำให้แสงทั่วถึงเสมอกันบนใบหน้า เป็นสาเหตุที่ทำให้หลายบริษัทต้องมีอุปกรณ์เสริมทางด้านแสงอินฟราเรดเข้ามาช่วยระบบรู้จำใบหน้า
   - **ทิศทางการวางหน้า (Facial Pose)** ปกติการถ่ายภาพหน้าตรงจะให้ผลลัพธ์ที่ดีต่อระบบรู้จำใบหน้า ถ้าภาพที่ถ่ายออกมาเป็นรูปแบบหน้าเฉียง ระบบรู้จำใบหน้าอาจมีปัญหาได้ ดังนั้น การลงทะเบียนในระบบโดยการให้วางหน้าในหลายมุมจะช่วยแก้ปัญหานี้ได้
   - **การถ่ายภาพ (Photography)** ปัญหาจากการถ่ายภาพก็อาจเป็นอีกสาเหตุหนึ่งที่ทำให้ระบบรู้จำใบหน้าผิดพลาดได้ เช่น การใช้เลนส์ที่มีขนาดแตกต่างกัน เช่น เลนส์มุมกว้าง เลนส์ระยะไกล ซึ่งจะทำให้ภาพมีความผิดเพี้ยนของเลนส์หรือที่เรียกกันว่า Lens Distortion นอกจากนี้ยังขึ้นอยู่กับปัจจัยอื่น ๆ ที่มีผลต่อคุณภาพของภาพใบหน้า เช่น ความละเอียดของภาพ (Resolution) ความคมชัดของภาพ (Contrast) การถ่ายภาพใบหน้าในที่มืดเกินไปหรือสว่างเกินไป (Over/Under Exposure) การบีบอัดภาพ (Compression) การถ่ายภาพที่ไม่โฟกัสหรือภาพเบลอ (Mis-focus or Blur) หรือระยะห่างจากกล้องถึงใบหน้าไกลเกินไป ทำให้มีรายละเอียดน้อย เป็นต้น
2) **ปัจจัยทางชีววิทยา (Biological Factors)** เหตุปัจจัยที่สามารถทำให้ใบหน้าเปลี่ยนแปลง ซึ่งเป็นสาเหตุทางชีววิทยาที่เกิดขึ้นตามธรรมชาติ ได้แก่
   - **ช่วงอายุ (Age)** โดยใบหน้าจะมีการเปลี่ยนแปลงไปตามอายุหรือตามช่วงวัย ตั้งแต่แรกเกิด ทารก เด็กวัยรุ่น ผู้ใหญ่ และคนชรา ซึ่งระบบรู้จำใบหน้าโดยทั่วไปไม่สามารถรองรับการเปลี่ยนแปลงเหล่านี้ได้เมื่อระยะห่างระหว่างเวลาการเก็บภาพใบหน้าที่ลงทะเบียนในระบบและภาพใบหน้าในเวลาปัจจุบันถ้ามีระยะเวลาห่างกันเกิน 6 ปี จะทำให้ระบบรู้จำใบหน้าเริ่มมีปัญหา (อ้างอิงจาก [Best-Rowden2017]) ตัวอย่างปัญหาการรู้จำใบหน้าเมื่อเวลาเปลี่ยนไป ดังแสดงในภาพที่ 4 จะเห็นว่า เมื่อเวลาเปลี่ยนไปคะแนนความเหมือนของภาพใบหน้าที่เข้ามาทีหลังเมื่อเปรียบเทียบกับภาพเมื่อลงทะเบียนแรกเริ่มจะมีคะแนนต่ำลงเรื่อย ๆ ซึ่งแสดงถึงการเปลี่ยนแปลงใบหน้าของบุคคลเดียวกันในระยะเวลาที่แตกต่างกัน

ภาพที่ 4 ภาพตัวอย่างที่ทำการทดสอบกับระบบรู้จำใบหน้า โดยเวลาที่เก็บภาพจะอยู่ด้านบนของภาพ และคะแนนที่ได้จากระบบจะอยู่ด้านล่าง (ภาพได้รับอนุญาตจาก Prof. Anil K. Jain, Michigan State University, USA)

- **การแสดงอารมณ์บนใบหน้า (Facial Expression)** ตามธรรมชาติของมนุษย์แล้วใบหน้าจะมีการเปลี่ยนแปลงไปตามอารมณ์และมีผลต่อระบบในการรู้จำใบหน้า ดังแสดงในภาพที่ 5

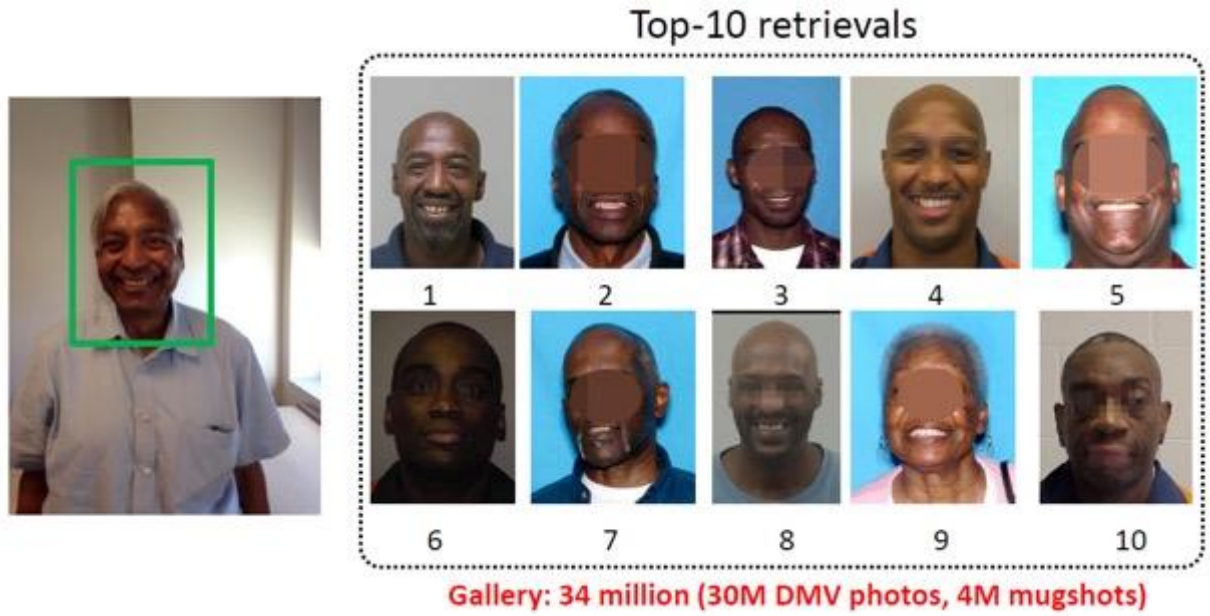
ภาพที่ 5 ความแตกต่างของใบหน้าของคนคนเดียวกัน ที่เกิดจากการแสดงอารมณ์บนใบหน้า
(ภาพ Creative Commons จาก Wikimedia Commons[4])

ศาสตราจารย์ Anil K. Jain แห่งมหาวิทยาลัยแห่งรัฐมิชิแกน (Michigan State University) ประเทศสหรัฐอเมริกา ซึ่งเป็นศาสตราจารย์ผู้นำการวิจัยทางด้านไบโอเมตริกได้ทดสอบระบบรู้จำใบหน้าในปี พ.ศ. 2558 (ค.ศ. 2015) ในระบบระบุตัวบุคคลด้วยใบหน้าในฐานข้อมูลใบขับขี่ของรัฐมิชิแกน ซึ่งมีภาพใบหน้าของบุคคลที่มีใบขับขี่อยู่ 34 ล้านคน ถ้าทำหน้าปกติสามารถระบุตัวบุคคลได้ตามภาพที่ 6 แต่เมื่อเปลี่ยนเป็นยิ้ม ปรากฏว่าระบบรู้จำใบหน้าค้นหาสิบอันดับแรกผิดหมดตามภาพที่ 7 ตัวอย่างนี้แสดงถึงระบบรู้จำใบหน้าในขณะนั้น ยังไม่สามารถรองรับการแสดงอารมณ์บนใบหน้าได้



ภาพที่ 6 การค้นหาบุคคลด้วยใบหน้าของระบบรู้จำใบหน้าสำหรับใบขับขี่มลรัฐมิชิแกน ประเทศสหรัฐอเมริกา ซึ่งสามารถค้นหาใบหน้าย้อนหลังไป 6 ปีได้อย่างแม่นยำ จากฐานข้อมูล 34 ล้านคน (ภาพได้รับอนุญาตจาก Prof. Anil K. Jain, Michigan State University, USA)

[4] https://commons.wikimedia.org/w/index.php?search=Facial+Expression&title=Special:MediaSearch&go=Go&type=image



ภาพที่ 7 เมื่อแสดงอาการยิ้มและทดสอบการระบุตัวบุคคลด้วยใบหน้า ปรากฏว่า ระบบระบุตัวผิดพลาดในสิบอันดับแรก แสดงว่าระบบรู้จำใบหน้าในขณะนั้น ยังไม่สามารถรองรับการเปลี่ยนแปลงใบหน้าที่เกิดจากการแสดงอารมณ์บนใบหน้าได้ (ภาพได้รับอนุญาตจาก Prof. Anil K. Jain, Michigan State University, USA)

- **กรรมพันธุ์ (Genetic)** ฝาแฝดไข่ใบเดียวกันที่มี DNA เหมือนกัน พี่น้องที่มีกรรมพันธุ์หน้าตาคล้ายกัน รวมทั้ง พ่อ แม่ ลูก ที่อาจมีหน้าตาที่คล้ายกันตามธรรมชาติของมนุษย์ สิ่งเหล่านี้ล้วนเป็นอีกปัจจัยที่จะทำให้ระบบรู้จำใบหน้าสับสน ไม่สามารถแยกความแตกต่างของบุคคลเหล่านี้ได้
- **สุขภาพ (Health)** สุขภาพของแต่ละบุคคล ความเจ็บป่วยด้วยโรคต่าง ๆ สามารถทำให้ใบหน้าเปลี่ยนแปลงไป ก็เป็นอีกปัจจัยที่ทำให้ระบบรู้จำใบหน้ามีประสิทธิภาพที่ลดต่ำลง

3) **ปัจจัยทางด้านสังคม (Social Factors)** มีเหตุปัจจัยทางด้านสังคมที่สามารถทำให้ระบบรู้จำใบหน้าทำงานผิดพลาดได้ ซึ่งเกิดได้หลายสาเหตุดังต่อไปนี้
   - รูปพรรณสัณฐาน (Appearance) เช่น การไว้หนวดเครา การแต่งหน้า เขียนคิ้ว ตัดผม ดัดผม หรือทรงผมที่แตกต่าง
   - การมีสิ่งปกปิดใบหน้า (Occlusion) เช่น การใส่แว่น การใส่หน้ากากอนามัยในยุคการแพร่ระบาดของ COVID-19 การปกปิดใบหน้าในศาสนา
   - การทำศัลยกรรม (Surgery) เป็นปัญหาใหญ่ของระบบรู้จำใบหน้า ซึ่งขึ้นอยู่กับว่ามีการเปลี่ยนแปลงใบหน้าไปมากน้อยเพียงใด อย่างไรก็ตาม ล้วนส่งผลต่อความแม่นยำที่ลดลงตามการเปลี่ยนแปลงที่เกิดขึ้น

1.1.6. ความเสี่ยงและข้อควรระวังการใช้งานการรู้จำใบหน้า

เนื่องจากใบหน้าเป็นไบโอเมตริกที่มีการเปิดเผยมากที่สุด ดังนั้น จึงเสี่ยงต่อการปลอมแปลงมากที่สุดด้วยเช่นกัน เช่น การใช้รูปถ่ายที่พิมพ์ออกมาเป็นภาพพิมพ์สีเพื่อหลอกระบบ หรือใช้การเล่นวีดิทัศน์ซ้ำในอุปกรณ์แสดงผลต่าง ๆ รวมถึงการใช้หน้ากากสามมิติหลอกระบบเพื่อให้เชื่อว่าเป็นบุคคลผู้นั้นจริง ดังตัวอย่างแสดงในภาพที่ 8

ภาพที่ 8 ตัวอย่างการโจมตีระบบด้วย ภาพพิมพ์สี การแสดงวีดิทัศน์ผ่านหน้าจออุปกรณ์ต่างๆ และการใช้หน้ากากในการหลอกระบบ (ภาพได้รับอนุญาตจาก Prof. Anil K. Jain, Michigan State University, USA)

แนวทางการป้องกันการโจมตีด้วยการหลอกระบบสามารถทำได้ 2 แนวทาง แนวทางแรก คือ การใช้ฮาร์ดแวร์ เช่น การใช้แสงสีต่าง ๆ ไม่ว่าจะเป็นแสงสีแดง สีเขียว สีฟ้า หรือแสงอินฟราเรด ฉายไปที่ใบหน้า ซึ่งการสะท้อนแสงและการดูดกลืนแสงจากใบหน้าจะมีความแตกต่างกันกับการสะท้อนจากภาพพิมพ์สี จอแสดงผล วัสดุที่ใช้ในการแต่งหน้าและวัสดุที่ใช้ทำหน้ากาก นอกจากนี้ ยังใช้กล้องตรวจจับอุณหภูมิตรวจสอบใบหน้า ซึ่งจะสามารถตรวจจับได้โดยง่าย เนื่องจากเห็นความแตกต่างที่ชัดเจนจากภาพใบหน้าที่จะมีอุณหภูมิที่สูงกว่าสภาพแวดล้อม แต่ที่ตรวจสอบได้ยากกว่า คือ การทำศัลยกรรมพลาสติกให้เหมือนบุคคลเป้าหมาย

อีกแนวทางเป็นการใช้ซอฟต์แวร์ในการตรวจจับภาพที่ผิดปกติ วิธีนี้จะยากกว่าเนื่องจากอาจมีการตกแต่งภาพ ในปัจจุบันระบบรู้จำใบหน้าจะเพิ่มขั้นตอนการป้องกันการโจมตีโดยวิเคราะห์ข้อมูลต่าง ๆ เพิ่มเติมประกอบด้วย เช่น การเคลื่อนไหวของมนุษย์ที่เป็นธรรมชาติเพื่อตรวจจับความมีชีวิต (Liveness Detection) เช่น การกระพริบตา การกรอกตา การเปลี่ยนแปลงแสงเงาและอารมณ์บนใบหน้า การสะท้อนแสงบนวัสดุพื้นผิว เป็นต้น เพื่อยืนยันความถูกต้องก่อนนำเข้าขั้นตอนการจับคู่ใบหน้าต่อไป

1.1.7. แนวโน้มงานวิจัยในปัจจุบันของการรู้จำใบหน้า

แนวโน้มงานวิจัยที่เกี่ยวข้องกับการรู้จำใบหน้าที่กำลังเป็นที่สนใจในปัจจุบัน ซึ่งผู้ที่สนใจสามารถศึกษาเพิ่มเติม (รายละเอียดปรากฏในเอกสารอ้างอิง) ได้แก่

1) การแก้ปัญหาการรู้จำใบหน้าให้ทนต่อการเปลี่ยนแปลง เช่น การแสดงสีหน้าที่แตกต่างกัน [Xia2021], [Huang2021] การวางทิศทางของหน้าที่แตกต่างกัน [Wang2021a], [Tu2021] หรือการถูกบดบังจากหน้ากาก [Qiu2021]
2) การป้องกันการโจมตีระบบรู้จำใบหน้าด้วยใบหน้าปลอม เช่น [Lin2021], [Wang2021b], [Shen2021], [Qin2021], [Yu2021], [Jia2021]
3) การเชื่อมโยงการรู้จำใบหน้าแบบแสงที่ตามองเห็นกับแสงอินฟราเรด เช่น [Hu2021a], [Hu2021b]
4) การประเมินคุณภาพของภาพใบหน้าเพื่อควบคุมความเสี่ยงของระบบรู้จำใบหน้า เช่น [Chen2021]
5) การรู้จำใบหน้าจากผู้ใช้อุปกรณ์เคลื่อนที่ เช่น [Keykhaie2021]

1.2. การรู้จำลายนิ้วมือ (Fingerprint Recognition)

การใช้ลายนิ้วมือในการระบุตัวบุคคลมีการค้นพบมาตั้งแต่สมัยราชวงศ์ฉิน (221-206 ปี ก่อนคริสต์ศักราช) ของจีน โดยอ้างอิงจาก [Barnes2011] และ History of Fingerprint ซึ่งเรียบเรียงโดย German [5] ลายนิ้วมือสามารถพบได้ทั่วไปบนตราดิน (Clay sealed) ของหนังสือที่ทำจากไม้ไผ่ โดยด้านหนึ่งของตราดินจะเป็นตัวอักษรชื่อ และอีกด้านจะเป็นลายนิ้วมือของผู้แต่งหนังสือ ที่ใช้เพื่อแสดงความเป็นเจ้าของผลงานของผู้แต่งหนังสือ ภายหลังในยุคที่มีการสร้างกระดาษได้ในประเทศจีน (ปี ค.ศ. 105) การทำเอกสารสัญญาทั้งทางธุรกิจ และการทหาร จะใช้การประทับลายนิ้วมือลงในเอกสาร การใช้ลายนิ้วมือในลักษณะนี้แสดงให้เห็นว่ามีการใช้ลายนิ้วมือในการระบุตัวบุคคลมานานแล้วในแถบทวีปเอเชีย

ในปี พ.ศ. 2331 (ค.ศ. 1788) ลักษณะเฉพาะที่เป็นเอกลักษณ์ (Uniqueness) ของลายนิ้วมือในแต่ละบุคคลได้ถูกค้นพบครั้งแรกในทวีปยุโรปโดยหมอชาวเยอรมันที่ชื่อว่า J.C.A. Mayer และมีการตีพิมพ์หนังสือเกี่ยวกับลักษณะเฉพาะที่เป็นเอกลักษณ์ และความคงทนถาวร (Permanence) ของลายนิ้วมือเล่มแรกโดยชาวอังกฤษ Sir Francis Galton ในปี พ.ศ. 2435 (ค.ศ. 1892) จากนั้นจึงเริ่มมีการนำลายนิ้วมือมาใช้ในหน่วยงานบังคับใช้กฎหมาย เช่น คดีฆาตกรรม Rojas ที่บัวโนสไอเรส ประเทศอาร์เจนตินา ในปี พ.ศ. 2435 (ค.ศ. 1892) ที่ถือเป็นคดีฆาตกรรมแรกที่คลี่คลายด้วยการใช้ลายนิ้วมือ เป็นต้น จากความสำเร็จในการนำลายนิ้วมือมาใช้ระบุตัวบุคคลทำให้ลายนิ้วมือถูกใช้อย่างแพร่หลาย และเทคโนโลยีที่เกี่ยวข้องได้ถูกพัฒนามาอย่างต่อเนื่อง ปัจจุบันมีการใช้ระบบระบุตัวบุคคลด้วยลายนิ้วมืออัตโนมัติ (Automated Fingerprint Identification System : AFIS) ทั้งในหน่วยงานรัฐบาลและเอกชน เช่น งานตรวจคนเข้าเมือง การตรวจสอบประวัติการทำงาน และการรักษาความปลอดภัยของทรัพย์สินต่าง ๆ เป็นต้น [Maltoni2009]

1.2.1. หลักการทำงานของการรู้จำลายนิ้วมือ

การระบุตัวบุคคลด้วยการรู้จำลายนิ้วมือ สามารถทำได้โดยพิจารณาลักษณะเฉพาะ (Feature) ของลายนิ้วมือ ซึ่งแบ่งออกได้เป็น 3 ระดับ โดยแต่ละระดับจะให้ประโยชน์ในกระบวนการการรู้จำลายนิ้วมือที่แตกต่างกันไป ดังนี้

ระดับที่ 1: ระดับครอบคลุม (Level 1: Global Level)

ลักษณะเฉพาะระดับครอบคลุม มีลักษณะเป็นรูปแบบ (Pattern) ของทิศทางเส้นลายนิ้วมือในภาพรวม หรือสนามทิศทาง (Orientation Field) ดังแสดงในภาพที่ 9 โดยรูปแบบของสนามทิศทางนี้สามารถใช้ในการบ่งชี้ชนิดของลายนิ้วมือ และใช้ในการระบุตำแหน่งของจุดเอกฐาน (Singular Point) ได้ โดยจุดเอกฐานสามารถจำแนกออกเป็น 2 ชนิด คือ จุดแก่น (Core Point) และจุดสามเหลี่ยม (Delta Point) โดยจุดแก่น คือ จุดที่มีความโค้งสูงที่สุด และอยู่ด้านในสุดของลายนิ้วมือ ในขณะที่จุดสามเหลี่ยมคือจุดที่เส้นลายนิ้วมือ 3 ทิศทางมาชนกันดังแสดงในภาพที่ 9 (ข)

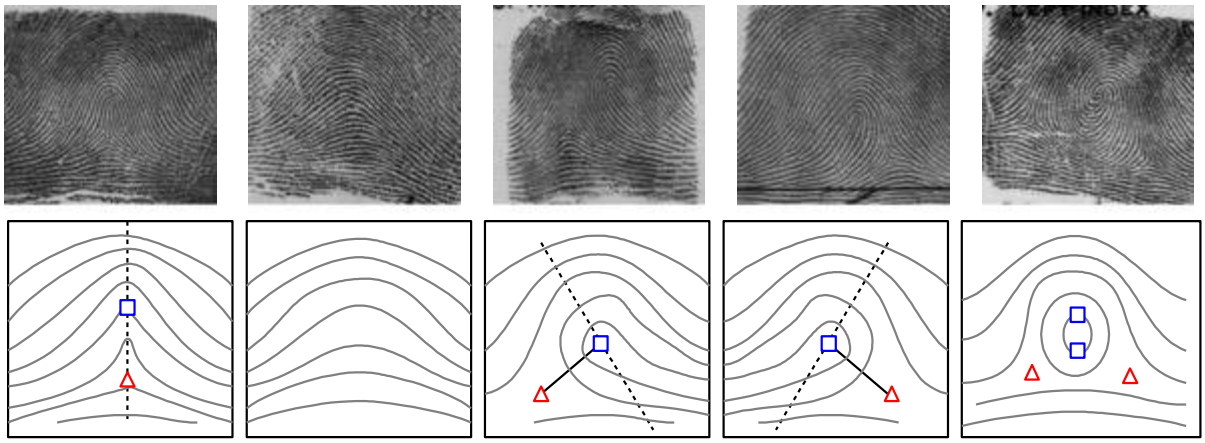
ลักษณะเฉพาะระดับครอบคลุมสามารถจำแนกได้เป็น 5 ชนิดตามแนวทางของ Henry [Henry1900] คือ มัดหวายปัดซ้าย (Left Loop) มัดหวายปัดขวา (Right Loop) ก้นหอย (Whorl) โค้งราบ (Plain Arch) และโค้งกระโจม (Tented Arch) ดังแสดงในภาพที่ 10

ลักษณะเฉพาะระดับนี้ มักใช้ในการแบ่งประเภทลายนิ้วมือก่อนการเปรียบเทียบลายนิ้วมือ เช่น การระบุตัวบุคคลด้วยลายนิ้วมือ ถ้าภาพลายนิ้วมือที่ต้องการค้นหาเป็นชนิดก้นหอย ระบบก็จะค้นหาข้อมูลเฉพาะลายนิ้วมือชนิดก้นหอย เป็นต้น หรือใช้เป็นลักษณะเฉพาะพื้นฐานในการประมวลผลขั้นถัดไป เช่น การหมุนลายนิ้วมือให้ตรงโดยการใช้จุดแก่น และจุดสามเหลี่ยมเป็นจุดอ้างอิง การใช้ทิศทางลายนิ้วมือสำหรับการต่อเส้นลายนิ้วมือในกระบวนการปรับปรุงภาพ เป็นต้น

[5] https://onin.com/fp/fphistory.html

ก) ลายนิ้วมือมัดหวายปัดขวา ข) สนามทิศทาง (จุดแก่น □, จุดสามเหลี่ยม Δ)

ภาพที่ 9 ลายนิ้วมือมัดหวายปัดขวาภาพที่ 10_5 จากฐานข้อมูลลายนิ้วมือมาตรฐาน FVC2004 DB1 [Maio2004] และสนามทิศทาง

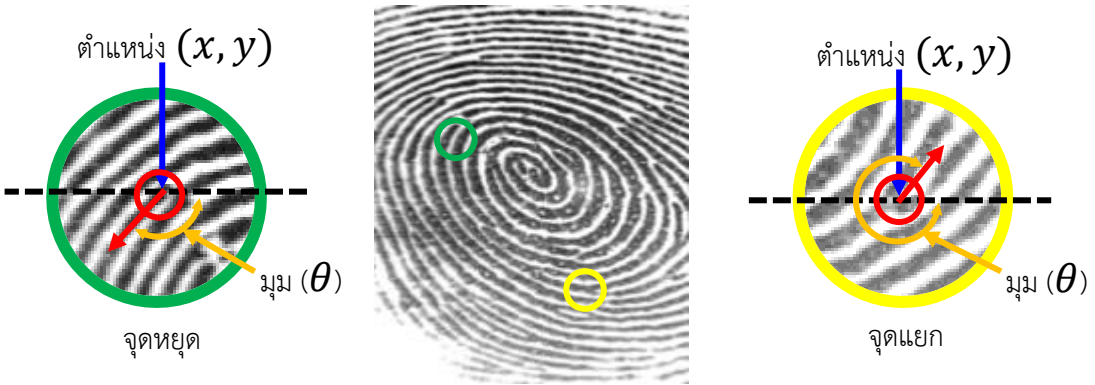


ก) โค้งกระโจม (Tented Arch) **ข) โค้งราบ (Plain Arch)** **ค) มัดหวายปัดขวา (Right Loop)** **ง) มัดหวายปัดซ้าย (Left Loop)** **จ) ก้นหอย (Whorl)**

ภาพที่ 10 ลายนิ้วมือทั้ง 5 ชนิดจากฐานข้อมูลมาตรฐาน NIST4 [Watson1992] ตามการจำแนกของ Henry [Henry1900]

ระดับที่ 2: ระดับเฉพาะที่ (Level 2: Local Level)

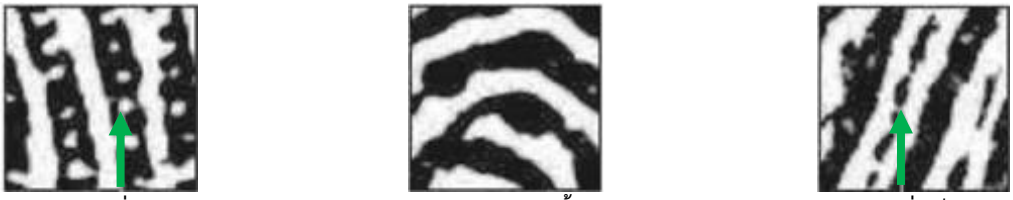
ลักษณะเฉพาะระดับเฉพาะที่ เป็นลักษณะเฉพาะที่แสดงรายละเอียดที่สามารถบ่งบอกความแตกต่างระหว่างลายนิ้วมือ ที่ใช้โดยทั่วไปจะเป็น จุดแยก (Bifurcation Point) และจุดหยุด (Ending Point) ของเส้นลายนิ้วมือ ดังแสดงในภาพที่ 11 โดยเรียกว่า จุดมินูเทียร์ (Minutia) ซึ่งค้นพบโดย Sir Francis Galton ในปี ค.ศ. 1888 จุดมินูเทียร์นี้เกิดกระจายอยู่ทั่วไปบนลายนิ้วมือในลักษณะสุ่ม (Random) ซึ่งทำให้แต่ละลายนิ้วมือของแต่ละบุคคลมีลักษณะเฉพาะที่โดดเด่นและแตกต่าง (Unique) โดยจุดมินูเทียร์จะประกอบไปด้วย ตำแหน่งพิกัดแกนตั้งและแกนนอนของภาพ x, y และทิศทางหรือมุมของจุดมินูเทียร์ θ ลักษณะเฉพาะระดับนี้จะถูกใช้ในการเปรียบเทียบลายนิ้วมือ เพื่อบ่งชี้ว่าเป็นลายนิ้วมือเดียวกันหรือไม่ โดยจะพิจารณาจากความสัมพันธ์ทางตำแหน่งและทิศทางของจุดมินูเทียร์



ภาพที่ 11 จุดมินูเทียร์แบบจุดหยุด และจุดแยก (ภาพจาก ฐานข้อมูลมาตรฐาน NIST4 [Watson1992])

ระดับที่ 3: ระดับละเอียดมาก (Level 3: Very-Fine Level)

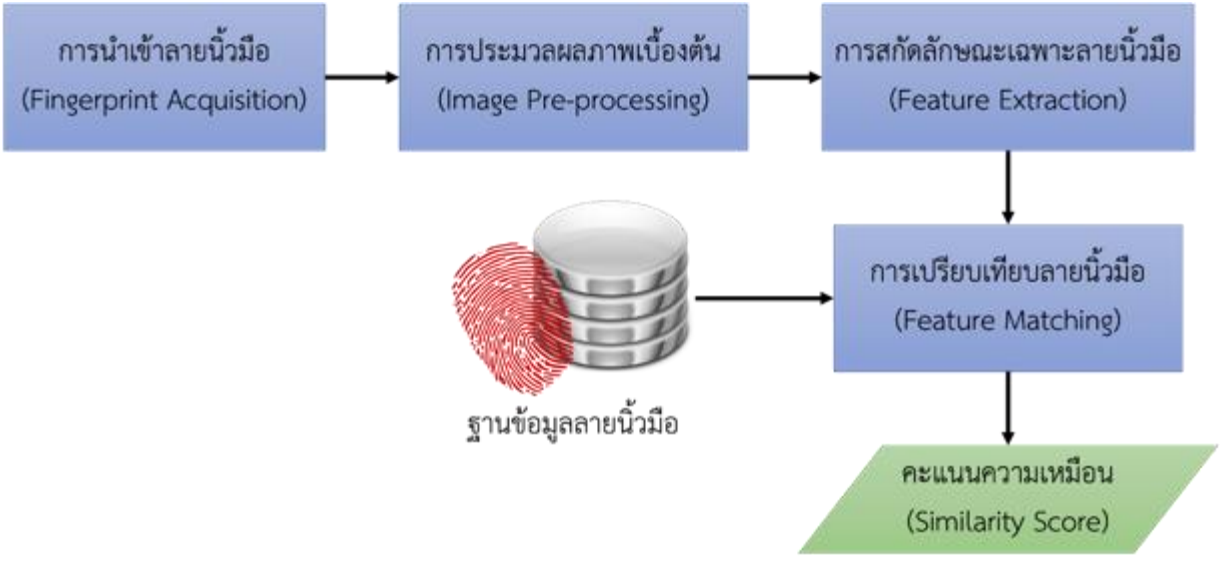
ลักษณะเฉพาะระดับละเอียดมาก เป็นลักษณะเฉพาะที่ที่มีรายละเอียดเกี่ยวข้องกับเส้นลายนิ้วมือ ได้แก่ รูเหงื่อ (Pore) รูปร่างของเส้นลายนิ้วมือ (Ridge Shape) เส้นเริ่มเป็นสัน (Incipient Ridge) หรือ เส้นสันรอง (Secondary Ridge) ดังแสดงในภาพที่ 12 ซึ่งลักษณะเฉพาะดังกล่าวจะสามารถตรวจจับได้เฉพาะในภาพที่มีความละเอียดสูง คือ 1,000 จุดภาพต่อนิ้ว (pixels per inch (ppi)) ขึ้นไปเท่านั้น ในขณะที่ความละเอียดภาพลายนิ้วมือตามมาตรฐาน ISO19794-4:2011 จะอยู่ที่ 500 ppi ทำให้การประยุกต์ใช้ลักษณะเฉพาะระดับนี้จำกัดอยู่ที่งานด้านนิติวิทยาศาสตร์ ที่ใช้ตำแหน่งของรูเหงื่อ และเส้นเริ่มเป็นสัน ในการเปรียบเทียบลายนิ้วมือเพื่อบ่งชี้ว่าเป็นลายนิ้วมือเดียวกันหรือไม่



ก) รูเหงื่อ ข) รูปร่างเส้นลายนิ้วมือ ค) เส้นเริ่มเป็นสัน

ภาพที่ 12 ลักษณะเฉพาะของลายนิ้วมือระดับที่ 3 [15] (ภาพจาก [15])

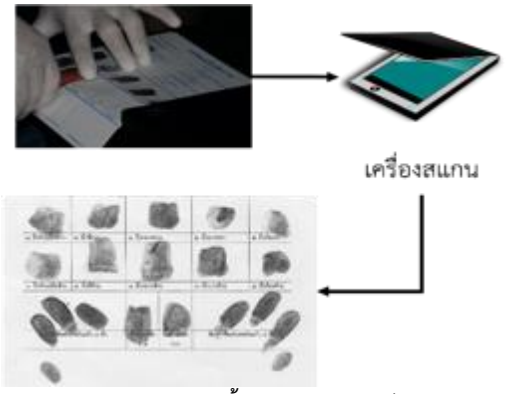
ระบบ AFIS ที่ใช้ในปัจจุบันมีกระบวนการทำงาน 2 รูปแบบ คือ การยืนยันตัวบุคคล (Verification) และการระบุตัวบุคคล (Identification) ในการยืนยันตัวบุคคล ซึ่งระบบจะเปรียบเทียบลายนิ้วมือแบบ 1 ต่อ 1 (1:1) โดยเปรียบเทียบลายนิ้วมือบุคคลจากการสแกนหรือป้อนเข้าระบบในขณะนั้น (Live Scan) กับลายนิ้วมือตามข้อมูลรหัสอ้างอิงของบุคคลนั้นที่อยู่ในฐานข้อมูลของระบบ แล้วตัดสินว่าเป็นบุคคลเดียวกันหรือไม่จากคะแนนความเหมือนที่วัดได้จากการเปรียบเทียบ ในขณะที่การระบุตัวบุคคลจะเปรียบเทียบลายนิ้วมือแบบ 1 ต่อ หลาย (1:N) โดยเปรียบเทียบลายนิ้วมือที่ป้อนเข้าระบบ กับลายนิ้วมือทั้งหมดในฐานข้อมูลของระบบ แล้วให้ผลลัพธ์เป็นลำดับรายการบุคคล (Candidate list) ที่เรียงลำดับรายการจากคะแนนความเหมือนจากมากไปหาน้อย (อันดับที่ 1 คือคะแนนสูงที่สุด) โดยกระบวนการการทำงานของทั้ง 2 รูปแบบจะคล้ายกันเพื่อให้ได้ผลลัพธ์เป็นคะแนนความเหมือนออกมา ซึ่งประกอบด้วย 4 กระบวนการหลัก ดังแสดงในภาพที่ 13 โดยมีรายละเอียดดังต่อไปนี้



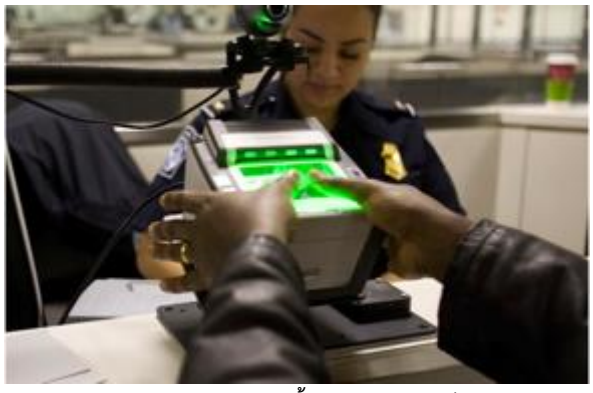
ภาพที่ 13 กระบวนการทำงานของการรู้จำลายนิ้วมือ

1) **การนำเข้าลายนิ้วมือ (Fingerprint Acquisition)** กระบวนการนี้จะได้ลายนิ้วมือมาในรูปแบบดิจิทัล หรือภาพลายนิ้วมือ ซึ่งอาจได้มาโดยตรงจากการสแกนผ่านเซนเซอร์ หรืออาจได้มาจากการสแกนภาพพิมพ์หมึก (ภาพที่ 14) โดยภาพลายนิ้วมือหนึ่งภาพจะต้องมีลายนิ้วมือปรากฏเพียงลายนิ้วมือเดียวเท่านั้น หากภาพมีมากกว่าหนึ่งลายนิ้วมือ จะต้องทำการตัดครอบ (Crop) แยกลายนิ้วมือ จากนั้นอาจมีการวัดคุณภาพของลายนิ้วมือว่าดีพอจะนำเข้าระบบหรือไม่ ถ้าคุณภาพต่ำกว่าเกณฑ์ที่กำหนดระบบอาจปฏิเสธการนำเข้าและ

ให้ผู้ใช้นำเข้าลายนิ้วมือใหม่ โดยค่าคุณภาพนี้อาจวัดจากความคมชัดของเส้นลายนิ้วมือกับร่องลายนิ้วมือ รวมถึงพื้นที่ลายนิ้วมือที่ปรากฏบนภาพว่ามีพื้นที่มากเพียงพอต่อการรู้จำของระบบหรือไม่ เป็นต้น



ก) การนำเข้าลายนิ้วมือจากภาพพิมพ์หมึก



ข) การนำเข้าลายนิ้วมือจากเซนเซอร์

ภาพที่ 14 การนำเข้าลายนิ้วมือ

(ภาพ (ก) จาก [วุฒิพงศ์2557] และภาพ (ข) จาก https://commons.wikimedia.org/wiki/File:US-VISIT_(CBP).jpg)

2) **การประมวลผลภาพเบื้องต้น (Image Pre-processing)** เป็นกระบวนการที่ทำให้ภาพลายนิ้วมือที่นำเข้าพร้อมใช้งานในกระบวนการถัดไป (ภาพที่ 15) โดยเกี่ยวข้องกับการระบุพื้นที่ลายนิ้วมือบนภาพ (Segmentation) ปรับลายนิ้วมือให้ตรง (Alignment) เช่น หมุนลายนิ้วมือให้ปลายนิ้วชี้ขึ้น เป็นต้น มีการปรับปรุงคุณภาพลายนิ้วมือ (Enhancement) เช่น ลบรอยเปื้อน ต่อเส้นลายนิ้วมือ ปรับให้เส้นลายนิ้วมือคมชัดมากขึ้น เป็นต้น

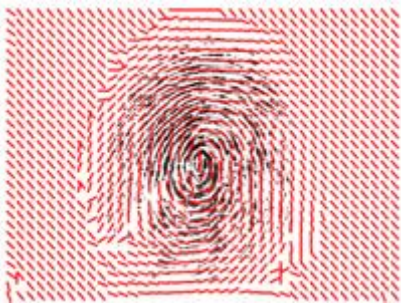
ก) ภาพต้นฉบับ

ข) พื้นที่ลายนิ้วมือ (สีขาว)

ค) ภาพลายนิ้วมือที่ผ่านการปรับปรุง

ภาพที่ 15 ผลลัพธ์การประมวลผลภาพเบื้องต้นของลายนิ้วมือภาพที่ 5_7 จากฐานข้อมูลมาตรฐาน FVC2004 DB1 [Maio2004]

3) **การสกัดลักษณะเฉพาะลายนิ้วมือ (Feature Extraction)** กระบวนการนี้เกี่ยวข้องกับการตรวจจับลักษณะเฉพาะของลายนิ้วมือ ดังแสดงในภาพที่ 16 ซึ่งส่วนใหญ่จะตรวจจับจุดมินูเทียร์โดยการหาตำแหน่งและทิศทาง



ก) สนามทิศทาง

ข) จุดมินูเทียร์

ภาพที่ 16 ลักษณะเฉพาะของลายนิ้วมือภาพที่ 5_7 จากฐานข้อมูลมาตรฐาน FVC2004 DB1 [Maio2004]

4) **การเปรียบเทียบลายนิ้วมือ (Feature Matching)** หลังจากได้ลักษณะเฉพาะที่ใช้ในการเปรียบเทียบแล้ว ในส่วนนี้จะสร้างตัวบ่งชี้ลักษณะเฉพาะ (Feature Descriptor) ขึ้นมา และใช้ตัวบ่งชี้นี้ในการเปรียบเทียบลายนิ้วมือ โดยลายนิ้วมือที่มาจากนิ้วเดียวกันจะมีตัวบ่งชี้ลักษณะเฉพาะที่เหมือนกัน ดังแสดงในภาพที่ 17 เช่น มีการกระจายตัวของจุดมินูเทียร์เหมือนกัน เป็นต้น ซึ่งจะให้ผลลัพธ์การเปรียบเทียบเป็นคะแนนความเหมือน

ก) ภาพที่ 5_3 ข) ภาพที่ 5_7

ภาพที่ 17 ผลลัพธ์การเปรียบเทียบจุดมินูเทียร์ของลายนิ้วมือภาพที่ 5_3 กับ 5_7 จากฐานข้อมูลมาตรฐาน FVC2004 DB1 [Maio2004]

1.2.2. อัลกอริทึมการรู้จำลายนิ้วมือ

อัลกอริทึมรู้จำลายนิ้วมือในปัจจุบันสามารถแบ่งได้เป็น 2 แนวทาง คือ แนวทางที่ใช้ความรอบรู้ของมนุษย์ (Knowledge-based Approach) และแนวทางที่ใช้การเรียนรู้ของคอมพิวเตอร์ (Learning-based Approach)

1) **แนวทางที่ใช้ความรอบรู้ของมนุษย์ (Knowledge-based Approach)**

แนวทางนี้มุ่งเน้นใช้ความรอบรู้ของมนุษย์ในการออกแบบทุกขั้นตอน ตั้งแต่การนำภาพลายนิ้วมือเข้า การประมวลภาพเบื้องต้น การสกัดลักษณะเฉพาะ และการเปรียบเทียบลายนิ้วมือ โดยรายละเอียดของแต่ละขั้นตอนและความหลากหลายในการแก้ปัญหาด้วยวิธีการต่าง ๆ ได้รวบรวมไว้ในหนังสือการประมวลลายนิ้วมือดิจิทัล [วุฒิพงศ์, 2557] แล้ว

หนึ่งในอัลกอริทึมที่มีการเปิดเผยกระบวนการทำงานที่ดีในปัจจุบัน คือ รหัสมินูเทียร์ทรงกระบอก (Minutiae Cylinder-Code (MCC)) [Cappelli2010] โดยตัวบ่งชี้ลักษณะเฉพาะของมินูเทียร์ที่สนใจ จะเป็นลักษณะทรงกระบอกที่แบ่งแต่ละส่วนเป็นเซลล์ ซึ่งแต่ละเซลล์ใช้บ่งชี้การปรากฏของมินูเทียร์เพื่อนบ้านทั้งความสัมพันธ์ทางตำแหน่งและความสัมพันธ์เชิงมุม โดยความสัมพันธ์ทางตำแหน่งจะถูกเข้ารหัสทางแกนแนวระนาบของทรงกระบอก ในขณะที่ความสัมพันธ์เชิงมุมจะถูกเข้ารหัสทางแกนแนวตั้งของทรงกระบอก ซึ่งการจับคู่โครงสร้างมินูเทียร์จะใช้รหัสทรงกระบอกนี้ในการพิจารณา โดยเปรียบเทียบความเหมือนของรหัสทรงกระบอกของมินูเทียร์ทั้งหมดระหว่างภาพลายนิ้วมือที่ต้องการตรวจสอบ (Query) และภาพลายนิ้วมือในฐานข้อมูล (Gallery) และใช้ฮังกาเรียนอัลกอริทึม (Hungarian Algorithm) ในการตัดสินว่ามินูเทียร์แต่ละจุดจากภาพ Query ต้องคู่กับมินูเทียร์จุดใดในภาพ Gallery ซึ่งพิจารณาจากความเหมือนของรหัสทรงกระบอกของมินูเทียร์และจะไม่จับคู่ซ้ำกัน จากนั้นจะนำมินูเทียร์ที่จับคู่กันได้มาใช้เป็นจุดมินูเทียร์อ้างอิงในการจับคู่มินูเทียร์ในภาพรวม โดยคะแนนความเหมือนจะคำนวนจากผลรวมเฉลี่ยของความเหมือนของรหัสทรงกระบอกของมินูเทียร์ที่จับคู่ได้ในภาพรวม

2) **แนวทางที่ใช้การเรียนรู้ของคอมพิวเตอร์ (Learning-based Approach)**

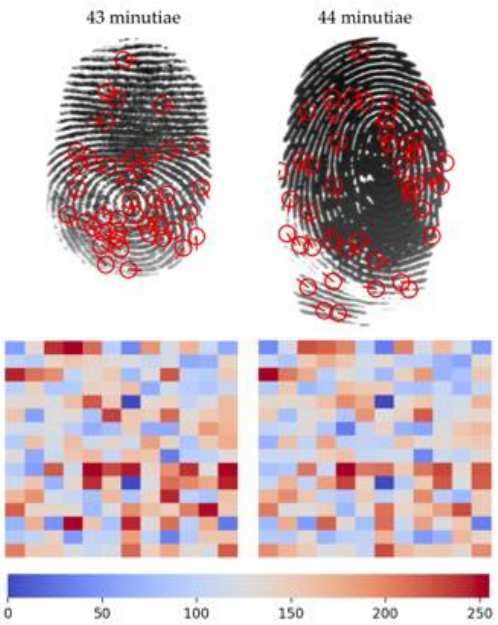
อัลกอริทึมที่ได้จากการเรียนรู้ของคอมพิวเตอร์มีการพัฒนาอย่างก้าวกระโดดเนื่องจากมีข้อมูลมากพอในการสอนคอมพิวเตอร์ (Training) และความก้าวหน้าของเทคนิคในการเรียนรู้ของคอมพิวเตอร์ โดยอัลกอริทึมในช่วงแรกจะอาศัยลักษณะเฉพาะของลายนิ้วมือจากแนวทางที่ใช้ความรอบรู้ของมนุษย์ (Knowledge-based Approach) ในการสอนคอมพิวเตอร์เพื่อทำงานเฉพาะส่วน หรือเฉพาะกระบวนการใดกระบวนการหนึ่งในระบบ เช่น NFIQ2 [Tabassi2021] ที่ใช้ประเมินคุณภาพลายนิ้วมือในภาพรวม ซึ่งอาศัยลักษณะเฉพาะต่าง ๆ ของลายนิ้วมือที่ใช้ในการบ่งชี้คุณภาพจากแนวทางที่ใช้ความรอบรู้ของมนุษย์ในการสอนคอมพิวเตอร์ด้วยวิธี Random Forest ที่เป็นการเทรนโมเดลที่เหมือนกันหลาย ๆ ครั้ง บนข้อมูลชุดเดียวกัน เพื่อให้ผลลัพธ์เป็นค่าคะแนนคุณภาพในช่วง 0-100 คะแนน ซึ่งคะแนน 100 คือ คะแนนคุณภาพดีที่สุด เป็นต้น

ในปัจจุบันหลังจากมีการค้นพบเทคนิคการเรียนรู้เชิงลึก (Deep Learning) ของคอมพิวเตอร์ อัลกอริทึมในรูปแบบนี้ได้ถูกพัฒนาให้ทำงานครอบคลุมหลายกระบวนการ เช่น กระบวนการประมวลผลภาพเบื้องต้น และกระบวนการสกัดลักษณะเฉพาะลายนิ้วมือ สามารถทำได้โดยใช้อัลกอริทึม FingerNet [Tang2017] อัลกอริทึมเดียวเพื่อให้ได้ภาพพื้นที่ลายนิ้วมือ ภาพลายนิ้วมือที่ผ่านการปรับปรุงแล้ว สนามทิศทางของลายนิ้วมือ และจุดมินูเทียร์ เป็นต้น แต่สำหรับอัลกอริทึมที่มีกระบวนการเปรียบเทียบลายนิ้วมือด้วยมักจะพัฒนาแบบครบวงจร (End-to-End) ซึ่งอัลกอริทึมที่ดีที่สุดในปัจจุบันที่เปิดเผยในงานวิจัย คือ ลักษณะเฉพาะลายนิ้วมือเชิงลึก (DeepPrint) [Engelsma2019] ซึ่งอาศัยภาพลายนิ้วมือและจุดมินูเทียร์ทั้งหมด 455,000 ภาพ จาก 38,291 นิ้ว (นิ้วละ ≈ 12 ภาพ แต่ละภาพมีช่วงเวลาเก็บต่างกันโดยช่วงเวลาที่ต่างกันน้อยที่สุดคือ 2 เดือน และระยะห่างมากที่สุดคือ 12 ปี) ในการสอนคอมพิวเตอร์โดยอัลกอริทึมจะตรวจจับลักษณะเฉพาะเชิงลึกออกมาได้ 2 ชนิด คือ ลักษณะเฉพาะองค์ประกอบ (Texture Feature) และลักษณะเฉพาะจุดมินูเทียร์ (Minutiae Feature) ซึ่งแต่ละชนิดมีค่าลักษณะเฉพาะ 96 ค่า (รวมสองชนิดมี 192 ค่า) ในการเปรียบเทียบลายนิ้วมือจะใช้ค่าลักษณะเฉพาะนี้ในการเปรียบเทียบโดยมองค่าลักษณะเฉพาะนี้เป็นเวกเตอร์ และให้คะแนนความเหมือนเท่ากับผลลัพธ์จากการวัดความเหมือนของเวกเตอร์แบบโคซายน์ (Cosine Similarity) ดังสมการที่ (1)

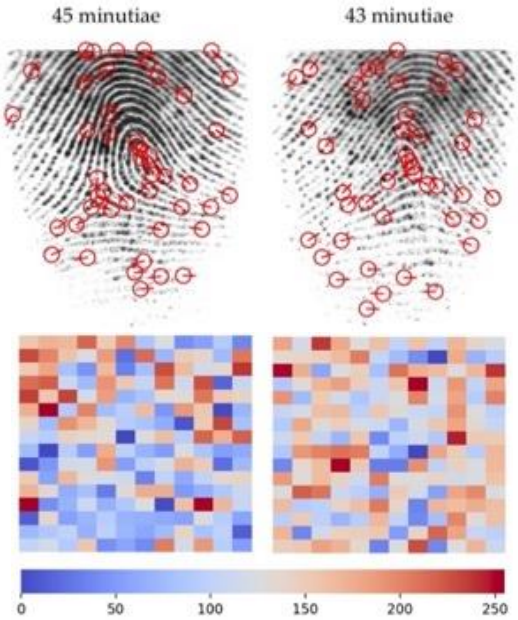
$$\text{คะแนนความเหมือน} = \mathbf{A}^{\mathrm{T}} \cdot \mathbf{B} = \frac{\sum_{i=1}^{192} A_i B_i}{\sqrt{\sum_{i=1}^{192} A_i^2}\sqrt{\sum_{i=1}^{192} B_i^2}} \quad (1)$$

โดยที่ $\mathbf{A}$ คือ เวกเตอร์ลักษณะเฉพาะจากภาพลายนิ้วมือ Query และ $\mathbf{B}$ คือ เวกเตอร์ลักษณะเฉพาะจากภาพลายนิ้วมือ Gallery

ภาพที่ 18 และ 19 แสดงตัวอย่างภาพลายนิ้วมือ และลักษณะเฉพาะลายนิ้วมือเชิงลึกที่ได้จากอัลกอริทึม DeepPrint โดยลายนิ้วมือในภาพที่ 18 เป็นลายนิ้วมือ 2 ภาพ จากนิ้วเดียวกันแต่มีการกระจายตัวมินูเทียร์ที่ต่างกัน ซึ่งเกิดจากสภาพผิว การวางนิ้ว และแรงกดที่ไม่เหมาะสม โดยอัลกอริทึมแนวทางที่ใช้ความรอบรู้ของมนุษย์ ที่พิจารณาความเหมือนจากการกระจายตัวมินูเทียร์เป็นหลักจะให้ค่าคะแนนความเหมือนต่ำและตัดสินว่าไม่ใช่นิ้วเดียวกัน ในขณะที่ลักษณะเฉพาะลายนิ้วมือเชิงลึกจาก DeepPrint มีความใกล้เคียงกัน (สังเกตได้จากค่าสีแต่ละช่องคล้ายกัน) จึงมีค่าคะแนนความเหมือนสูงและตัดสินว่าเป็นภาพลายนิ้วมือที่มาจากนิ้วเดียวกัน และในทางตรงกันข้ามภาพที่ 19 เป็นลายนิ้วมือ 2 ภาพ ที่มาจากคนละนิ้วแต่มีการกระจายตัวมินูเทียร์ที่ใกล้เคียงกัน อัลกอริทึมแนวทางที่ใช้ความรอบรู้ของมนุษย์ จะให้ค่าคะแนนความเหมือนสูงและตัดสินว่าเป็นภาพลายนิ้วมือที่มาจากนิ้วเดียวกัน ในขณะที่ลักษณะเฉพาะลายนิ้วมือเชิงลึกมีความแตกต่างกันมากจึงมีค่าคะแนนความเหมือนต่ำและตัดสินว่าเป็นภาพลายนิ้วมือที่ไม่ได้มาจากนิ้วเดียวกัน



ภาพที่ 18 ตัวอย่างภาพลายนิ้วมือที่มาจากนิ้วเดียวกันที่อัลกอริทึมแนวทางที่ใช้ความรอบรู้ของมนุษย์ตัดสินว่าไม่ใช่นิ้วเดียวกัน ในขณะที่ DeepPrint ตัดสินว่ามาจากนิ้วเดียวกัน [Engelsma2019] (ภาพได้รับอนุญาตจาก Prof. Anil K. Jain, Michigan State University, USA)



ภาพที่ 19 ตัวอย่างภาพลายนิ้วมือที่มาจากคนละนิ้วที่อัลกอริทึม Knowledge-based Method ตัดสินว่ามาจากนิ้วเดียวกัน ในขณะที่ DeepPrint ตัดสินว่าไม่ใช่นิ้วเดียวกัน [Engelsma2019] (ภาพได้รับอนุญาตจาก Prof. Anil K. Jain, Michigan State University, USA)

เมื่อเปรียบเทียบอัลกอริทึมสำหรับการรู้จำลายนิ้วมือแล้ว ทำให้เห็นว่าอัลกอริทึมแนวทางที่ใช้การเรียนรู้ของคอมพิวเตอร์ โดยเฉพาะอัลกอริทึมการเรียนรู้เชิงลึกมีประสิทธิภาพเหนือกว่าอัลกอริทึมแนวทางที่ใช้ความรอบรู้ของมนุษย์ที่พิจารณาเฉพาะการกระจายตัวของมินูเทียร์ 3 ประการ ดังนี้

(1) อัลกอริทึมแนวทางที่ใช้ความรอบรู้ของมนุษย์จะใช้จำนวนมินูเทียร์ ซึ่งในแต่ละภาพมีจำนวนไม่เท่ากัน โดยเกิดจากสภาพผิวหนังและการวางนิ้ว ทำให้เวลาในการคำนวณของแต่ละคู่ภาพไม่เท่ากัน ในขณะที่อัลกอริทึมการเรียนรู้เชิงลึกมีจำนวนลักษณะเฉพาะที่คงที่ ทำให้การคำนวณรวดเร็วกว่ามาก

(2) ความยืดหยุ่นของนิ้วทำให้ตำแหน่งจุดมินูเทียร์มีความคลาดเคลื่อนสูง ซึ่งอาจทำให้ลายนิ้วมือจากนิ้วเดียวกันมีตำแหน่งมินูเทียร์แตกต่างกันมาก และในทางตรงกันข้ามลายนิ้วมือที่มาจากคนละนิ้วอาจมีตำแหน่งมินูเทียร์คล้ายกัน ในขณะที่อัลกอริทึมการเรียนรู้เชิงลึกไม่ได้พิจารณาจากตำแหน่งมินูเทียร์เพียงอย่างเดียว แต่ใช้ลักษณะเฉพาะองค์ประกอบ (Texture Feature) ร่วมกันด้วย ทำให้สามารถรักษาความเหมือนของลายนิ้วมือจากนิ้วเดียวกัน และจำแนกความแตกต่างระหว่างลายนิ้วมือจากนิ้วคนละนิ้วได้ ดังตัวอย่างในภาพที่ 18 และ 19

(3) ในบริเวณลายนิ้วมือคุณภาพต่ำ อาจทำให้เกิดจุดมินูเทียร์ปลอม (Spurious) หรือไม่สามารถตรวจจับจุดมินูเทียร์ได้ (Missing) ซึ่งความผิดพลาดเหล่านี้ส่งผลกระทบต่อการพิจารณาความเหมือนของการกระจายตัวมินูเทียร์ ในขณะที่อัลกอริทึมการเรียนรู้เชิงลึกสามารถทนต่อบริเวณลายนิ้วมือคุณภาพต่ำได้ ดังตัวอย่างในภาพที่ 18

อย่างไรก็ตาม ผลจากการวิจัยยังพบว่า ความแม่นยำของอัลกอริทึมที่ใช้ความรอบรู้ของมนุษย์ ยังเหนือกว่าอัลกอริทึมที่ใช้การเรียนรู้ของคอมพิวเตอร์อยู่ [Engelsma2019] แต่ในอนาคตอันใกล้จากความสำเร็จของอัลกอริทึมการเรียนรู้เชิงลึกดังกล่าว อาจทำให้อัลกอริทึมที่มุ่งเน้นไปที่การพัฒนาอัลกอริทึมที่ใช้การเรียนรู้ของคอมพิวเตอร์ เหนือกว่าอัลกอริทึมที่ใช้ความรอบรู้ของมนุษย์ได้ในที่สุด

อัลกอริทึมเปิดเผยชุดคำสั่ง (Open Source Algorithms)

อัลกอริทึมที่เปิดเผยชุดคำสั่ง (Open Source Code) สำหรับการรู้จำลายนิ้วมือให้บุคคลทั่วไปดาวน์โหลดและนำไปใช้งานได้มีดังตารางที่ 2

ตารางที่ 2 รายชื่ออัลกอริทึมที่เปิดเผยชุดคำสั่งสำหรับการรู้จำลายนิ้วมือ

รูปแบบการทำงานของอัลกอริทึม	ชื่ออัลกอริทึม [Ref]	แหล่งดาวน์โหลด
การประเมินคุณภาพลายนิ้วมือ (Fingerprint Quality Assessment)	**NFIQ2** [Tabassi2021]	https://www.nist.gov/services-resources /software/nfiq-2
การสกัดลักษณะเฉพาะลายนิ้วมือ (Fingerprint Feature Extraction)	**FingerNet** [Tang2017]	https://github.com/592692070/FingerNet
	MinutiaeNet [Nguyen2018]	https://github.com/luannd/MinutiaeNet
การเปรียบเทียบลายนิ้วมือ (Fingerprint Matching)	**Minutia Cylinder-Code** [Cappelli2010]	http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=82&pathSubj=111%7C%7C8%7C%7C82&Req=&
ครบวงจร (End-to-End)	**FPRFramework** [Medina-Pérez2014]	https://sites.google.com/site/miguelmedinaperez/software/fprframework
	Source AFIS	https://sourceafis.machinezoo.com
	MSU-LatentAFIS [Cao2019]	https://github.com/prip-lab/MSU-LatentAFIS

1.2.3. การนำเทคโนโลยีการรู้จำลายนิ้วมือไปประยุกต์ใช้งาน

เทคโนโลยีการรู้จำลายนิ้วมือถูกนำไปประยุกต์ใช้งานในรูปแบบต่าง ๆ อย่างแพร่หลายเป็นเวลานานแล้ว ตั้งแต่การบังคับใช้ตามกฎหมาย การควบคุมการข้ามแดน ไปจนถึงการเข้าใช้งานคอมพิวเตอร์ส่วนบุคคล มีตัวอย่างดังต่อไปนี้

1) การควบคุมการเข้าถึง (Access Control)

การประยุกต์ใช้การรู้จำลายนิ้วมือในการควบคุมการเข้าถึง มีใช้อย่างแพร่หลาย มีตัวอย่างดังนี้

- สวนสนุกดิสนีย์ที่มีการเก็บลายนิ้วมือลูกค้าผู้ซื้อตั๋วรายปี (Annual Pass) ซึ่งสามารถเข้าได้ไม่จำกัดครั้งในระยะเวลาหนึ่งปี โดยการเข้าสวนสนุกต้องตรวจบัตรและสแกนลายนิ้วมือ เพื่อป้องกันการให้ผู้อื่นยืมตั๋วรายปีไปใช้
- ตู้เอทีเอ็มในประเทศบราซิลมีการใช้ลายนิ้วมือแทนการใช้รหัสยืนยันตัวบุคคล (Personal Identification Number (PIN))
- การใช้ลายนิ้วมือเพื่อการยืนยันตัวบุคคลก่อนการเข้าถึงหรือใช้คอมพิวเตอร์ส่วนบุคคล

2) การยืนยันตัวบุคคล (Identity Verification)

การประยุกต์ใช้การรู้จำลายนิ้วมือในการยืนยันตัวบุคคล โดยใช้กับบัตรประจำตัวประชาชน หรือ หนังสือเดินทาง มีใช้อย่างแพร่หลายมานานแล้ว มีตัวอย่างดังนี้

- ระบบ “Aadhaar” ในประเทศอินเดียมีการใช้เลขระบุตัวบุคคลจำนวน 12 หลักร่วมกับการจัดเก็บข้อมูลไบโอเมตริกของบุคคล คือ ลายนิ้วมือทั้ง 10 นิ้ว ม่านตาทั้งสองข้าง และใบหน้า เพื่อให้มั่นใจว่าบุคคลแต่ละคนมีเลขระบุตัวบุคคลเพียง 1 เลข [Aadhaar2020][6]
- ประเทศสหรัฐอเมริกาได้มีโครงการ US-VISIT ซึ่งจะเก็บลายนิ้วมือทั้งสิบนิ้วและใบหน้าของชาวต่างชาติเพื่อทำ VISA เข้าประเทศสหรัฐอเมริกา โดยเริ่มตั้งแต่ปี พ.ศ. 2547 (ค.ศ. 2004) โครงการนี้มีเป้าหมายเพื่อใช้ในการคัดกรองผู้เข้าประเทศ รวมทั้งระบุตัวบุคคลต้องสงสัยและตรวจจับการปลอมแปลงวีซ่าเพื่อเพิ่มการรักษาความปลอดภัยในกระบวนการข้ามแดน
- ในหนังสือเดินทางอิเล็กทรอนิกส์ของหลายประเทศรวมทั้งประเทศไทย ได้มีการใส่ข้อมูลลายนิ้วมือเข้าไปเพื่อให้ความสะดวกในการเข้าหรือออกประเทศในสนามบินนานาชาติผ่าน Auto Gate

3) การรักษาความปลอดภัยและนิติวิทยาศาสตร์ (Security and Forensic)

การประยุกต์ใช้การรู้จำลายนิ้วมือในการรักษาความปลอดภัยและนิติวิทยาศาสตร์ มีการใช้งานมาอย่างยาวนาน มีตัวอย่างดังต่อไปนี้

- FBI ได้เริ่มตั้งหน่วยงาน Fingerprint Identification Division ตั้งแต่ปี พ.ศ. 2467 (ค.ศ. 1924) ติดตั้งระบบ Automatic Fingerprint Identification System (AFIS) ตั้งแต่ปี พ.ศ. 2513 (ค.ศ. 1970) เพื่อเก็บลายนิ้วมือ

[6] https://uidai.gov.in/images/AADHAR_AR_2019_20_ENG_approved.pdf

ของอาชญากรและติดตามประวัติอาชญากรรม เนื่องจากผู้กระทำผิดมีโอกาสกระทำผิดซ้ำ ปัจจุบันเปลี่ยนเป็น Next Generation Identification program (NGI) ซึ่งรวมการรู้จำใบหน้า รอยสัก รอยแผลเป็น เพิ่มเข้าไปด้วย

- หน่วยงานตำรวจทั่วโลก ได้มีระบบ AFIS ไว้ใช้งานในกรณีเดียวกับ FBI ในการทำงานทางด้านนิติวิทยาศาสตร์และตรวจสอบผู้กระทำผิดซึ่งมีโอกาสกระทำผิดซ้ำ

1.2.4. จุดเด่นของการรู้จำลายนิ้วมือ

การใช้ลายนิ้วมือในการยืนยันตัวบุคคลหรือระบุตัวบุคคล มีจุดเด่นและจุดด้อย ดังต่อไปนี้

จุดเด่นของการใช้ลายนิ้วมือ

1) ระบบการรู้จำลายนิ้วมือมีราคาถูก
2) ลายนิ้วมือของแต่ละบุคคลมีความเป็นเอกลักษณ์และไม่เปลี่ยนแปลงตามกาลเวลา (เมื่อบุคคลเจริญเติบโตเต็มที่แล้ว)
3) ลายนิ้วมือทั้ง 10 นิ้วของแต่ละบุคคลยากที่จะเหมือนกับทั้ง 10 นิ้วของอีกบุคคล ซึ่งยังไม่เคยมีการค้นพบว่าบุคคลสองคนที่มีลายนิ้วมือทั้งสิบเหมือนกัน
4) ลายนิ้วมือของฝาแฝดไม่เหมือนกัน ในขณะที่ใบหน้า หรือรหัสพันธุกรรม ของฝาแฝดร่วมไข่จะเหมือนกัน
5) เป็นมิตรกับผู้ใช้ (User Friendly) โดยผู้ใช้ไม่รู้สึกฝืนหรือได้รับความลำบากในการใช้งาน

จุดด้อยของการใช้ลายนิ้วมือ

1) ประสิทธิภาพของระบบอาจลดลงจากสภาพผิวหนัง เช่น ผิวแห้ง เปียก หรือ ลอก เป็นต้น
2) ลายนิ้วมือถูกทำลายได้ง่าย เช่น การผ่าตัด การแช่น้ำกรดอ่อน เป็นต้น
3) การปลอมแปลงลายนิ้วมือสามารถทำได้ง่าย เช่น การใช้กาวไม้ ซิลิโคน หรือ เจลาติน ในการสร้างลายนิ้วมือปลอม เป็นต้น

1.2.5. ข้อจำกัดหรืออุปสรรคของการใช้งานการรู้จำลายนิ้วมือ

การรู้จำลายนิ้วมือมีข้อจำกัดในการใช้งาน หรืออุปสรรค ที่ทำให้ไม่สามารถรู้จำตัวบุคคลจากลายนิ้วมือได้ 3 ประการ คือ

1) **ความเปลี่ยนแปลงของลายนิ้วมือจากเด็กเป็นผู้ใหญ่ (Growth Condition)** โดยลายนิ้วมือของบุคคลจะเปลี่ยนแปลงในเชิงของขนาด (Scale) ซึ่งเกิดจากขนาดนิ้วที่โตและขยายขึ้นตามวัย ดังภาพที่ 20 โดยการขยายของนิ้วนี้ทำให้ระยะห่างระหว่างเส้นลายนิ้วมือ และตำแหน่งจุดมินูเทียร์เลื่อน ส่งผลให้คะแนนความเหมือนของลายนิ้วมือจากนิ้วเดียวกันลดลง ซึ่งในกรณีนี้อัลกอริทึมส่วนใหญ่จะเปิดช่องทางในการปรับค่าเพื่อรองรับการขยายของลายนิ้วมือไว้ เช่น การเปรียบเทียบลายนิ้วมือทั่วไปจะตั้งเงื่อนไขการจับคู่จากค่าระยะทางของมินูเทียร์ไว้ที่ 10 จุดภาพ (Pixel) แต่ถ้าเปรียบเทียบลายนิ้วมือที่ต้องพิจารณาปัจจัยการเจริญเติบโตด้วยอาจเปลี่ยนเป็น 20 จุดภาพ เป็นต้น

ก) ลายนิ้วมือที่เก็บตอนอายุ 11 ปี ข) ลายนิ้วมือที่เก็บตอนอายุ 21 ปี

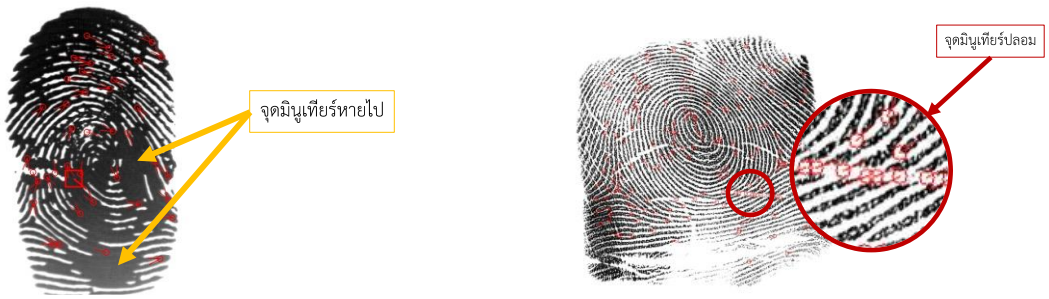
ภาพที่ 20 ภาพลายนิ้วมือ 2 ภาพที่มาจากนิ้วเดียวกันที่รายละเอียด 500 dpi แต่เก็บในช่วงอายุต่างกัน [Yoon2015]

2) **ความเปลี่ยนแปลงที่เกิดจากสภาพผิว (Skin Condition)** สภาพผิวหนังของลายนิ้วมืออาจเปลี่ยนตามสภาพแวดล้อม หรือ การใช้งาน เช่น ผิวแห้ง ที่มักเกิดในพื้นที่อากาศหนาวหรือบุคคลสูงวัย โดยลายนิ้วมือจะจางและขาดเป็นบางส่วน ดังแสดงในภาพที่ 21 (ก) หรือมีรอยย่นคล้ายรอยขนแมว (Scratch) ดังภาพที่ 21 (ข) หรือมีรอยพับ ดังภาพที่ 21 (ค) เป็นต้น ในขณะที่ผิวเปียก จะทำให้เส้นลายนิ้วมือติดกัน ดังภาพที่ 21 (ง) ซึ่งสภาพลายนิ้วมือเหล่านี้ทำให้เกิดจุดมินูเทียร์ปลอม หรือจุดมินูเทียร์หายไปในบริเวณที่เป็นปัญหา ดังภาพที่ 22 โดยในทางปฏิบัติหากพบกรณีนี้จะให้เก็บลายนิ้วมือใหม่ ซึ่งสามารถใช้ครีมบำรุงผิวเพื่อเพิ่มความชุ่มชื้นให้ผิว หรือให้เช็ดมือให้แห้งก่อนทำการเก็บลายนิ้วมืออีกครั้ง หรืออาจใช้เซนเซอร์ลายนิ้วมือแบบ Optical Coherence Tomography (OCT) ที่จะเก็บลายนิ้วมือด้วยการสแกนผิวหนังชั้นในซึ่งจะไม่ได้รับผลกระทบจากสภาพผิวหนังชั้นนอก [Darlow2015], [Auksorius2020] ดังภาพที่ 23

ก) ผิวแห้ง ข) รอยย่นคล้ายขนแมว ค) รอยพับ ง) ผิวเปียก

ภาพที่ 21 ปัญหาลายนิ้วมือที่เกิดจากสภาพผิว

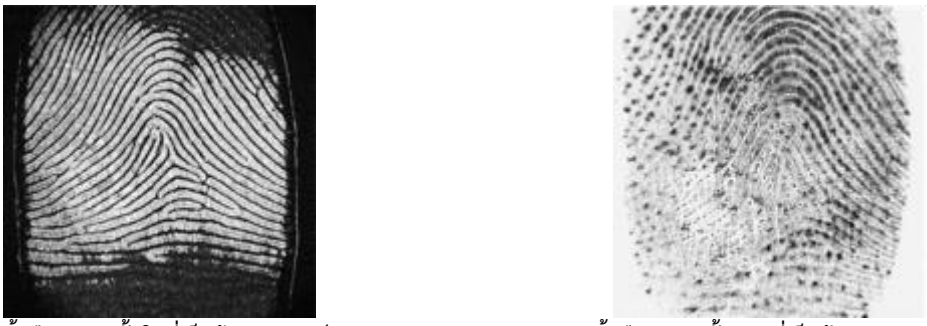
(ภาพจากฐานข้อมูลมาตรฐาน FVC2000 [Maio2002a], FVC2002 [Maio2002b], FVC2004 [Maio2004])



ก) จุดมินูเทียร์หายไปในบริเวณผิวเปียก ข) จุดมินูเทียร์ปลอมในบริเวณรอยพับ

ภาพที่ 22 ความผิดพลาดของการตรวจจับจุดมินูเทียร์ในลายนิ้วมือที่มีปัญหาจากสภาพผิว

(ภาพจากฐานข้อมูลมาตรฐาน FVC2004 [Maio2004] และ NIST4 [Watson1992])

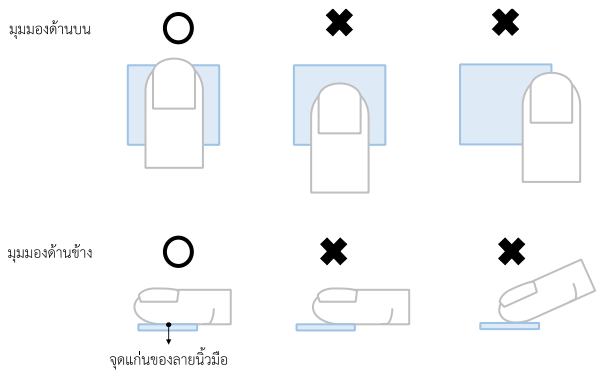


ก) ลายนิ้วมือจากผิวชั้นในที่เก็บด้วยเซนเซอร์ OCT ข) ลายนิ้วมือจากผิวชั้นนอกที่เก็บด้วยเซนเซอร์แสงปกติ

ภาพที่ 23 ภาพลายนิ้วมือที่เก็บด้วยเซนเซอร์ OCT [Darlow2015] และเซนเซอร์แสงปกติ (ภาพจาก [Auksorius2020])

3) **ความเปลี่ยนแปลงที่เกิดจากการวางนิ้วไม่เหมาะสม (Impression Condition)** การวางนิ้วมืออย่างไม่เหมาะสมบนเซนเซอร์เก็บลายนิ้วมือทำให้เกิดปัญหา 2 ประการ คือ ปัญหาลายนิ้วมือปรากฏบางส่วน (Partial) และปัญหาลายนิ้วมือบิดเบี้ยวผิดรูป (Deformation) ซึ่งการวางนิ้วมือบนเซนเซอร์ที่เหมาะสมจะต้องวางจุดแก่นหรือบริเวณกลางนิ้วให้อยู่ตรงกลางเซนเซอร์ในแนวราบไม่ยกข้อมือขึ้น ดังภาพที่ 24 โดยปัญหาลายนิ้วมือ

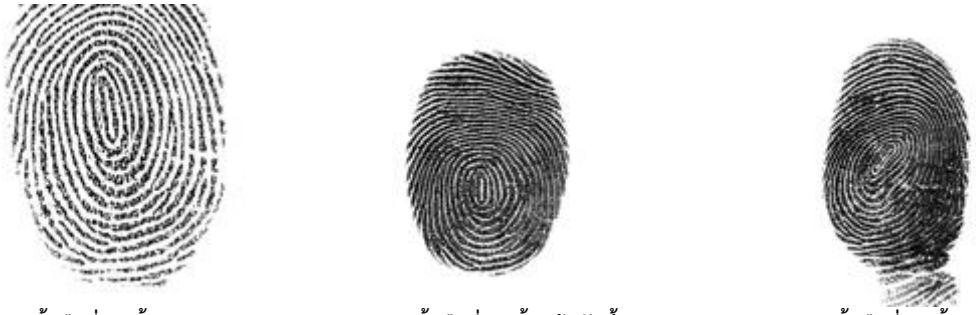
ปรากฏบางส่วนเกิดจากการวางนิ้วไม่เต็มบนเซนเซอร์ ดังภาพที่ 25 ซึ่งทำให้มีพื้นที่ในการเปรียบเทียบน้อย ส่งผลให้คะแนนความเหมือนลดลง ในทางปฏิบัติจะมีการตรวจวัดขนาดพื้นที่ของลายนิ้วมือที่ปรากฏบนภาพว่ามีขนาดพื้นที่เพียงพอต่อการรู้จำหรือไม่ หากไม่เพียงพอจะต้องทำการเก็บลายนิ้วมือใหม่ ในขณะที่ปัญหาลายนิ้วมือบิดเบี้ยวผิดรูปเกิดจากการวางนิ้วแล้วดันหรือบิดไปในทิศทางต่าง ๆ ดังภาพที่ 26 ทำให้ทิศทางลายนิ้วมือและตำแหน่งมินูเทียร์เลื่อน ส่งผลให้คะแนนความเหมือนลดลง ในทางปฏิบัติอาจใช้เซนเซอร์สำหรับตรวจจับแรงกด หากแรงกดมากเกินกำหนดจะต้องทำการเก็บลายนิ้วมือใหม่ หรืออาจใช้อัลกอริทึมเฉพาะทางที่รองรับลายนิ้วมือแบบบิดเบี้ยวได้



ภาพที่ 24 การวางนิ้วมือบนเซนเซอร์อย่างเหมาะสม (O) และไม่เหมาะสม (X)

ก) ลายนิ้วมือปรากฏเต็ม **ข) ลายนิ้วมือปรากฏบางส่วน**

ภาพที่ 25 ตัวอย่างปัญหาลายนิ้วมือปรากฏบางส่วน [28]
(ภาพจากฐานข้อมูลมาตรฐาน FVC2004 [Maio2004])



ก) ลายนิ้วมือที่วางนิ้วปกติ **ข) ลายนิ้วมือที่วางนิ้วแล้วดันขึ้น** **ค) ลายนิ้วมือที่วางนิ้วแล้วบิด**

ภาพที่ 26 ตัวอย่างปัญหาลายนิ้วมือบิดเบี้ยวผิดรูป (ภาพจากฐานข้อมูลลายนิ้วมือของ ม.เกษตรศาสตร์)

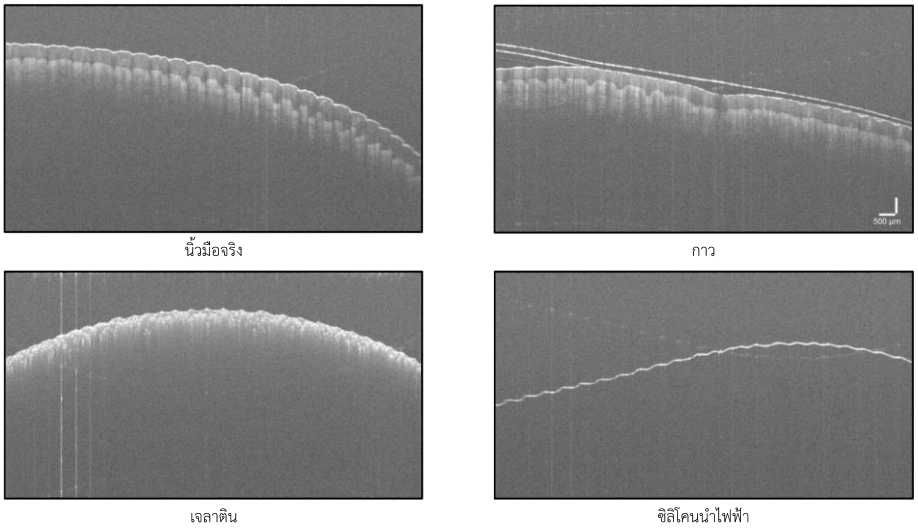
1.2.6. ความเสี่ยงและข้อควรระวังการใช้งานการรู้จำลายนิ้วมือ

การโจมตีระบบการรู้จำลายนิ้วมือสามารถแบ่งออกได้เป็น 2 ประเภท คือ การสวมสิทธิ์โดยการปลอมลายนิ้วมือเป็นบุคคลอื่น (Fingerprint Spoofing) และการเปลี่ยนแปลงลายนิ้วมือ หรือ ทำลายลายนิ้วมือเพื่อหลบเลี่ยงการตรวจสอบตัวตน (Fingerprint Alteration)

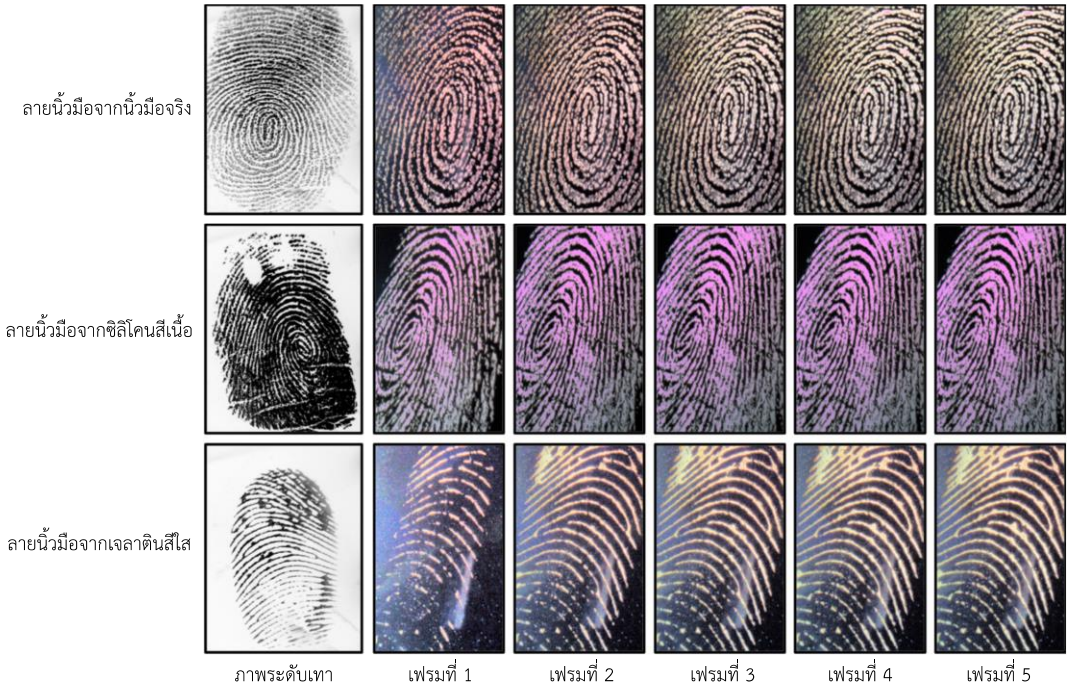
การปลอมลายนิ้วมือเป็นบุคคลอื่น สามารถทำได้โดยการสร้างพิมพ์ลายนิ้วมือจากวัสดุต่าง ๆ เช่น เจลาติน ซิลิโคน ยาง กาวไม้ เพื่อใช้กับเซนเซอร์ประเภทที่ใช้แสงในการเก็บภาพลายนิ้วมือ (Optical Sensor) หรือวัสดุที่สามารถนำไฟฟ้าได้ เช่น ทอง และหมึกที่ผสมสารนำไฟฟ้า เพื่อใช้กับเซนเซอร์ประเภทที่ใช้ตัวเก็บประจุในการเก็บภาพลายนิ้วมือ (Capacitive Sensor) ดังแสดงในภาพที่ 27

ภาพที่ 27 ตัวอย่างพิมพ์ลายนิ้วมือปลอมและภาพลายนิ้วมือที่สแกนได้จากวัสดุต่าง ๆ [Chugh2020a]
(ภาพจาก [Chugh2020a])

ซึ่งการตรวจจับการโจมตีระบบประเภทนี้สามารถทำได้ 2 วิธี คือการใช้อุปกรณ์เฉพาะในการตรวจจับและการใช้อัลกอริทึมตรวจจับ ในกรณีการใช้อุปกรณ์เฉพาะมักเป็นการเพิ่มอุปกรณ์เสริมเข้าไปในขั้นตอนการเก็บลายนิ้วมือ เช่น การใช้อุปกรณ์ตรวจจับการไหลเวียนของเลือด เป็นต้น หรืออาจเปลี่ยนไปใช้เซนเซอร์แบบ OCT ที่สามารถอ่านลายนิ้วมือด้วยการสแกนผิวหนังชั้นในแทนการใช้เซนเซอร์ปกติที่เก็บลายนิ้วมือจากผิวหนังชั้นนอก ดังภาพที่ 28 โดยนิ้วจริงจะปรากฏเป็นชั้นผิวหนังและเนื้อเยื่อ ในขณะที่พิมพ์ลายนิ้วมือจากกาวจะเห็นเป็นชั้นกาวแยกจากชั้นผิวหนังและเนื้อเยื่อชัดเจน และพิมพ์ลายนิ้วมือจากเจลาตินและซิลิโคนนำไฟฟ้าจะไม่เห็นชั้นผิวหนังและเนื้อเยื่อ สำหรับการใช้อัลกอริทึมตรวจจับจะใช้การจำแนกความแตกต่าง ของลักษณะเฉพาะลายนิ้วมือระหว่างนิ้วจริงและนิ้วปลอมจากภาพ เช่น การพิจารณาสีที่สะท้อนจากผิวหนังจริง กับสีที่สะท้อนจากพิมพ์ลายนิ้วมือปลอมที่ทำจากวัสดุต่าง ๆ จะไม่เหมือนกัน ดังภาพที่ 29 โดยนิ้วจริงจะปรากฏเป็นสีชมพูแดงในเฟรมที่ 1 และเปลี่ยนเป็นสีซีดลงจนใกล้ขาวในเฟรมที่ 5 ซึ่งเกิดจากการกดนิ้วแล้วทำให้เลือดเคลื่อนตัวออกจากบริเวณที่ได้รับแรงกด ในขณะที่วัสดุอื่น ๆ สีจะไม่เปลี่ยน



ภาพที่ 28 ผลการสแกนชั้นผิวหนังและเนื้อเยื่อของนิ้วมือจริงและพิมพ์ลายนิ้วมือปลอมจากวัสดุต่าง ๆ ด้วยเซนเซอร์แบบ OCT [Chugh2019]
(ภาพจาก [Chugh2019])

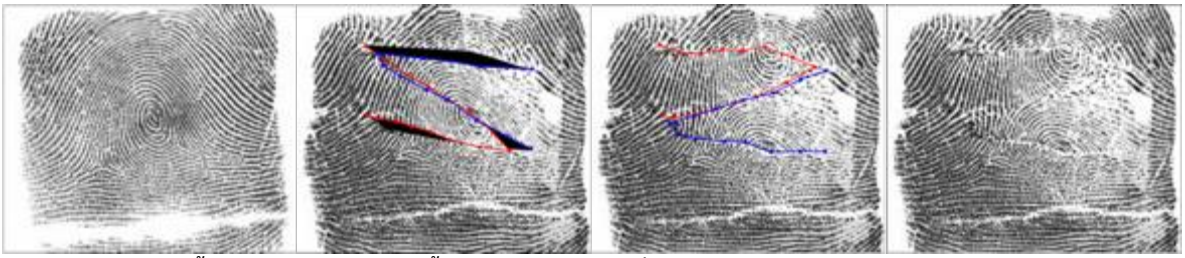


ภาพที่ 29 การจำแนกความแตกต่างของนิ้วจริงและนิ้วปลอมจากการพิจารณาสีที่สะท้อนจากผิวหนัง [Chugh2020b]
(ภาพจาก [Chugh2020b])

การเปลี่ยนแปลงลายนิ้วมือ หรือ ทำลายลายนิ้วมือเพื่อหลบเลี่ยงการตรวจสอบตัวตน มักพบในกรณีของนักโทษหลบหนี โดยการเปลี่ยนแปลงลายนิ้วมือทำให้ปรากฏรอยแผลเป็นบนลายนิ้วมือ ซึ่งสามารถแบ่งออกเป็นแผลเป็นแบบรอยตัด (Cutting Scar) และแผลเป็นแบบหูด (Wart) โดยแผลเป็นแบบรอยตัดอาจเกิดจากของมีคมหรือการศัลยกรรม ดังแสดงในภาพที่ 30 ในขณะที่แผลเป็นแบบหูดที่อาจเกิดจากการใช้กรดกัดผิวหนัง หรือการตัดเฉือนหรือขัดถูผิวหนังบริเวณดังกล่าวออก ดังแสดงในภาพที่ 31 ซึ่งในทางปฏิบัติจะตรวจจับรอยแผลเหล่านี้ เพื่อบ่งชี้ว่าลายนิ้วมือของบุคคลดังกล่าวไม่น่าเชื่อถือและให้ใช้นิ้วอื่น หรือไบโอเมตริกอื่นในการยืนยันตัวบุคคลแทน โดยการตรวจจับจะพิจารณาจากความแตกต่างของทิศทางลายนิ้วมือที่สกัดได้เทียบกับโมเดลทิศทางลายนิ้วมือที่กำหนด ดังแสดงในภาพที่ 32 และความแตกต่างของการกระจายตัวจุดมินูเทียร์ โดยจุดมินูเทียร์จะกระจายตัวห่างจากกันทั่วทั้งนิ้วในกรณีนิ้ว ปกติ ในขณะที่นิ้วที่มีแผลเป็นจุดมินูเทียร์จะกระจุกตัวอย่างหนาแน่นในบริเวณแผลเป็นดังแสดงในภาพที่ 33

ก) ลายนิ้วมือก่อนการศัลยกรรมชนิดมัดหวายปัดขวา

ข) ลายนิ้วมือหลังการศัลยกรรมเปลี่ยนเป็นชนิดโค้งราบ



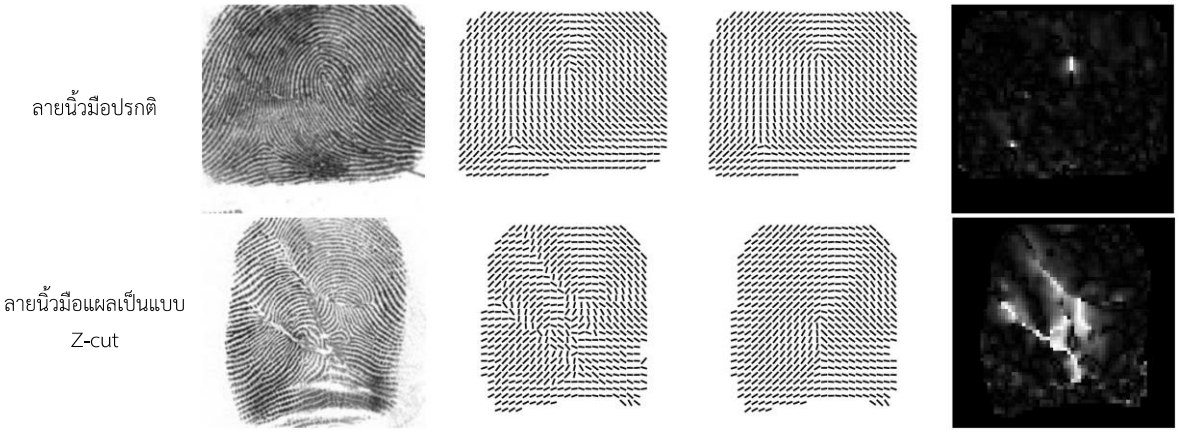
ค) การศัลยกรรมลายนิ้วมือแบบ Z-cut โดยเรียงขั้นตอนจากซ้ายไปขวา เริ่มจากการตัดผิวหนังเป็นตัวอักษร Z แล้วสลับปลายด้านแหลมจากด้านบนมาด้านล่างและด้านล่างขึ้นไปด้านบน แล้วจึงเย็บผิวหนังกลับคืน

ภาพที่ 30 ลายนิ้วมือก่อนและหลังศัลยกรรมที่มีรอบแผลเป็นแบบตัด [Yoon2012a], [Yoon2012b]
(ภาพจาก [Yoon2012a], [Yoon2012b])

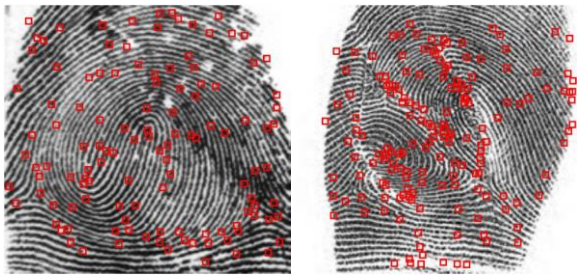
ก) แผลที่เกิดจากการใช้กรดกัดลายนิ้วมือ

ข) แผลที่เกิดจากการพยายามลบลายนิ้วมือด้วยการขัดถูหรือตัดเฉือนผิวออก

ภาพที่ 31 ลายนิ้วมือที่มีรอบแผลเป็นแบบหูด [Watson1992], [Feng2010] (ภาพจาก NIST4 [Watson1992] และ [Feng2010])



ภาพที่ 32 การจำแนกลายนิ้วมือปกติและลายนิ้วมือที่ถูกเปลี่ยนแปลงจากการพิจารณาความแตกต่างของทิศทางลายนิ้วมือที่สกัดได้เทียบกับโมเดล โดยความสว่างหมายถึงค่าความแตกต่างมาก [Yoon2012a] (ภาพจาก [Yoon2012a])



ลายนิ้วมือปรกติ ลายนิ้วมือแผลเป็นแบบ Z-cut

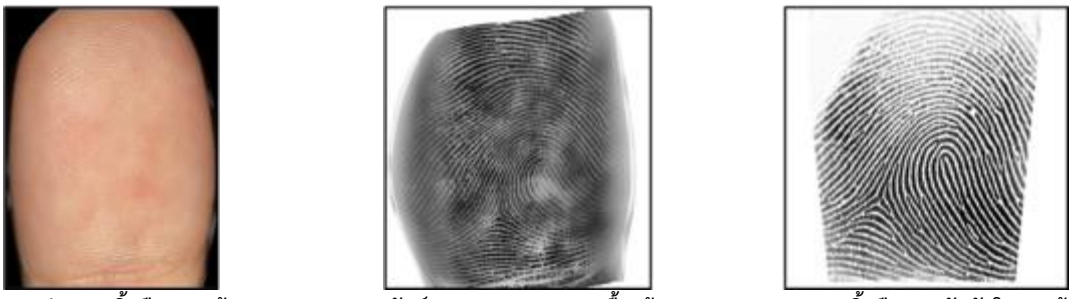
ภาพที่ 33 การกระจายตัวจุดมินูเทียร์ของลายนิ้วมือปกติและลายนิ้วมือที่ถูกเปลี่ยนแปลง [Yoon2012a] (ภาพจาก [Yoon2012a])

1.2.7. แนวโน้มงานวิจัยในปัจจุบันของการรู้จำลายนิ้วมือ

ในปัจจุบันปัญหาลายนิ้วมือที่กำลังได้รับความสนใจแบ่งได้เป็น 4 ประเภท ได้แก่

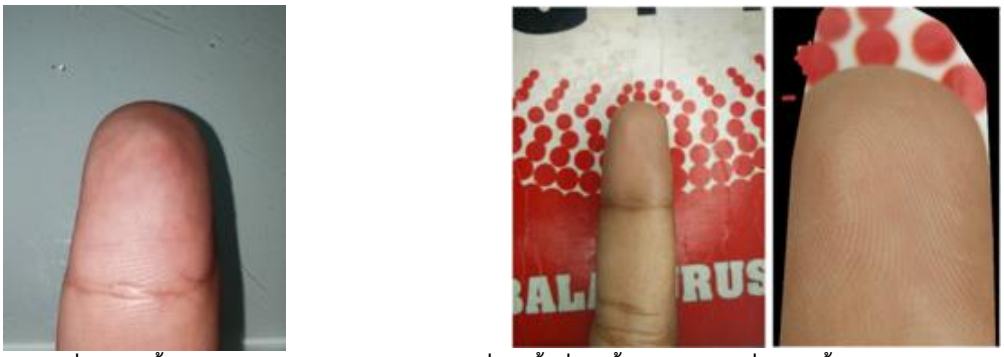
1) **การใช้งานลายนิ้วมือแบบไม่สัมผัสกับเซนเซอร์ (Touchless Fingerprint Recognition)** การเก็บลายนิ้วมือด้วยเซนเซอร์แบบไม่สัมผัสเริ่มได้รับความสนใจตั้งแต่ปี พ.ศ. 2547 (ค.ศ. 2004) [Song2004] แต่ยังไม่ได้ถูกใช้งานอย่างแพร่หลาย จนกระทั่งเกิดการแพร่ระบาดของโรคโควิด-19 ที่ต้องการหลีกเลี่ยงการสัมผัสและรักษาความสะอาด การใช้ลายนิ้วมือแบบไม่สัมผัสจึงกลับมาได้รับความสนใจ โดยงานวิจัยในปัจจุบันได้มีการทดสอบประสิทธิภาพการรู้จำลายนิ้วมือจากภาพลายนิ้วมือที่ถ่ายจากกล้องบนโทรศัพท์มือถือ เปรียบเทียบกับลายนิ้วมือในฐานข้อมูลที่เก็บโดยใช้เซนเซอร์สัมผัส [Priesnitz2021] ซึ่งภาพถ่ายลายนิ้วมือจะต้องถูกประมวลผลเบื้องต้น เพื่อระบุพื้นที่ลายนิ้วมือบนภาพ ปรับขนาดให้สอดคล้องกับมาตรฐาน ISO (500 dpi) และปรับปรุงคุณภาพเพื่อสกัดลักษณะเฉพาะ

ของลายนิ้วมือ โดยประสิทธิภาพของอัลกอริทึมที่ดีที่สุดที่เผยแพร่ในงานวิจัยปัจจุบันมีประสิทธิภาพเทียบเท่าลายนิ้วมือแบบสัมผัส [Grosz2021] ดังแสดงในภาพที่ 34 อย่างไรก็ตามภาพลายนิ้วมือที่ใช้กล้องถ่ายยังได้รับผลกระทบจากสภาพแวดล้อมในการถ่าย เช่น ตำแหน่งนิ้ว ระยะการถ่าย แสง และพื้นหลังที่หลากหลาย ที่อาจทำให้เส้นลายนิ้วมือไม่ชัดเจน หรืออาจทำให้ระบุพื้นที่ลายนิ้วมือผิดพลาด เป็นต้น ดังแสดงในภาพที่ 35 รวมถึงยังไม่มีการตรวจจับการโจมตีระบบด้วยการใช้นิ้วมือปลอมที่นำไปใช้ได้ในทางปฏิบัติ ดังนั้นงานวิจัยปัจจุบันจึงมุ่งเน้นไปที่การลดผลกระทบจากสภาพแวดล้อมในการถ่าย และการตรวจจับการโจมตีระบบ



ก) ภาพถ่ายลายนิ้วมือจากกล้องโทรศัพท์มือถือ ข) ผลลัพธ์จากการประมวลผลเบื้องต้นจากภาพถ่ายลายนิ้วมือ ค) ภาพลายนิ้วมือแบบสัมผัสในฐานข้อมูล

ภาพที่ 34 ภาพถ่ายลายนิ้วมือจากกล้องโทรศัพท์มือถือ ผลลัพธ์จากการประมวลผลเบื้องต้นด้วยอัลกอริทึม [Grosz2021] เปรียบเทียบกับภาพลายนิ้วมือแบบสัมผัสในฐานข้อมูล (ภาพจาก [Grosz2021])



ก) ภาพถ่ายที่เส้นลายนิ้วมือด้านบนปรากฏไม่ชัดเจนเนื่องจากแสงน้อย ข) ภาพถ่ายที่ระบุพื้นที่ลายนิ้วมือผิดพลาดเนื่องจากพื้นหลังมีสีใกล้เคียงกับสีผิวของนิ้วมือ

ภาพที่ 35 ตัวอย่างผลกระทบจากสภาพแวดล้อมในการถ่ายภาพ [Grosz2021] (ภาพจาก [Grosz2021])

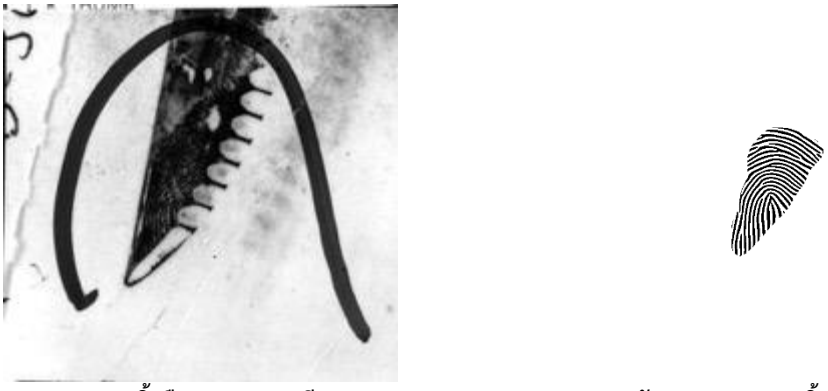
2) **การใช้งานลายนิ้วมือในเด็กทารก (Infant Prints)** ในประเทศกำลังพัฒนาบางประเทศไม่มีการออกเอกสารระบุตัวบุคคลสำหรับเด็กทารก บางครั้งจึงเกิดความผิดพลาดหรือความยากลำบากในการติดตามการให้วัคซีนและยาต่าง ๆ ของเด็กแต่ละคน ในปัจจุบันจึงเริ่มมีการวิจัยการใช้การรู้จำตัวบุคคลด้วยลายนิ้วมือสำหรับเด็กทารกในประเทศอินเดียเพื่อแก้ปัญหาดังกล่าว โดยใช้ภาพลายนิ้วมือที่สแกนด้วยความละเอียดสูง 1,900 dpi ดังแสดงในภาพที่ 36 จากงานวิจัยพบว่าสามารถลงทะเบียนลายนิ้วมือในฐานข้อมูลได้ตั้งแต่อายุ 2-3 เดือน และใช้ลายนิ้วมือนั้นในการยืนยันตัวบุคคลได้ 1 ปี โดยที่ไม่ต้องเก็บภาพลายนิ้วมือเพื่อลงทะเบียนใหม่ ซึ่งมีความถูกต้องอยู่ที่ 85% (เทียบจากฐานข้อมูลทดสอบ) [Engelsma2021]

ภาพที่ 36 ลายนิ้วมือเด็กทารกในช่วงอายุต่าง ๆ ที่ความละเอียด 1,900 dpi [Engelsma2021] (ภาพจาก [Engelsma2021])

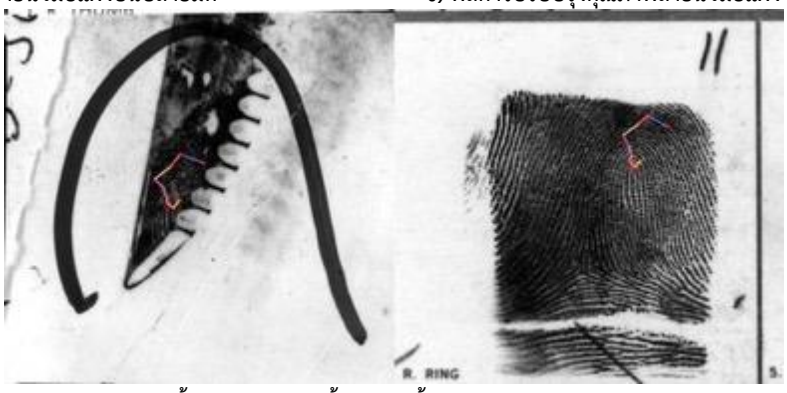
3) **ลายนิ้วมือแฝง (Latent Fingerprint)** ลายนิ้วมือที่แฝงอยู่ในวัสดุ สิ่งของ หรือสถานที่ต่าง ๆ โดยเจ้าของลายนิ้วมือไม่ได้ตั้งใจทิ้งลายนิ้วมือไว้ แบบนี้เรียกว่าลายนิ้วมือแฝง การรู้จำลายนิ้วมือลักษณะนี้มักถูกใช้ในการติดตามจับกุมคนร้าย ซึ่งลายนิ้วมือลักษณะนี้มักมีคุณภาพต่ำ มีพื้นที่ลายนิ้วมือน้อย และอยู่บนพื้นผิวต่าง ๆ ที่ทำให้มองเห็นลายนิ้วมือไม่ชัด ดังแสดงในภาพที่ 37

ก) ลายนิ้วมือแฝงบนเช็ค ข) ลายนิ้วมือแฝงบนธนบัตร

ภาพที่ 37 ลายนิ้วมือแฝงบนพื้นผิวต่าง ๆ [Garris2001] (ภาพจากฐานข้อมูลมาตรฐาน NIST SD27 [Garris2001])



ก) ลายนิ้วมือแฝงบนปลายมีด ข) ผลการปรับปรุงคุณภาพลายนิ้วมือแฝง [Horapong2021]



ค) ผลการเปรียบเทียบลายนิ้วมือแฝงกับลายนิ้วมือจากนิ้วเดียวกันในฐานข้อมูล (ภาพจาก [Garris2001])

ภาพที่ 38 ลายนิ้วมือแฝงจากฐานข้อมูลมาตรฐาน NIST SD27 [Garris2001] และผลการปรับปรุงคุณภาพของอัลกอริทึมที่ดีที่สุดในปัจจุบัน [Horapong2021] และผลการเปรียบเทียบลายนิ้วมือแฝงจากจุดมินูเทียร์ที่ระบุโดยผู้เชี่ยวชาญ

เนื่องจากภาพลายนิ้วมือแฝงมีคุณภาพต่ำมาก ส่งผลให้การสกัดลักษณะเฉพาะจากลายนิ้วมือแฝงแบบอัตโนมัติมีความผิดพลาดสูง และการรู้จำลายนิ้วมือแฝงอัตโนมัติมีประสิทธิภาพต่ำ ในทางปฏิบัติจึงต้องอาศัยผู้เชี่ยวชาญในการช่วยระบุลักษณะเฉพาะบนลายนิ้วมือแฝง ก่อนจะป้อนเข้าระบบรู้จำลายนิ้วมืออัตโนมัติ ซึ่งเป็นขั้นตอนที่ใช้ทรัพยากรสูง ดังนั้น ปัญหาลายนิ้วมือแฝงจึงได้รับความสนใจ ในการพัฒนาอัลกอริทึมที่เกี่ยวข้องต่าง ๆ เพื่อลดภาระงานของผู้เชี่ยวชาญ ซึ่งได้แก่ อัลกอริทึมการปรับปรุงคุณภาพ [Horapong2021] การสกัดลักษณะเฉพาะ [Tang2017] รวมถึงการรู้จำลายนิ้วมือแฝงอัตโนมัติ [Cao2019] ภาพที่ 38 แสดงการปรับปรุงคุณภาพของภาพลายนิ้วมือแฝงโดยเป็นผลงานของคนไทย [Horapong2021]

4) **การตรวจจับลายนิ้วมือปลอม (Presentation Attack Detection)** การตรวจจับการปลอมลายนิ้วมือเป็นบุคคลอื่น มีข้อจำกัดในการตรวจจับจากคุณสมบัติเฉพาะของวัสดุที่นำมาใช้สร้างพิมพ์ลายนิ้วมือปลอม ซึ่งหากมีการใช้วัสดุชนิดใหม่ที่ระบบไม่เคยพบ หรือไม่รองรับการตรวจจับไว้ก่อน จะทำให้ไม่สามารถตรวจจับได้ ในงานวิจัยปัจจุบันจึงได้มีการจำลองความเป็นไปได้ของลักษณะเฉพาะของภาพลายนิ้วมือปลอมจากวัสดุต่าง ๆ แล้วให้คอมพิวเตอร์เรียนรู้และคาดคะเนลักษณะเฉพาะลายนิ้วมือปลอมดังกล่าว เพื่อเพิ่มโอกาสในการตรวจจับลายนิ้วมือปลอมจากวัสดุที่ระบบยังไม่เคยพบมาก่อน [Chugh2020a] ดังแสดงในภาพที่ 39

ลายนิ้วมือปลอมจากวัสดุซิลิโคน ลายนิ้วมือปลอมจากวัสดุยาง

ลายนิ้วมือปลอมจากวัสดุผสมซิลิโคน และยาง ในอัตราส่วน 1:1 ลายนิ้วมือผสมระหว่างซิลิโคนและยางจากการคาดคะเนของคอมพิวเตอร์

ภาพที่ 39 ลายนิ้วมือจากพิมพ์นิ้วปลอมที่ทำด้วยซิลิโคน ยาง และผสมซิลิโคนกับยาง และผลลายนิ้วมือปลอมจากการคาดคะเนของคอมพิวเตอร์ [Chugh2020a] (ภาพจาก [Chugh2020a])

1.3. การรู้จำลายม่านตา (Iris Recognition)

การใช้ลายม่านตาเป็นข้อมูลไบโอเมตริก ได้เริ่มมีการคิดค้นมาตั้งแต่ปี พ.ศ. 2479 (ค.ศ. 1936) โดย Frank Burch ซึ่งเป็นจักษุแพทย์ ที่ได้พยายามระบุความแตกต่างของม่านตามนุษย์และเสนอเป็นรูปแบบการรู้จำตัวบุคคลโดยใช้ลายม่านตา จนกระทั่งต่อมา Leonard Flom และ Aran Safir ได้เสนอแนวคิดของระบบการรู้จำตัวบุคคลด้วยลายม่านตา และได้จดสิทธิบัตรประเทศสหรัฐอเมริกา [Flom1987] ไว้ในปี พ.ศ. 2530 (ค.ศ. 1987) อย่างไรก็ตาม ระบบการรู้จำที่ได้นำเสนอดังกล่าวยังขาดอัลกอริทึม จนกระทั่งในปี พ.ศ. 2535 (ค.ศ. 1992) ศาสตราจารย์ John G. Daugman แห่งมหาวิทยาลัยแคมบริดจ์ ได้พัฒนาอัลกอริทึมระบบการรู้จำลายม่านตา [Daugman1993] ขึ้นมาสำเร็จและจดสิทธิบัตร [Daugman1994] ในปี พ.ศ. 2537 (ค.ศ. 1994) โดยผลงานวิจัยชิ้นนี้ได้แสดงให้เห็นถึงประสิทธิภาพของลักษณะเฉพาะภายในข้อมูลลายม่านตา ซึ่งเป็นจุดเด่นที่สำคัญของไบโอเมตริกชนิดนี้ และสามารถนำมาใช้พิสูจน์ตัวบุคคล (Authentication) ได้อย่างแม่นยำและมีความน่าเชื่อถือสูง

ภายหลังสิทธิบัตรได้หมดอายุ ประกอบกับความรุดหน้าของการพัฒนาทางด้านเทคโนโลยีการประมวลผลภาพด้วยคอมพิวเตอร์ ปัจจุบันจึงมีการผลิตและจำหน่ายระบบการรู้จำลายม่านตาเกิดขึ้นในหลายประเทศ จนทำให้มีการใช้งานระบบการรู้จำลายม่านตาเพื่อพิสูจน์ตัวบุคคลกันอย่างแพร่หลาย และได้รับการยอมรับในการนำมาใช้งานมากขึ้น เช่น การรักษาความปลอดภัยในการเข้าถึงสถานที่ การยืนยันตัวบุคคลก่อนการทำธุรกรรมอิเล็กทรอนิกส์ การผสมผสานร่วมกันกับไบโอเมตริกชนิดอื่นเพื่อป้องกันการปลอมแปลง ในที่นี้ จึงได้รวบรวมรายชื่อบริษัทผู้จัดจำหน่ายระบบการรู้จำลายม่านตาในปัจจุบัน มาแสดงไว้ในตารางที่ 3

ตารางที่ 3 รายชื่อบริษัทผู้จัดจำหน่ายระบบการรู้จำลายม่านตา

ชื่อบริษัท	เว็บไซต์
Aware	https://www.aware.com/
BioID	https://www.bioid.com/
NEC (1st Ranked with FNIR=0.41%*)	https://www.nec.com/
Biometric Intelligence and Identification Technologies	http://www.bi2technologies.com/
HID Global (formerly Crossmatch)	https://www.hidglobal.com/
EyeLock	https://www.eyelock.com/
Gemalto (was acquired by Thales)	http://www.gemalto.com/
Idemia (2nd Ranked with FNIR=0.52%*)	https://www.idemia.com/
Iridian Technologies	http://www.iridiantech.com/
Iris Guard	https://www.irisguard.com/
Iris ID (formerly LG Electronics)	https://www.irisid.com/
IriTech	http://www.iritech.com/
Neurotechnology (3rd Ranked with FNIR=0.53%*)	https://www.neurotechnology.com/verieye.html
Panasonic	https://na.panasonic.com/us/
Tascent	https://tascent.com/
SRI International	https://www.sri.com/hoi/iris-recognition/
Unisys	https://www.unisys.com/

หมายเหตุ * แสดงอันดับของผลการทดสอบ Iris recognition technology benchmark test โดยการระบุตัวบุคคลด้วยการใช้ม่านตาคู่ (both eye) บนฐานข้อมูลม่านตาคู่จำนวน 500K คู่ และแสดงผลความแม่นยำเป็นค่า False Negative Identification Rate (FNIR) ซึ่งจัดโดย U.S. National Institute of Standards and Technology (NIST) [7]

1.3.1. หลักการทำงานของการรู้จำลายม่านตา

ระบบการรู้จำลายม่านตาโดยทั่วไป อาศัยภาพลายม่านตาซึ่งถ่ายจากกล้องและอุปกรณ์จัดแสง เพื่อให้ได้ภาพลายม่านตาที่มีความคมชัด และเห็นข้อมูลของลายม่านตาที่มีความชัดเจนมากที่สุด โดยภาพลายม่านตาที่ได้จะถูกนำไปประมวลผลด้วยอัลกอริทึมภายในคอมพิวเตอร์แม่ข่ายหลัก (Main Server) หรือภายในฮาร์ดแวร์ของเครื่องสแกนม่านตา (Iris Scanner) ซึ่งจะมีการตรวจสอบและประเมินข้อมูลของลายม่านตา เทียบกับฐานข้อมูลที่มีอยู่ในระบบ โดยผลที่ได้จะอยู่ในรูปแบบของคะแนนการจับคู่ (Matching Score) อย่างไรก็ตาม การประยุกต์ใช้ผลคะแนนการจับคู่ที่ได้มาจาก

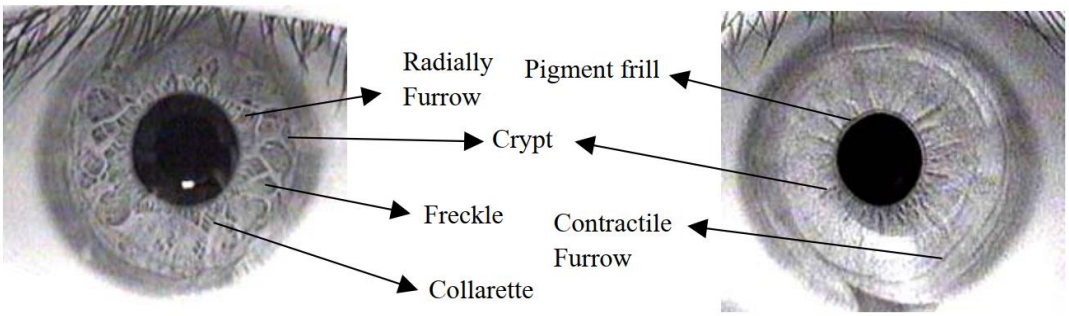
[7] https://pages.nist.gov/IREX10/

ระบบการรู้จำลายม่านตา จะขึ้นอยู่กับลักษณะการนำไปใช้พิสูจน์ตัวบุคคลของแต่ละหน่วยงาน ได้แก่ การใช้งานแบบระบุตัวตน (Identification) หรือการใช้งานแบบยืนยันตัวตน (Verification)

การรู้จำลายม่านตาสามารถทำได้โดยพิจารณาจาก ลักษณะเด่นของรูปแบบลายม่านตา (Iris Pattern) ที่เกิดขึ้นโดยรูปแบบลายม่านตาจะเกิดจากการรวมกันของส่วนประกอบย่อยต่าง ๆ ซึ่งปรากฏอยู่บนชั้นพื้นผิวด้านบนสุด (Anterior Border Layer) ของม่านตา [โหราพงศ์2549] ตามรายละเอียดที่ได้แสดงในตารางที่ 4 นอกจากนี้ ตัวอย่างส่วนประกอบย่อยที่ประกอบกันเป็นลายม่านตาได้แสดงไว้ในภาพที่ 40 ซึ่งเป็นภาพม่านตาจากฐานข้อมูล KSIP DB01R ของห้องปฏิบัติการประมวลสัญญาณและดิจิทัลเกษตรศาสตร์

ตารางที่ 4 สรุปรูปแบบของส่วนประกอบย่อยที่ประกอบกันเป็นลายม่านตา

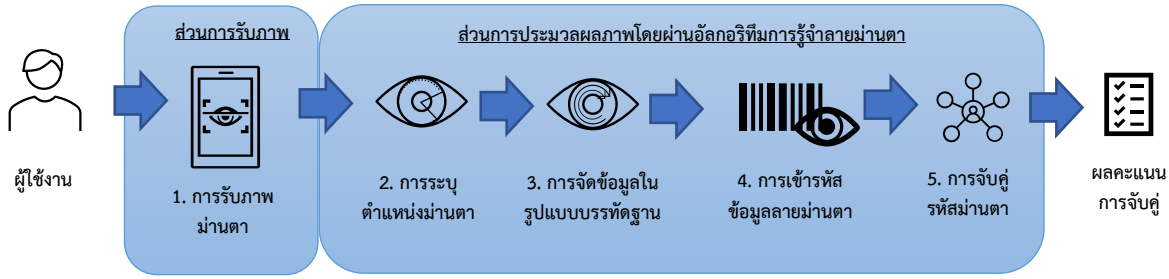
รูปแบบของส่วนประกอบย่อยภายในลายม่านตา	ลักษณะที่พบ	บริเวณที่พบ
Crypt	เส้นในแนวรัศมีรอยแต้ม	ตั้งแต่รูม่านตาจนถึงขอบนอกของม่านตา
Freckles	จุด หรือ รอยแต้ม	พบได้ทั่วไป
Radially furrow	เส้นเล็ก ๆ ในแนวรัศมี	รอบ ๆ รูม่านตาจนถึงรอยต่อของ collarette
Contractile furrow	ร่องในแนวเส้นรอบวง	ใกล้กับขอบนอกของม่านตา
Collarette	เส้นขอบคดเคี้ยวเป็นวงรอบ	รอยต่อระหว่างพื้นที่ส่วนบริเวณรอบรูม่านตากับพื้นที่ส่วนกล้ามเนื้อปรับเลนส์
Pigment frill	เส้นทึบเป็นวงรอบรูม่านตา	บริเวณวงรอบใกล้กับรูม่านตา



ภาพที่ 40 ส่วนประกอบย่อยของรูปแบบลายม่านตา (Iris Pattern) ในตัวอย่างภาพม่านตาจากฐานข้อมูล KSIP DB01R ของห้องปฏิบัติการประมวลสัญญาณและดิจิทัลเกษตรศาสตร์ [โหราพงศ์2549]

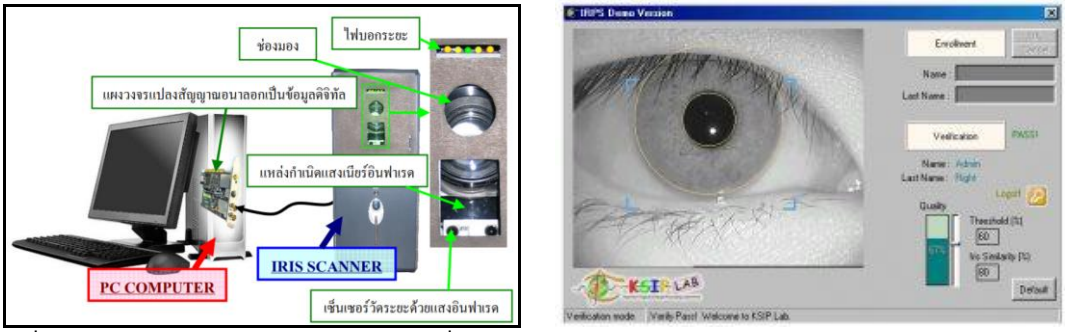
โดยปกติ รูม่านตาจะมีขนาดเส้นผ่านศูนย์กลางเฉลี่ย 1 มม. ถึง 8 มม. (ขึ้นกับการหดขยายตามปริมาณแสงที่ตาได้รับ) และขนาดของม่านตาจะมีขนาดเส้นผ่านศูนย์กลางเฉลี่ย 12 มม. [Wildes1994]

สำหรับหลักการทำงานของการรู้จำลายม่านตามีอยู่ด้วยกัน 2 ส่วน คือ ส่วนการรับภาพ และส่วนการประมวลผลภาพโดยผ่านอัลกอริทึมรู้จำม่านตา โดยถ้าแบ่งอย่างละเอียด สามารถแบ่งออกได้เป็น 5 ขั้นตอน [Ross2010] ตามภาพที่ 41 ซึ่งมีรายละเอียดของแต่ละขั้นตอนดังต่อไปนี้



ภาพที่ 41 แผนภาพ (Block Diagram) การทำงานของระบบการรู้จำลายม่านตา

1) **ส่วนการรับภาพม่านตา (Iris Image Acquisition)** ภายในเครื่องสแกนม่านตา ภาพม่านตาจะถูกถ่ายด้วยกล้องที่สามารถรับแสงอินฟราเรดย่านใกล้ (Near-Infrared, NIR) โดยแสงอินฟราเรดย่านใกล้นั้นเป็นช่วงแสงที่มีความยาวคลื่นสั้นอยู่ระหว่าง 700–900 นาโนเมตร (nm) ซึ่งการถ่ายภาพด้วยเทคนิคนี้สามารถช่วยให้ลายม่านตามีความคมชัดและเห็นข้อมูลลายม่านตาชัดเจน รวมทั้งสามารถลดแสงสะท้อนได้ค่อนข้างดีเมื่อเทียบกับการถ่ายภาพภายใต้ช่วงแสงปกติที่ตามองเห็น (Visible Light) [Wildes1994] ทั้งนี้ ระยะการรับภาพของกล้องโดยส่วนใหญ่จะห่างจากผู้ใช้งานประมาณ 20-40 เซนติเมตร ภาพที่ 42 แสดงถึงตัวอย่างการถ่ายภาพพร้อมอุปกรณ์จัดแสง [โหราพงศ์2549] [ทูลแสงงาม 2549]



ภาพที่ 42 ตัวอย่างการถ่ายภาพพร้อมอุปกรณ์จัดแสงที่ได้มีการนำเสนอโดยห้องปฏิบัติการประมวลสัญญาณและภาพเกษตรศาสตร์ [โหราพงศ์2549] [ทูลแสงงาม 2549]

2) **การระบุตำแหน่งม่านตา (Iris Localization)** ภาพม่านตาที่รับเข้ามาโดยส่วนมากจะไม่ได้เห็นเพียงแค่ลูกตา (Eyeball) แต่จะเห็นทั้งดวงตาหรือแม้กระทั่งเห็นทั้งใบหน้า สำหรับเครื่องสแกนม่านตาของบางบริษัทผู้ผลิตดังนั้น ขั้นตอนการระบุตำแหน่งม่านตาในภาพที่รับเข้ามานั้นจึงมีความจำเป็นอย่างยิ่ง โดยในขั้นตอนนี้ถือเป็นขั้นตอนหนึ่งที่มีความสำคัญต่อผลคะแนนการจับคู่ภาพม่านตา หากมีความผิดพลาดของการหาตำแหน่งม่านตาจะทำให้ผลคะแนนของการจับคู่มีค่าต่ำ และส่งผลให้ปฏิเสธการเข้าใช้งานของผู้ใช้ได้ ทั้งนี้ ปัจจัยของความถูกต้องแม่นยำในขั้นตอนการระบุตำแหน่งม่านตาจะขึ้นกับ 5 ปัจจัยหลัก ดังนี้
   (1) คุณภาพและความคมชัดของภาพที่รับเข้ามา
   (2) ขนาดพื้นที่ม่านตาจากระยะการถ่ายภาพที่ไกลเกินไป
   (3) ปริมาณแสงที่ได้รับมากหรือน้อยเกินไปในระหว่างถ่ายภาพ
   (4) การบดบังดวงตาจากการกระพริบตา
   (5) ความเบลอของดวงตาในภาพจากการกลอกตาหรือกลอกหน้าไปมา
3) **การจัดข้อมูลในรูปแบบบรรทัดฐาน (Iris Normalization)** เนื่องจากม่านตามีลักษณะตามธรรมชาติเป็นพื้นที่รูปวงแหวนโดยที่ส่วนของตาดำจะอยู่เป็นแกนกลาง ซึ่งการหดขยายของม่านตาจะแปรผันตามปริมาณแสงที่ส่องเข้ามายังม่านตาอันเป็นผลให้เกิดการดึงรั้งของกล้ามเนื้อ (Pupillae Muscle) ภายในลูกตาขึ้นและจะส่งผลให้พื้นที่ม่านตาสามารถหดขยายไม่เท่ากันทั้งการหดขยายในแนววงรอบ (Circular) และการหดขยายในแนวรัศมี (Radial) ดังแสดงตามภาพที่ 43 โดยระยะการหดขยายของม่านตาทำให้ขนาดพื้นที่การประมวลผลลายม่านตาเปลี่ยนแปลงไป ดังนั้น จำเป็นต้องจัดข้อมูลลายม่านตาให้อยู่ในรูปแบบบรรทัดฐาน (Normalization) เพื่อเป็นการชดเชยการหดขยายพื้นที่ดังที่ได้กล่าวมานี้ และไม่ทำให้เกิดการลำเอียงของขอบเขตที่จะใช้ในการสร้างรหัสม่านตาและการเปรียบเทียบข้อมูลต่อไป

(ก) การหดขยายในแนววงรอบ (circular) ด้วยกล้ามเนื้อ sphincter pupillae muscle

(ข) การหดขยายในแนวรัศมี (radial) ด้วยกล้ามเนื้อ dilator pupillae muscle

ภาพที่ 43 ระยะการหดขยายของม่านตาทำให้ขนาดพื้นที่การประมวลผลลายม่านตาเปลี่ยนแปลงไป

4) **การเข้ารหัสข้อมูลลายม่านตา (Iris Pattern Encoding)** วิธีการสร้างรหัสเพื่อเป็นตัวแทนข้อมูลลายม่านตา (Data Representation) นั้น อัลกอริทึมจะสกัดลักษณะเด่นที่มีลักษณะเฉพาะของลายม่านตา (Iris Pattern) ออกมาก่อน โดยการออกแบบจะมีเทคนิคด้วยกันหลายประเภท เช่น การใช้โมเดลสกัดลักษณะเฉพาะผ่านตัวกรองที่ได้กำหนดไว้ (Feature Engineering) หรือ การใช้โมเดลการเรียนรู้ด้วยเครื่อง (Machine learning) หลังจากนั้นจะนำลักษณะเฉพาะที่ได้มาทำการเข้ารหัส (เป็นแบบเลขฐานสองหรือเข้ารหัสแบบค่าตัวเลขตามแต่ละเทคนิคที่ใช้งาน) เพื่อใช้เป็นเทมเพลตในการจับคู่กับฐานข้อมูลต่อไป
5) **การจับคู่ข้อมูลลายม่านตา (Iris Pattern Matching)** การทำงานขั้นตอนสุดท้ายของการรู้จำลายม่านตาจะเป็นการเปรียบเทียบข้อมูลกับฐานข้อมูลที่มีอยู่ แล้วจะให้ผลคะแนนการจับคู่ออกมาเป็นค่าตัวเลข ซึ่งค่าตัวเลขที่ได้จะขึ้นอยู่กับการออกแบบวิธีการเปรียบเทียบของอัลกอริทึมชนิดต่าง ๆ ดังนี้
   (1) ค่าคะแนนที่บอกความเหมือนกัน (Similarity Score) ระหว่างคู่รหัสม่านตาแบบจำกัดค่า เช่น 0-1 คะแนน หรือ 0-100 คะแนน
   (2) ค่าคะแนนที่บอกความเหมือนกัน (Similarity Score) ระหว่างคู่รหัสม่านตาแบบไม่จำกัดค่า เช่น เริ่มตั้งแต่ 0 คะแนน เป็นต้นไป
   (3) ค่าคะแนนที่บอกความต่างกัน (Dissimilarity Score) ระหว่างคู่รหัสม่านตาแบบจำกัดค่า เช่น 0-1 คะแนน หรือ 0-100 คะแนน
   (4) ค่าคะแนนที่บอกความต่างกัน (Dissimilarity Score) ระหว่างคู่รหัสม่านตาแบบไม่จำกัดค่า เช่น เริ่มตั้งแต่ 0 คะแนน เป็นต้นไป

1.3.2. อัลกอริทึมการรู้จำลายม่านตา

อัลกอริทึมหลักของระบบการรู้จำลายม่านตา ที่มีการใช้งานอย่างแพร่หลายของบริษัทผู้ผลิตหลาย ๆ แห่ง คือ อัลกอริทึมที่ถูกพัฒนาขึ้นโดย ศาสตราจารย์ John Daugman (Daugman's System) [Daugman1993, 1994, 2004, 2006, 2007] ที่ได้เริ่มนำเสนอไว้ตั้งแต่ปี พ.ศ. 2535 (ค.ศ. 1992) ซึ่งอัลกอริทึมนี้ประสบความสำเร็จเป็นอย่างมาก โดยมีผลยืนยันความแม่นยำจากการทดสอบล่าสุดในปี พ.ศ. 2549 (ค.ศ. 2006) [Daugman2006] ซึ่งมีค่า FNMR ระหว่าง 1.1% ถึง 1.4% ที่ค่า FMR เท่ากับ 0.1% จากการทดสอบโดยกลุ่มตัวอย่าง 316,250 คน (ทำให้ได้จำนวนภาพม่านตาทดสอบเท่ากับ 632,500 ภาพ) ซึ่งกลุ่มตัวอย่างเหล่านี้เป็นบุคคลที่มาจากเชื้อชาติที่แตกต่างกันถึง 152 เชื้อชาติ

1) **อัลกอริทึมการระบุตำแหน่งม่านตา (Iris Localization Algorithm)** การทำงานของอัลกอริทึมการระบุตำแหน่งม่านตา จะทำหน้าที่กำหนดขอบเขตพื้นที่เฉพาะในส่วนที่มีข้อมูลลายม่านตาจากภาพที่รับเข้ามา โดยพื้นที่ของม่านตาจะอยู่ระหว่างรัศมีของส่วนตาดำ (Pupil) และรัศมีของส่วนตาขาว (Sclera) นอกจากนี้ บางอัลกอริทึมจะมีความสามารถเพิ่มเติมในการหลบหลีกขนตา (Eyelash) และ เปลือกตา (Eyelid) รวมทั้งแสงไฟสะท้อนต่าง ๆ ที่มาบดบังพื้นที่ของลายม่านตาได้

   สำหรับการระบุตำแหน่งม่านตา จะนำอัลกอริทึมการตรวจจับขอบเขตและพื้นที่ (Boundary and Region Detection) ต่าง ๆ มาประยุกต์ใช้ โดยการกำหนดขอบเขตของม่านตาจะมีอยู่ด้วยกัน 2 กลุ่ม คือ
   (1) อัลกอริทึมซึ่งกำหนดขอบเขตม่านตาแบบเป็นวงกลม (Circular Boundaries) อัลกอริทึมกลุ่มนี้จะให้ผลลัพธ์ของวงกลมตาดำเป็นขอบเขตภายใน และวงกลมตาขาวเป็นขอบเขตภายนอก ซึ่งหลักการหาขอบเขตจะประกอบด้วย 2 ขั้นตอน คือ ขั้นตอนแรกเป็นการหาขอบของตาดำและตาขาว

(Edge Detection) ขั้นตอนที่สองเป็นการประมาณพารามิเตอร์วงกลมเพื่อใช้แทนขอบเขตของวงกลมตาดำและขอบเขตของวงกลมตาขาว (Circular Parameter Estimation)

ในขั้นตอนแรก ผลงานของศาสตราจารย์ John Daugman ได้นำเสนอการหาผลต่างสูงสุดในแต่ละรัศมีวงกลม ซึ่งตรวจจับขอบการเปลี่ยนแปลงค่าความเข้ม โดยสามารถหารัศมีวงกลมของขอบตาดำหรือรูม่านตา และสามารถหารัศมีวงกลมรอบส่วนตาขาวได้

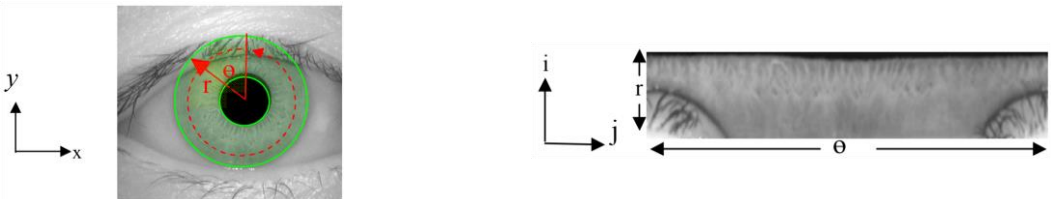
(2) **อัลกอริทึมซึ่งกำหนดขอบเขตม่านตาแบบไม่เป็นวงกลม (Noncircular Boundaries)** ตามสมมติฐานที่ขอบเขตวงกลมตาดำและวงกลมตาขาวอาจจะไม่เป็นวงกลมสมบูรณ์ จึงได้มีผลงานวิจัยออกมาเพิ่มเติมโดยใช้โมเดลของการทำ เส้นรูปร่างไวงาน (Active Contour) ซึ่งมีรายละเอียดผลงานวิจัยตีพิมพ์ใน [Daugman2007] ทำให้การประมาณขอบเขตม่านตามีรูปร่างเป็นเส้นรอบรูปตามค่าสีที่เปลี่ยนแปลงจริงรอบขอบเขตตาดำและตาขาว

ผลลัพธ์ที่ได้จากขั้นตอนการระบุตำแหน่งม่านตาจะเป็นหน้ากาก (Binary Mask) ของตำแหน่งม่านตา ซึ่งหน้ากากที่ได้นี้จะนำไปใช้กำหนดขอบเขตพื้นที่ในการสกัดลักษณะเด่นของขั้นตอนเข้ารหัสข้อมูลลายม่านตา และใช้กำหนดขอบเขตพื้นที่ในการเปรียบเทียบข้อมูลของขั้นตอนการจับคู่รหัสม่านตา

2) **อัลกอริทึมการจัดข้อมูลในรูปแบบบรรทัดฐาน (Iris Normalization Algorithm)** การชดเชยการหดขยายพื้นที่จะกระทำให้อยู่ในรูปแบบบรรทัดฐานที่มีขนาดพื้นที่ม่านตาเป็นค่าคงที่เท่ากันสำหรับทุกม่านตา โดยเป็นการนำโมเดลแผ่นยางยืดที่เป็นเนื้อเดียวกัน (Homogeneous Rubber Sheet Model) ซึ่งนำเสนอโดยศาสตราจารย์ John Daugman [Daugman2004] มาประยุกต์ใช้ โดยมีสมมติฐานของการหดขยายของม่านตาเป็นแบบเชิงเส้นในแนวรัศมี เพื่อฉาย (mapping) ให้อยู่ในรูปแบบบรรทัดฐาน ดังแสดงวิธีการฉายตามภาพที่ 44

ภาพที่ 44 การจัดข้อมูลให้อยู่ในรูปแบบบรรทัดฐาน (Normalization) ด้วยโมเดลแผ่นยางยืดที่เป็นเนื้อเดียวกัน

อย่างไรก็ตาม การทำงานของขั้นตอนนี้จะสัมพันธ์อย่างมากกับวิธีการสกัดลักษณะเฉพาะ (Feature Extraction) ที่อยู่ในขั้นตอนของการเข้ารหัสข้อมูลลายม่านตา (ซึ่งเป็นขั้นตอนถัดไป) กล่าวคือ หากวิธีการสกัดลักษณะเด่นได้เลือกใช้ตัวกระทำแบบพิกัดเชิงขั้ว (Polar-based Operator) เช่น วิธีการของศาสตราจารย์ John Daugman [Daugman1993, 1994, 2004, 2006, 2007] ผลลัพธ์ของการทำงานนี้จะถูกยกไปรวมกันกับขั้นตอนของการเข้ารหัสข้อมูลลายม่านตา แต่ทว่า หากวิธีการสกัดลักษณะเด่นได้เลือกใช้ตัวกระทำแบบพิกัดคาร์ทีเชียน (Cartesian-based operator) การทำงานในขั้นตอนนี้จะต้องคลี่ข้อมูลลายม่านตาโดยแปลงออกมาอยู่บนพิกัดคาร์ทีเชียนในรูปแบบบรรทัดฐาน ดังตัวอย่างที่แสดงไว้ในภาพที่ 45



(ก) ข้อมูลแบบพิกัดเชิงขั้วบนภาพลายม่านตา (ข) จัดข้อมูลบนพิกัดคาร์ทีเชียนให้อยู่ในรูปแบบบรรทัดฐาน

ภาพที่ 45 ลายม่านตาซึ่งถูกจัดให้อยู่ในรูปแบบบรรทัดฐาน (Normalization) บนพิกัดคาร์ทีเชียน [12]

3) **อัลกอริทึมการเข้ารหัสข้อมูลลายม่านตา (Iris Pattern Encoding Algorithm)** ขั้นตอนนี้จะเริ่มจากการสกัดลักษณะเด่น เพื่อนำเฉพาะข้อมูลที่สามารถใช้งานได้ ในการเปรียบเทียบออกมาจากภาพลายม่านตา ซึ่งมีเทคนิคการใช้โมเดลของตัวกรองที่ได้กำหนดไว้ (Feature Engineering) อยู่ด้วยกันหลายวิธี เช่น การใช้ตัวกรองกาเบอร์เวฟเล็ต 2 มิติ (2D Gabor Wavelets) [Daugman1993, 1994, 2004, 2006, 2007] การใช้ชุดตัวกรองที่สร้างจากการวิเคราะห์องค์ประกอบอิสระ (Independent Component Analysis (PCA)) ของภาพม่านตาด้วยวิธี Binarized Statistical Image Features (BSIF) [Raja2014] หรือการแปลงเวฟเล็ตแบบ Haar (Haar Wavelet Analysis) [Krichen2005]

นอกจากนี้เทคนิคการใช้โมเดลการเรียนรู้ด้วยเครื่อง (Machine Learning) เพื่อใช้โครงข่ายประสาทเทียมที่ได้เรียนรู้แล้วนำมาสกัดลักษณะเด่นของข้อมูลลายม่านตา เช่น โครงข่าย DeepIrisNet ซึ่งใช้โครงข่ายประสาทแบบคอนโวลูชัน (Convolutional Neural Network, CNN) [Gangwar2016] หรือ การประยุกต์โครงข่ายประสาท CNN ที่มีชื่อว่า Densely Connected Convolutional Networks (DenseNet) [Hafner2021]

จะเห็นได้ว่าแนวโน้มการตีพิมพ์ผลงานวิจัย จะเน้นการนำเสนออัลกอริทึมต่าง ๆ เพื่อเสนอวิธีการสกัดลักษณะเด่นของข้อมูลลายม่านตาให้มีประสิทธิภาพมากที่สุด ซึ่งผู้ผลิตระบบการรู้จำลายม่านตาสามารถนำเทคนิคและวิธีการใหม่ ๆ เข้ามาปรับปรุงผลิตภัณฑ์ระบบการรู้จำลายม่านตาได้ต่อไป

เมื่ออัลกอริทึมได้ลักษณะเด่นของลายม่านตาออกมา จะทำการเอาข้อมูลเฉพาะที่เป็นตัวเลขมาเข้ารหัสให้อยู่ในรูปแบบไบนารี่ที่มีขนาดความยาวคงที่ (Fixed-length Binary Code) โดยการใช้รหัสแบบไบนารี่นั้นมีข้อดีที่ได้เปรียบมากกว่าการใช้รหัสแบบค่าตัวเลข (Numerical Code) ดังนี้ คือ

(1) การเปรียบเทียบแบบไบนารี่ด้วยคอมพิวเตอร์มีการคำนวณที่ซับซ้อนน้อยกว่า ทำให้มีความรวดเร็วในการประมวลผล

(2) การเก็บข้อมูลแบบไบนารี่จะประหยัดพื้นที่จัดเก็บข้อมูลในหน่วยความจำมากกว่า ทำให้สามารถใช้กับฮาร์ดแวร์ต่าง ๆ ได้หลากหลาย

(3) การถ่ายโอนข้อมูลแบบไบนารี่มีความรวดเร็ว

4) **อัลกอริทึมการจับคู่ข้อมูลลายม่านตา (Iris Pattern Matching Algorithm)** การเปรียบเทียบข้อมูลลายม่านตาจะขึ้นอยู่กับผลลัพธ์ที่ออกแบบของค่าลักษณะเด่น ที่สกัดได้จากขั้นตอนการเข้ารหัสข้อมูลลายม่านตา โดยการออกแบบอัลกอริทึมจะต้องทำควบคู่กันไปแล้วแต่กรณี

(1) กรณีที่วัดความต่างกันของรหัสม่านตาแบบไบนารี โดยส่วนมากจะใช้วิธีการวัดระยะทางแฮมมิง (Hamming Distance) เช่น รายงานผลการวิจัยของ [Chen2005] และของศาสตราจารย์ John Daugman [Daugman1993, 1994, 2004, 2006, 2007]

(2) กรณีที่วัดความต่างกันของรหัสม่านตาแบบค่าตัวเลข โดยส่วนมากจะใช้วิธีการวัดระยะทางแบบยุคลิด (Euclidean Distance) เช่น รายงานผลการวิจัยของ [Yuan2005]

อัลกอริทึมเปิดเผยชุดคำสั่ง (Open Source Algorithms)

อัลกอริทึมที่เปิดเผยชุดคำสั่ง (Open Source Code) สำหรับการรู้จำลายม่านตาให้บุคคลทั่วไปดาวน์โหลดและนำไปใช้งานได้มีดังตารางที่ 5

ตารางที่ 5 รายชื่ออัลกอริทึมที่เปิดเผยชุดคำสั่งสำหรับการรู้จำลายม่านตา

รูปแบบการทำงานของอัลกอริทึม	ชื่ออัลกอริทึม [Ref]	แหล่งดาวน์โหลด
ระบบการรู้จำลายม่านตาทั้งระบบ (Localization, Normalization, Feature extraction and Matching)	**OSIRIS [Othman2016]**	https://github.com/tohki/iris-osiris
ระบบการรู้จำลายม่านตาทั้งระบบ (รวบรวมมาจากหลากหลายอัลกอริทึมในขั้นตอนต่าง ๆ)	**USIT [Rathgeb2016]**	https://github.com/ngoclamvt123/usit-v2.2.0

1.3.3. การนำเทคโนโลยีการรู้จำลายม่านตาไปประยุกต์ใช้งาน

การรู้จำลายม่านตามีการนำไปประยุกต์ใช้งานในหลายรูปแบบที่แตกต่างกัน และมีการใช้งานที่หลากหลายในหลาย ๆ ประเทศ เช่น โครงการ NEXUS/CANPASS Air ซึ่งใช้ในการตรวจสอบผู้เดินทางที่มีความเสี่ยงต่ำที่ได้รับการอนุมัติล่วงหน้า ในสนามบินของแคนาดาหลายแห่ง[89] การลงทะเบียนประชากรของโครงการ AADHAAR ในประเทศอินเดีย [Aadhaar2020] รวมทั้งการใช้งานในหนังสือเดินทางประเภท Biometric Passport (e-Passport) [Atanasiu2010], [Ng-Kruelle2006]

แต่อย่างไรก็ตามการใช้งานระบบการรู้จำลายม่านตา ยังไม่ได้มีความแพร่หลายเมื่อเทียบกับการรู้จำใบหน้าหรือการรู้จำลายนิ้วมือ

1.3.4. จุดเด่นของการรู้จำลายม่านตา

ลายม่านตาเป็นหนึ่งในข้อมูลไบโอเมตริก ที่สามารถนำมาใช้ในการพิสูจน์ตัวบุคคลได้อย่างมีประสิทธิภาพ ซึ่งจุดเด่นและจุดด้อยของการรู้จำลายม่านตา มีดังนี้

จุดเด่นของการรู้จำลายม่านตา

1) ลายม่านตามีความเป็นเอกลักษณ์ที่สูงมากแม้กระทั่งฝาแฝดก็ตาม
2) ลายม่านตาไม่เปลี่ยนแปลงตามเวลา ซึ่งการพัฒนาลายม่านตาจะเสร็จสมบูรณ์หลังจากขวบปีแรก และรูปแบบที่ได้จะคงที่ตลอดอายุขัย
3) การใช้งานร่วมกันของม่านตาทั้งสองข้างจะทำให้โอกาสการพิสูจน์ตัวบุคคลผิดพลาดได้น้อยมาก
4) การใช้งานเป็นแบบไร้สัมผัส ซึ่งทำให้การตรวจพิสูจน์ทำได้ด้วยความรวดเร็วไม่สร้างความลำบากให้แก่ผู้ใช้ และลดโอกาสการแพร่เชื้อต่าง ๆ ที่เกิดจากการสัมผัสได้
5) การผ่าตัดเปลี่ยนแปลงลายม่านตาแบบถาวรทำได้ยาก ยกเว้น การสวมคอนแทคเลนส์ ซึ่งหากเทคโนโลยีที่นำมาใช้มีระบบป้องกันการหลอก (Liveness Detection) ร่วมด้วยจะทำให้สามารถป้องกันการปลอมแปลงนี้ได้
6) ดวงตาเป็นอวัยวะที่มนุษย์มีแต่กำเนิด โดยทั่วไปแล้วมนุษย์จะมีลายม่านตาสองข้าง ทำให้ระบบการรู้จำลายม่านตามีข้อเด่นที่ชุดข้อมูลสำรอง (Reservation) เพิ่มมาอีกด้วย

จุดด้อยของการรู้จำลายม่านตา

1) ระบบการรู้จำลายม่านตามีราคาสูง เนื่องจากต้องใช้การรับภาพที่ดีเพื่อให้มีคุณภาพและความคมชัดของลายม่านตาที่สูง
2) การรับภาพลายม่านตาจำเป็นต้องใช้ควบคู่กับอุปกรณ์จัดแสงอินฟราเรดย่านใกล้ ซึ่งหากปริมาณแสงที่ส่องเข้าดวงตามีปริมาณมาก อาจส่งผลกระทบต่อการมองเห็นได้ในอนาคต และทำให้ผู้ใช้งานไม่ให้ความร่วมมือหรือไม่ยินดีใช้เครื่องสแกนม่านตาได้

1.3.5. ข้อจำกัดหรืออุปสรรคของการใช้งานการรู้จำลายม่านตา

การรู้จำลายม่านตามีข้อจำกัดหรืออุปสรรคส่วนใหญ่ เกิดมาจากการรับภาพลายม่านตาที่ผู้ใช้งานอยู่ในระยะไกลเกินกว่า 2-3 เมตร หรือผู้ใช้งานมีการเคลื่อนที่อยู่ซึ่งทำให้ตาไม่ได้มองตรงเข้าไปยังเครื่องสแกน โดยในปัจจุบัน ได้มีการพัฒนางานวิจัยเพื่อแก้ไขจุดบกพร่องนี้ และเพื่อเพิ่มประสิทธิภาพของการใช้งานระบบการรู้จำลายม่านตาให้ง่ายขึ้นต่อผู้ใช้ (Less Constrained Iris Recognition System) [Nguyen2011] โดยได้มีการนำเสนอนวัตกรรมออกมาอยู่ในชื่อ “Iris-at-a-distance, IAAD” [Nguyen2017] ซึ่งมีความสามารถระบุตัวบุคคลได้ไกลขึ้น หรือ “Iris-on-the-move, IOM” [Matey2006] ของ Princeton Identity ซึ่งเครื่องสแกนจะสามารถทำงานได้ เมื่อผู้ใช้งานเดินผ่านเครื่องสแกนด้วยความเร็วปกติที่น้อยกว่า 1 เมตร/วินาที ที่ระยะห่างได้ถึง 3 เมตร

1.3.6. ความเสี่ยงและข้อควรระวังการใช้งานการรู้จำลายม่านตา

การสวมสิทธิ์โดยการปลอมลายม่านตาเป็นบุคคลอื่น (Spoofed Iris) สามารถเกิดขึ้นได้ในการใช้งานระบบการรู้จำลายม่านตา ซึ่งสามารถแบ่งออกได้เป็น 3 ประเภท คือ

---

[8] https://www.cbp.gov/travel/trusted-traveler-programs/nexus

[9] http://www.nexus.gc.ca

1) **การปลอมโดยคัดลอกลายม่านตาของบุคคลอื่น (Spoofed Iris from Image)** สามารถทำได้โดยการนำภาพถ่ายลายม่านตาของบุคคลอื่น มาคัดลอกและทำเป็นคอนแทคเลนส์เพื่อไว้ใช้ใส่ในการปลอมลายม่านตา [Sharma2020] โดยการปลอมลายม่านตานั้นจะใช้การถ่ายภาพภายใต้แสงอินฟาเรดย่านใกล้ (Near infrared, NIR) ที่มีความยาวช่วงคลื่นแสง 700-900 นาโนเมตร (nm) เพื่อให้เห็นรายละเอียดภายในชั้นเส้นเลือด (Stromal features) รวมกับการถ่ายภาพภายใต้แสงที่ตามองเห็น (Visible spectrum, VIS) ที่มีความยาวช่วงคลื่นแสง 400-700 นาโนเมตร (nm) เพื่อให้เห็นรายละเอียดของเม็ดสี (Pigment melanin)
2) **การปลอมโดยทำขึ้นจากรหัสม่านตาของบุคคลอื่น (Spoofed Iris from Code Template)** สามารถทำได้โดยการใช้โมเดลย้อนกลับ ของการรู้จำลายม่านตาเพื่อสร้างรูปแบบลายม่านตาขึ้น [Venugopalan2011] จากรหัสม่านตา ซึ่งมีความแตกต่างจากการปลอมลายม่านตาในหัวข้อแรก ที่ใช้การเลียนแบบและคัดลอกมาจากภาพม่านตา
3) **การรวมลายม่านตา (Iris Morph Attack)** การรวมลายม่านตา หมายถึง ภาพลายม่านตา 1 ภาพ สามารถใช้ระบุตัวบุคคลได้ตรงกันถึง 2 คน โดยที่ระบบการรู้จำลายม่านตาไม่ได้มีการทำงาน หรือประสิทธิภาพลดลงแต่อย่างใด ซึ่งหลักการที่ใช้จะเป็นการผสมภาพ (Blending) [Sharma2021] ในการสร้างภาพลายม่านตาใหม่ ขึ้นมาจากข้อมูลลายม่านตาจากทั้ง 2 ภาพ

1.3.7. แนวโน้มงานวิจัยในปัจจุบันของการรู้จำลายม่านตา

งานวิจัยและพัฒนาในปัจจุบันของระบบการรู้จำลายม่านตา มีแนวโน้มเพื่อเสริมประสิทธิภาพการใช้งานของระบบการรู้จำลายม่านตาเดิม ซึ่งมีอยู่ด้วยกัน 4 ด้าน ได้แก่

1) **การใช้งานในระหว่างที่เดินหรือเคลื่อนไหว (Iris at-a-distance and On-the-move)** ด้วยแนวโน้มของการใช้งานที่ต้องการความสะดวกสบาย จึงทำให้ผู้วิจัย/นักพัฒนา หาวิธีการสร้างระบบการจับภาพม่านตาในขณะที่ผู้ใช้เคลื่อนไหว [Zhang2020] ซึ่งเครื่องสแกนม่านตาจะถูกติดตั้งจากระยะไกลและต้องให้ภาพลายม่านตาที่มีคุณภาพเพียงพอสำหรับใช้ในระบบการรู้จำลายม่านตา โดยภายในจะใช้เทคนิคการวิเคราะห์ภาพต่อเนื่องเพื่อรวมให้ได้ภาพลายม่านตาที่คุณภาพดี และสามารถเอาไปใช้งานกับระบบการรู้จำลายม่านตาปกติได้

   นอกจากนี้ ภาพที่ถ่ายจากระยะไกลจะต้องมีใบหน้าปรากฏอยู่ในภาพเสมอ จึงทำให้เกิดการใช้งานร่วมกันกับระบบการรู้จำใบหน้าได้ และทำให้เกิดการพัฒนาของไบโอเมตริกร่วมระหว่างใบหน้าและม่านตาขึ้น [Azom2015]
2) **การรู้จำลายม่านตาข้ามสเปกตรัม (Cross-spectral Iris Recognition)** ด้วยความต้องการเพิ่มประสิทธิภาพของระบบการรู้จำ (Recognition performance boosting) จึงมีการนำภาพลายม่านตาที่ถ่ายจากแสงอินฟาเรดย่านใกล้ (NIR) และแสงที่ตามองเห็น (VIS) มาใช้ร่วมกัน [Oktiana2019] เนื่องจากรายละเอียดของรูปแบบลายม่านตาจากหลาย ๆ ย่านแสงนั้น สามารถเพิ่มลักษณะเด่นให้กับระบบการรู้จำได้มากขึ้น
3) **ระบบการรู้จำลายม่านตาที่ยกเลิกได้ (Cancelable Iris Recognition)** ด้วยความปลอดภัยของการใช้งานไบโอเมตริกเป็นเรื่องที่มีความสำคัญ เนื่องจากเป็นข้อมูลส่วนบุคคลที่ติดอยู่กับร่างกายและคนทั่วไปไม่ต้องการให้ไบโอเมตริกของตนเองถูกปลอมแปลง นำไปใช้สวมสิทธิ์ต่าง ๆ จึงทำให้การวิจัยทางด้านนี้มีการตีพิมพ์ออกมาต่อเนื่องอย่างสม่ำเสมอ โดยระบบการรู้จำลายม่านตาที่ยกเลิกได้ [Ouda2021] มีจุดประสงค์เพื่อรักษาความปลอดภัยของเทมเพลตหรือรหัสลายม่านตา หากเกิดการขโมยออกไปจากระบบได้
4) **การตรวจจับการโจมตี (Presentation Attack Detection)** ด้วยระบบการรู้จำลายม่านตาต้องมีความน่าเชื่อถือสำหรับการตรวจพิสูจน์และยืนยันตัวตน ระบบจึงจำเป็นต้องมีการป้องกันการปลอมลายม่านตาเป็นบุคคลอื่น ทำให้งานวิจัยในด้านนี้มีการนำเสนอมาอย่างต่อเนื่อง [Yadav2021], [Fang2021] โดยการโจมตีจะมีทั้งในรูปแบบของ การใช้ภาพพิมพ์ (Printed photo) การใช้ลูกตาปลอม (Artificial eyes) การใส่คอนแทคเลนส์เพื่อปลอมลายม่านตา (Cosmetic contact lens) ซึ่งทำให้เทคนิคของการตรวจจับความมีชีวิต (Liveness detection) สำหรับภาพลายม่านตาต้องมีประสิทธิภาพที่ซับซ้อนมากยิ่งขึ้น

1.4. การรู้จำลายเส้นเลือด (Vascular Recognition)

ลายเส้นเลือดเป็นหนึ่งในอัตลักษณ์ของมนุษย์ ที่สามารถใช้ในการระบุตัวบุคคลได้ มีการเริ่มต้นการศึกษาทางด้านนิติเวชในช่วงปี 1890s พบว่าไม่มีรูปแบบของลายเส้นเลือด ในมือคู่ใดของมนุษย์แต่ละคน มีโครงสร้างที่เหมือนกัน โดยตัวอย่างเส้นเลือดที่มีในมือแสดงดังภาพที่ 46 ทำให้ในช่วงเวลาต่อมาได้มีการศึกษาค้นคว้าการนำโครงสร้างของเส้นเลือดมายืนยันตัวตนของมนุษย์

นอกเหนือจากเส้นเลือดบริเวณมือของมนุษย์แล้ว ยังมีลายเส้นเลือดในบริเวณอื่นที่สามารถใช้ในการรู้จำตัวตนได้ เช่น ลายเส้นเลือดที่บริเวณนิ้วมือ ลายเส้นเลือดที่บริเวณข้อมือ และลายเส้นเลือดในดวงตา ต่อมาจึงเริ่มมีการพัฒนาเครื่องมือที่ใช้ในการเก็บภาพของลายเส้นเลือด การพัฒนามาจากการใช้งานทางการแพทย์ โดยมีการถ่ายภาพด้วยคลื่นสนามแม่เหล็ก (Magnetic Resonance Angiography : MRA) เป็นการเก็บข้อมูลภาพในช่วงแสง 900 – 1700 nm อย่างไรก็ตาม เพื่อความเหมาะสมในการใช้งาน จึงมีการปรับเปลี่ยนไปใช้เครื่องมือการเก็บภาพที่มีราคาถูกกว่า โดยเป็นการเก็บภาพในย่านความถี่ 800 nm ซึ่งเป็นย่านใกล้อินฟราเรด (Near-Infrared : NIR) แทน เนื่องจากเฮโมโกลบินที่อยู่ในเส้นเลือดยังสามารถดูดซับแสงในย่านนี้ได้ ทำให้ภาพที่ถ่ายได้เห็นบริเวณของเส้นเลือดเป็นสีดำและยังคงใช้ระบุตัวบุคคลได้

ภาพที่ 46 ภาพถ่ายลายเส้นเลือดด้วยคลื่นสนามแม่เหล็ก (ภาพจาก MBq at German [10])

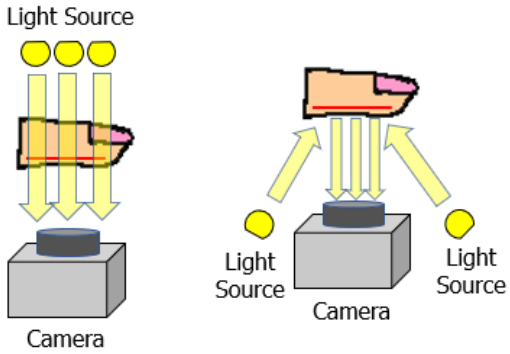
1.4.1. หลักการทำงานของการรู้จำลายเส้นเลือด

ปัจจุบันบริเวณของลายเส้นเลือดที่นิยมนำมาใช้ในการรู้จำมีอยู่ 2 บริเวณ คือ ลายเส้นเลือดที่บริเวณฝ่ามือและลายเส้นเลือดที่บริเวณดวงตา เนื่องจากอุปกรณ์ที่ใช้ในการเก็บข้อมูลส่วนใหญ่ มักจะถูกรวมเข้ากับระบบรู้จำอัตลักษณ์ที่มีอยู่เดิม เช่น อุปกรณ์เก็บข้อมูลลายเส้นเลือดจะถูกควบรวม เข้ากับอุปกรณ์เก็บข้อมูลภาพลายฝ่ามือ เป็นต้น ดังนั้นในการอธิบายหลักการทำงานของการรู้จำลายเส้นเลือดจึงแบ่งออกเป็น 2 ส่วนตามบริเวณของลายเส้นเลือดที่นำมาใช้งาน คือ

1) **การรู้จำลายเส้นเลือดบริเวณมือ (Hand-based Vascular Recognition)** การรู้จำลายเส้นเลือดบริเวณมือเริ่มต้นจากการออกแบบกระบวนการเก็บภาพ การเก็บภาพลายเส้นเลือดบริเวณมือสามารถทำได้ 2 รูปแบบ จากการเปลี่ยนตำแหน่งของแหล่งกำเนิดแสง (Light Source) และอุปกรณ์บันทึกภาพ (Camera) รูปแบบที่หนึ่งเป็นการเก็บภาพโดยใช้หลักการสะท้อนแสง (Reflected Light) การเก็บภาพในรูปแบบนี้แหล่งกำเนิดแสงและอุปกรณ์บันทึกภาพจะอยู่ในด้านเดียวกัน และรูปแบบที่สองจะเป็นการเก็บภาพโดยให้แสงส่องทะลุผ่านเนื้อเยื่อ (Transillumination) ดังแสดงในภาพที่ 47 ในการเก็บภาพรูปแบบนี้ อุปกรณ์บันทึกภาพ จะอยู่ด้านตรงข้ามกับแหล่งกำเนิดแสง ข้อแตกต่างระหว่างการเก็บข้อมูลทั้งสองรูปแบบนี้คือ ถ้าใช้การสะท้อนแสงจะเก็บ

[10] https://commons.wikimedia.org/wiki/File:CT-Angiografie-Haende.jpg

ข้อมูลเส้นเลือดที่อยู่ฝั่งเดียวกับฝ่ามือ (Palmar) ได้ดี และสามารถเก็บภาพลายเส้นเลือดในบริเวณข้อมือได้ แต่ถ้าหากใช้การเก็บภาพโดยให้แสงส่องผ่านมือจะสามารถเก็บข้อมูลเส้นเลือดได้ทั้งด้านฝ่ามือ (Palmar) และหลังมือ (Dorsal) แต่จะไม่สามารถเก็บภาพเส้นเลือดที่บริเวณข้อมือได้



ภาพที่ 47 การเก็บภาพเส้นเลือดแบบแสงส่องผ่าน (Transillumination) และการสะท้อนแสง (Reflected Light)

2) **การรู้จำลายเส้นเลือดบริเวณดวงตา (Eye-based Vascular Recognition)** การรู้จำลายเส้นเลือดบริเวณดวงตา จะเป็นการเก็บข้อมูลด้วยการใช้ภาพถ่ายจากแสงย่านการมองเห็นปกติ (Visible Light) ซึ่งอุปกรณ์ที่ใช้ในการเก็บภาพจะเป็นเครื่องมือที่ใช้ทางจักษุแพทย์เรียกว่า Fundus Cameras ในการบันทึกภาพจะมีการเก็บได้สองรูปแบบ คือ ใช้แสงปกติและการบันทึกภาพแบบที่คัดกรองสีเขียว (Green-pass filter) ที่มีย่านแสงอยู่ในช่วง (540 – 570 nm) เพื่อให้เกิดภาพเส้นเลือดที่มีระดับความแตกต่างของความเข้มสี (Contrast) สูง

เมื่ออุปกรณ์สามารถเก็บภาพของลายเส้นเลือดได้แล้ว ขั้นตอนในลำดับถัดมาจะเป็นการดึงลักษณะเฉพาะ (Feature Extraction) ออกจากภาพลายเส้นเลือดเพื่อแปลงข้อมูลให้อยู่ในรูปแบบที่เหมาะสมสำหรับการนำไปใช้ในการเปรียบเทียบด้วยระบบคอมพิวเตอร์ วิธีการดึงลักษณะเฉพาะของลายเส้นเลือดในปัจจุบันจะแบ่งออกเป็น 2 กลุ่ม คือ กลุ่มที่ใช้วิธีการดึงลักษณะเฉพาะจากโครงสร้างของเส้นเลือดโดยตรง (Structure-based) และการดึงลักษณะเฉพาะแบบไม่ใช้โครงสร้างของเส้นเลือดโดยตรง (Unstructured-based)

(1) การดึงลักษณะเฉพาะที่ใช้โครงสร้างของเส้นเลือดโดยตรง เป็นการใช้การตรวจหาตำแหน่งในภาพว่าบริเวณใดเป็นเส้นเลือด และทำให้อยู่ในรูปแบบของข้อมูลภาพสองระดับ (Binary Image) จากนั้นจึงใช้ลักษณะเฉพาะการแตกแขนงของเส้นเลือดในตำแหน่งที่แตกต่างกันเป็นลักษณะเฉพาะในการรู้จำบุคคล

(2) การดึงลักษณะเฉพาะแบบที่ไม่ใช้โครงสร้างของเส้นเลือดโดยตรง วิธีการดึงลักษณะเฉพาะนี้จะใช้เทคนิคการประมวลผลภาพในการรู้จำลักษณะของพื้นผิว (Texture) ในภาพ โดยไม่คำนึงว่าเป็นลักษณะของเส้นเลือดหรือไม่ โดยวิธีการที่นิยมใช้ในปัจจุบันจะเป็นการใช้การเรียนรู้ของเครื่อง (Machine Learning) เพื่อป้อนข้อมูลภาพลายเส้นเลือดให้ระบบทำการสร้างแบบจำลอง (Model) สำหรับใช้ในการรู้จำบุคคล

1.4.2. อัลกอริทึมการรู้จำลายเส้นเลือด

อัลกอริทึมที่มีลักษณะเป็น Open Source สำหรับการพัฒนาระบบรู้จำลายเส้นเลือด ปัจจุบันมีการพัฒนาโดยห้องปฏิบัติการ The Multimedia Signal Processing and Security Lab (WaveLab) ซึ่งเป็นทีมผู้พัฒนา PLUS OpenVein Toolkit ซึ่งรวบรวมวิธีการดึงลักษณะเฉพาะและการเปรียบเทียบลายเส้นเลือดหลายรูปแบบเข้าไว้ด้วยกัน โดยสามารถดูรายละเอียดเพิ่มเติมได้จากเว็บไซต์[11]

[11] https://www.wavelab.at/sources/OpenVein-Toolkit/

1.4.3. การนำเทคโนโลยีการรู้จำลายเส้นเลือดไปประยุกต์ใช้งาน

การนำระบบการรู้จำลายเส้นเลือดไปใช้งานในปัจจุบัน ยังมีการใช้งานที่ไม่แพร่หลายมากนัก เนื่องจากมีผู้พัฒนาผลิตภัณฑ์และเทคโนโลยีทางด้านนี้จำนวนไม่มาก อย่างไรก็ตาม ยังคงมีตัวอย่างการนำระบบรู้จำลายเส้นเลือดไปใช้งานในรูปแบบต่าง ๆ ตัวอย่างเช่น ระบบการชำระสินค้า Hand Pay ของบริษัท Lotte Card ในประเทศเกาหลี และระบบบันทึกการเข้าทำงานของบริษัท Fujitsu ในประเทศญี่ปุ่น นอกจากนี้ทางฝั่งยุโรปได้มีการพัฒนาอุปกรณ์รูปแบบนาฬิกา LeBracelet โดยบริษัท BiowatchID จากประเทศสวิตเซอร์แลนด์ เพื่อใช้ทดแทนการใช้งาน Password หรือ PIN ต่าง ๆ รวมไปถึงการยืนยันตัวบุคคล โดยการใช้ข้อมูลจากเส้นเลือดบริเวณข้อมือ (Wrist Vein) อย่างไรก็ตาม ปัจจุบันยังไม่พบรายงานในการนำอุปกรณ์ดังกล่าวไปใช้งานจริง มีเพียงรายงานผลการทดสอบประสิทธิภาพผ่านทางเว็บไซต์ของโครงการ Horizon2020 [12] ซึ่งเป็นแหล่งเงินทุนพัฒนางานวิจัยของทางยุโรป โดยอุปกรณ์นี้ทำการทดสอบกับกลุ่มตัวอย่างประมาณ 800 ข้อมือ เป็นภาพจำนวนมากกว่า 10,000 ภาพ และกำหนดค่า False Accept Rate ไว้ที่ 0.001% ประสิทธิภาพที่ทำได้อยู่ที่ False Reject Rate<5%

1.4.4. จุดเด่นของการรู้จำลายเส้นเลือด

จุดเด่นของการรู้จำลายเส้นเลือดบริเวณมือ

1) ภาพลายเส้นเลือดไม่ได้รับผลกระทบจากสภาพผิวหนัง (ผิวแห้ง ผิวมัน หรือมีการใช้โลชั่น) และไม่ได้รับผลกระทบจากการเปลี่ยนแปลงบริเวณผิวหนัง (การเกิดรอยแผลเป็น หรือการติด Tattoo)
2) การเก็บภาพเส้นเลือดสามารถเก็บได้โดยไม่ต้องสัมผัสอุปกรณ์ จึงป้องกันการติดเชื้อที่เกิดจากการสัมผัส และช่วยลดความเสียหายที่เกิดขึ้นกับอุปกรณ์เก็บข้อมูลได้
3) ภาพลายเส้นเลือดสามารถเก็บได้ในระยะทางที่ไม่ไกลจากกล้องที่บันทึกภาพได้มากนัก ดังนั้น จึงช่วยป้องกันการถูกเก็บข้อมูล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลได้ดีกว่า เมื่อเปรียบเทียบกับการใช้ลักษณะเฉพาะอื่นที่สามารถเก็บภาพได้ง่าย เช่น การเก็บภาพใบหน้า
4) การเก็บภาพลายเส้นเลือดสามารถตรวจจับการปลอมแปลงที่เกิดจากสิ่งไม่มีชีวิตได้จากการตรวจจับการไหลเวียนของเลือด (Blood Flow) ทำให้มีความทนทานต่อกระบวนการโจมตีได้ดีในระดับหนึ่ง

จุดเด่นของการรู้จำลายเส้นเลือดบริเวณดวงตา

1) ภาพเส้นเลือดบริเวณดวงตานั้น มีการเปลี่ยนแปลงน้อยและปลอมแปลงได้ยาก เป็นลักษณะเฉพาะที่ไม่ได้รับผลกระทบจากกระบวนการศัลยกรรม และไม่มีการเปลี่ยนแปลงไปตามอายุ
2) สามารถตรวจจับการปลอมแปลงที่เกิดจากสิ่งไม่มีชีวิตได้จากการตรวจจับการไหลเวียนของเลือด
3) การเก็บข้อมูลภาพลายเส้นเลือดบริเวณดวงตา ไม่จำเป็นต้องใช้แสงย่านใกล้อินฟราเรด (NIR) ในลักษณะเดียวกับการรู้จำลายม่านตา โดยสามารถใช้แสงย่านปกติได้ ทำให้มีโอกาสในการใช้งานร่วมกับอัตลักษณ์อื่นที่ใกล้เคียงได้ง่าย เช่น การใช้งานร่วมกับระบบรู้จำใบหน้า เป็นต้น แต่อย่างไรก็ตามในปัจจุบันยังไม่มีการทำผลิตภัณฑ์ที่สามารถรองรับการทำงานในลักษณะดังกล่าวได้

1.4.5. ข้อจำกัดหรืออุปสรรคของการใช้งานการรู้จำลายเส้นเลือด

อุปสรรคของการรู้จำลายเส้นเลือดบริเวณมือ

1) การเก็บภาพด้วยแสงใกล้อินฟราเรดจะมีความชัดเจนและคุณภาพที่ต่ำกว่าการถ่ายภาพทั่วไป เนื่องจากเนื้อเยื่อของมือนั้นมีการทำให้แสงกระจัดกระจาย (Scatter) ออกบางส่วน
2) ในปัจจุบันยังไม่มีการทดสอบผลกระทบที่แน่ชัดของการเปลี่ยนแปลงอุณหภูมิ หรืออาการป่วยที่เกี่ยวข้องกับเลือดต่อโครงสร้างของลายเส้นเลือดว่ามีผลกระทบต่อกระบวนการรู้จำหรือไม่

อุปสรรคของการรู้จำลายเส้นเลือดบริเวณดวงตา

1) การใช้แสงเพื่อถ่ายภาพบริเวณดวงตา ให้ผลกระทบและความรู้สึกที่ไม่ดีต่อผู้ใช้งาน
2) อุปกรณ์ที่ใช้ในการบันทึกภาพบริเวณดวงตามีราคาที่สูงและมักใช้ในงานทางการแพทย์เท่านั้น

---

[12] https://cordis.europa.eu/project/id/837512

3) การเก็บข้อมูลลายเส้นเลือดบริเวณดวงตาไม่สามารถทำในระยะไกลมากได้ และปัจจุบันยังไม่มีผู้ให้บริการรายใดมีการออกแบบผลิตภัณฑ์หรือวิธีการในการแก้ปัญหาต่าง ๆ เหล่านี้

1.4.6. ความเสี่ยงและข้อควรระวังการใช้งานการรู้จำลายเส้นเลือด

ในปัจจุบันยังไม่มีการนำการรู้จำลายเส้นเลือดไปใช้ในระบบที่มีฐานข้อมูลขนาดใหญ่ และยังมีบริษัทที่พัฒนาเทคโนโลยีทางด้านนี้ไม่มากนัก การนำระบบการรู้จำลายเส้นเลือดไปใช้งานในปัจจุบัน จึงต้องคำนึงถึงการเปลี่ยนแปลงของอุปกรณ์และซอฟต์แวร์ ที่อาจมีการเปลี่ยนแปลงได้ง่าย เนื่องจากอยู่ในช่วงของการพัฒนาระบบให้มีประสิทธิภาพสูงยิ่งขึ้น

1.4.7. แนวโน้มงานวิจัยในปัจจุบันของการรู้จำลายเส้นเลือด

แนวโน้มงานวิจัยที่น่าสนใจที่เกี่ยวข้องกับการรู้จำลายเส้นเลือดในปัจจุบัน มีดังต่อไปนี้

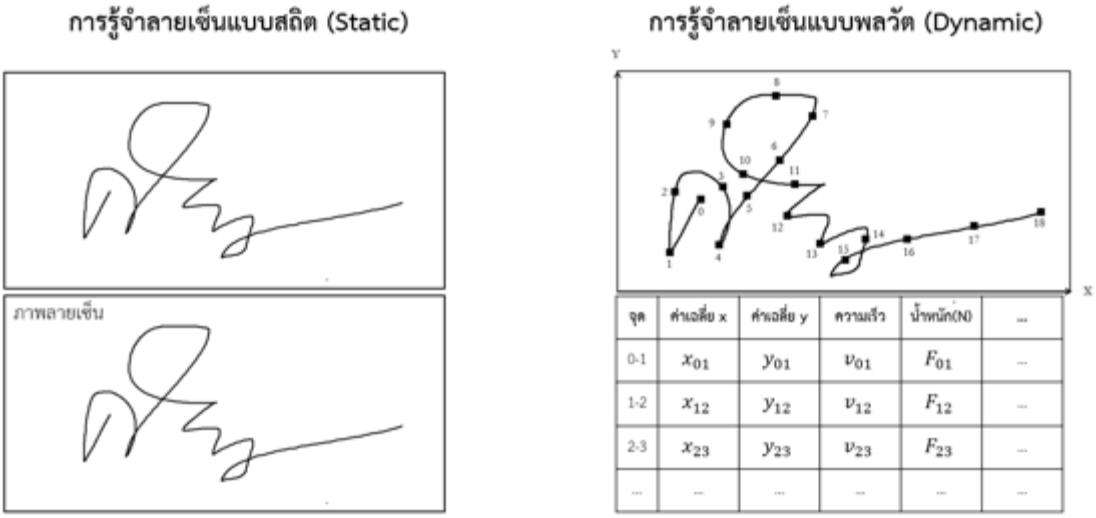
1) งานวิจัยทางด้านการพัฒนาอัลกอริทึมการรู้จำลายเส้นเลือด โดยใช้การเรียนรู้เชิงลึก [Wang2021c] [Qin2021b], [Hou2021a], [Hou2020b]
2) งานวิจัยทางด้านการป้องกันการโจมตีปลอมแปลงการรู้จำลายเส้นเลือด เช่น [Kauba2021], [Shahreza2021]
3) งานวิจัยทางด้านการตรวจจับลายเส้นเลือดด้วยคลื่นความถี่เหนือเสียง (Ultrasonic) [Peng2021] หรือการตรวจจับลายเส้นเลือดจากการสะท้อนแสง [Zhang2021]

1.5. การรู้จำลายเซ็น (Signature Recognition)

ลายเซ็นเป็นสัญลักษณ์ที่ตัวบุคคลสร้างขึ้น เพื่อใช้แทนตัวตนในกระบวนการยืนยันตัวตนสำหรับเอกสารสำคัญต่าง ๆ เช่น สนธิสัญญา ข้อตกลง เอกสารที่ต้องลงนาม ตั้งแต่ในอดีตจนถึงปัจจุบัน ลายเซ็นได้ถูกนำมาใช้ในระบบยืนยันตัวตนแบบดิจิทัล โดยกำหนดนิยามให้ลายเซ็นเป็นประเภทหนึ่งของไบโอเมตริกที่ถูกสร้างขึ้นจากพฤติกรรมของมนุษย์ [Jain2007]

การรู้จำลายเซ็นใช้วิธีการสังเกตและเรียนรู้ลักษณะของลายเซ็น รวมถึงพฤติกรรมของผู้เขียนลายเซ็น โดยทั่วไปสามารถจำแนกประเภทของการรู้จำลายเซ็นออกเป็น 2 ประเภท [Hennige2009] ตามประเภทของข้อมูลที่ถูกบันทึกและการนำเข้าสู่ระบบรู้จำ ดังแสดงในภาพที่ 48 โดยสามารถแจกแจงได้ดังนี้

1) **การรู้จำลายเซ็นแบบสถิต หรือออฟไลน์ (Static, Off-line)** เป็นการรู้จำลายเซ็นโดยการเก็บภาพลายเซ็นหลังจากเขียนเสร็จสิ้น และนำภาพลายเซ็นเข้าสู่ระบบรู้จำ
2) **การรู้จำลายเซ็นแบบพลวัต หรือออนไลน์ (Dynamic, On-line)** เป็นการรู้จำลายเซ็นโดยการเก็บข้อมูล ณ ขณะที่กำลังเขียนลายเซ็น โดยเก็บข้อมูลเป็นชุดด้วยความถี่ของเวลาหนึ่ง ภายในชุดข้อมูลประกอบไปด้วยข้อมูล พิกัดบนแผ่นเขียนอิเล็กทรอนิกส์ แรงกดจากปากกาอิเล็กทรอนิกส์ ความเร็วของการลากเส้น เป็นต้น และนำข้อมูลเหล่านี้เข้าสู่ระบบรู้จำ



ภาพที่ 48 ตัวอย่างการรู้จำลายเซ็น

1.5.1. หลักการทำงานของการรู้จำลายเซ็น

หลักการทำงานของการรู้จำลายเซ็น มีกระบวนการคล้ายกับหลักการทำงานรู้จำของไบโอเมตริกอื่น ๆ โดยเริ่มจากการบันทึกข้อมูลที่จะนำเข้าระบบ สำหรับการรู้จำลายเซ็นแบบสถิตใช้การเก็บภาพลายเซ็นเป็นภาพดิจิทัลประเภทภาพขาว-ดำเป็นข้อมูลนำเข้า และสำหรับการรู้จำลายเซ็นแบบพลวัต ใช้ชุดข้อมูลที่ถูกบันทึกในช่วงเวลาที่เขียนลายเซ็นจากเครื่องมืออิเล็กทรอนิกส์ เป็นข้อมูลนำเข้า

จากนั้นนำข้อมูลข้างต้นเข้าสู่ระบบเปรียบเทียบเพื่อระบุตัวตน โดยเปรียบเทียบระหว่างข้อมูลนำเข้าข้างต้นกับข้อมูลลายเซ็นที่ถูกเก็บไว้ในฐานข้อมูล ที่เป็นของบุคคลที่ต้องการเปรียบเทียบ ก่อนเข้าสู่ระบบเปรียบเทียบอาจนำข้อมูลนำเข้าและข้อมูลในฐานข้อมูล เข้ากระบวนการสกัดลักษณะเฉพาะ (Feature Extraction) เพื่อให้ระบบเปรียบเทียบดำเนินการเปรียบเทียบได้ง่ายมากยิ่งขึ้น สำหรับตัวระบบเปรียบเทียบอาจใช้ระบบการตัดสินใจทั่วไปหรือเทคโนโลยีที่ใช้ในปัจจุบันอย่างเช่น การเรียนรู้เครื่องจักร (Machine Learning) ในการสร้างระบบเปรียบเทียบ

ผลลัพธ์จากระบบเปรียบเทียบ อาจออกมาในรูปแบบของคะแนนความเหมือน ระหว่างข้อมูลนำเข้ากับข้อมูลในฐานข้อมูล แล้วกำหนดค่าเกณฑ์ที่จะผ่านการยืนยันตัวตนแล้ว

1.5.2. อัลกอริทึมการรู้จำลายเซ็น

ผู้ให้บริการทางระบบการรู้จำลายเซ็น ประเภทการยืนยันตัวตน มีทั้งในรูปแบบสถิต และแบบพลวัต โดยมีตัวอย่างผู้ให้บริการและลักษณะการใช้งาน ดังตารางที่ 6 นี้

ตารางที่ 6 รายชื่อบริษัทผู้จัดจำหน่ายระบบการรู้จำลายเซ็น

ชื่อบริษัท	ลักษณะการใช้งาน	เว็บไซต์
Witswell	CS-Plus เอ็นจิ้นที่ถูกใช้งานในระบบการรู้จำลายเซ็นรูปแบบพลวัต ที่เก็บข้อมูล ณ ขณะเขียน	http://www.cybersign.com/
Namirial DTM	ระบบการรู้จำลายเซ็นในรูปแบบเรียนรู้และอัพเดทลายเซ็นของแต่ละบุคคลทุก ๆ การเรียกขอการยืนยันตัวตน ทำให้สามารถติดตามการเปลี่ยนแปลงลายเซ็นของบุคคลนั้นตามกาลเวลาได้	https://www.xyzmo.com/digital-signature/e-signing-software
ProgressSoft	ระบบยืนยันตัวตนลายเซ็นแบบสถิตที่ใช้เทคโนโลยีการเรียนรู้เครื่องจักร (Machine Learning) ช่วยในการสกัดลักษณะเฉพาะ (Feature Extraction) เพื่อใช้ในการเปรียบเทียบลายเซ็นสำหรับระบุตัวตน	https://www.progressoft.com/products/signature-verification-recognition/ps-asv

1.5.3. การนำเทคโนโลยีการรู้จำลายเซ็นไปประยุกต์ใช้งาน

การรู้จำลายเซ็นแบบสถิต สามารถนำไปประยุกต์ใช้กับการตรวจสอบลายเซ็นของแต่ละบุคคลในเอกสารสำคัญ

การรู้จำลายเซ็นแบบพลวัต สามารถนำไปประยุกต์ใช้กับการยืนยันตัวตนในรูปแบบเวลาจริง (Real Time) และเหมาะสำหรับการเก็บเป็นข้อมูลการเขียนลายเซ็นของบุคคลนั้น ๆ ในฐานข้อมูลเพื่อพัฒนาระบบการรู้จำให้เรียนรู้วิธีการเขียนแทนการเรียนรู้รูปร่างลักษณะ

1.5.4. จุดเด่นของการรู้จำลายเซ็น

การรู้จำลายเซ็นแบบสถิต มีจุดเด่นในด้านความสะดวกในการเก็บข้อมูลลายเซ็น ที่ใช้เพียงภาพลายเซ็นประเภทภาพขาว-ดำหลังจากเขียนสำเร็จแล้ว

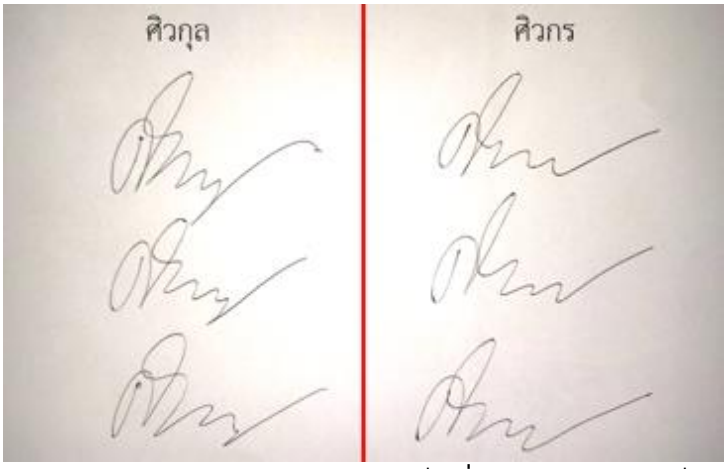
การรู้จำลายเซ็นแบบพลวัต มีจุดเด่นเรื่องความสามารถในการยืนยันและเปรียบเทียบลายเซ็นได้ถูกต้องและแม่นยำกว่าการรู้จำลายเซ็นแบบสถิต เนื่องจากมีการบันทึกข้อมูล ณ ขณะเขียนลายเซ็น จึงทำให้มีรายละเอียดข้อมูลจากลายเซ็นมากกว่าการรู้จำลายเซ็นแบบสถิต เมื่อนำเข้าระบบเปรียบเทียบลายเซ็น

1.5.5. ข้อจำกัดหรืออุปสรรคของการใช้งานการรู้จำลายเซ็น

ผลลัพธ์ข้อมูลลายเซ็นที่ได้ในแต่ละการเขียน โดยทั่วไปไม่ได้มีความเหมือนกันอย่างสมบูรณ์ เนื่องจากเป็นลักษณะพฤติกรรม ซึ่งขึ้นอยู่กับหลายปัจจัยในการเซ็นลายเซ็นแต่ละครั้งของแต่ละบุคคล การเซ็นลายเซ็นของคน ๆ เดียวกันมีความหลากหลายในตัวค่อนข้างสูง นอกจากนี้ อาจมีความไปคล้ายคลึงกับบุคคลอื่น ๆ อีกทั้ง ลายเซ็นยังมีข้อจำกัดของการใช้งานแตกต่างกัน ดังนี้

1) การรู้จำลายเซ็นแบบสถิต มีข้อจำกัดในเรื่องของรายละเอียดของข้อมูลลายเซ็นที่มีน้อย เนื่องจากใช้เพียงภาพลายเซ็นที่เขียนสำเร็จแล้วเพียงอย่างเดียว ทำให้มีผลกระทบต่อการเปรียบเทียบลายเซ็น ที่อาจเกิดความผิดพลาดได้มากกว่า

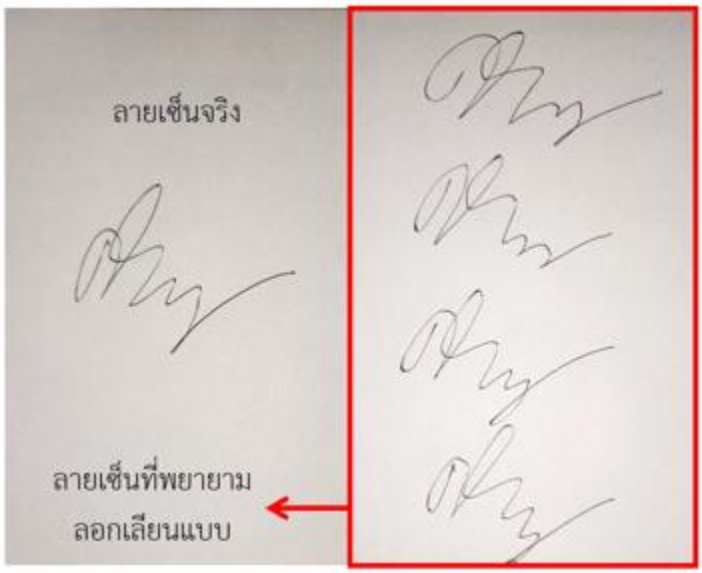
2) การรู้จำลายเซ็นแบบพลวัต มีข้อจำกัดทางด้านอุปกรณ์การเก็บข้อมูลลายเซ็นซึ่งต้องใช้อุปกรณ์พิเศษในขั้นตอนการรู้จำลายเซ็นจะต้องเตรียมอุปกรณ์ที่สามารถเก็บข้อมูล ณ ขณะที่เขียนลายเซ็นได้ เช่น แผ่นเขียนอิเล็กทรอนิกส์ ปากกาอิเล็กทรอนิกส์ แท็บเล็ตที่มีปากกา เป็นต้น



ภาพที่ 49 ตัวอย่างข้อจำกัดหรืออุปสรรคของการรู้จำลายเซ็น ซึ่งมีความต่างในลายเซ็นของบุคคลเดียวกัน และมีความเหมือนในบุคคลต่างกัน

1.5.6. ความเสี่ยงและข้อควรระวังการใช้งานการรู้จำลายเซ็น

ปัญหาการปลอมหรือพยายามลอกเลียนแบบลายเซ็น (Forgery) เนื่องจากลายเซ็นเป็นหนึ่งในลักษณะพฤติกรรมของมนุษย์ ไม่ใช่ลักษณะติดตัวมนุษย์ ดังนั้น มนุษย์ที่มีความสามารถในการลอกเลียนแบบพฤติกรรมต่าง ๆ จึงสามารถลอกเลียนแบบลายเซ็นของเป้าหมายได้ ทำให้ระบบยืนยันตัวตนด้วยลายเซ็นยังคงมีความเสี่ยง จึงจำเป็นจะต้องทราบตัวบุคคลที่เขียนลายเซ็น เพื่อหลีกเลี่ยงการปลอมแปลงตัวบุคคล



ภาพที่ 50 ตัวอย่างความเสี่ยงของการรู้จำลายเซ็น

1.5.7. แนวโน้มงานวิจัยในปัจจุบันของการรู้จำลายเซ็น

งานวิจัยทางด้านการรู้จำลายเซ็นมีจำนวนไม่มาก เมื่อเทียบกับงานวิจัยการรู้จำของไบโอเมตริกชนิดอื่น ๆ ด้วยข้อจำกัดและความเสี่ยงที่กล่าวมาข้างต้น เป็นปัญหาที่แก้ไขได้ยากสำหรับงานวิจัยการรู้จำลายเซ็น มุ่งเน้นไปทางการพัฒนาระบบการยืนยันตัวตน โดยส่วนมากจะวิจัยศึกษาการรู้จำลายเซ็น แบบยืดหยุ่นมากกว่าการรู้จำลายเซ็นแบบสถิต และทั้งสองรูปแบบใช้การประยุกต์หลักการเรียนรู้เครื่องจักร (Machine Learning) เพื่อสร้างกระบวนการสกัดลักษณะเฉพาะ (Feature Extraction) และตัวเปรียบเทียบลายเซ็นสำหรับระบบการยืนยันตัวตน

แนวโน้มงานวิจัยที่น่าสนใจที่เกี่ยวข้องกับการรู้จำลายเซ็นในปัจจุบัน มีดังต่อไปนี้

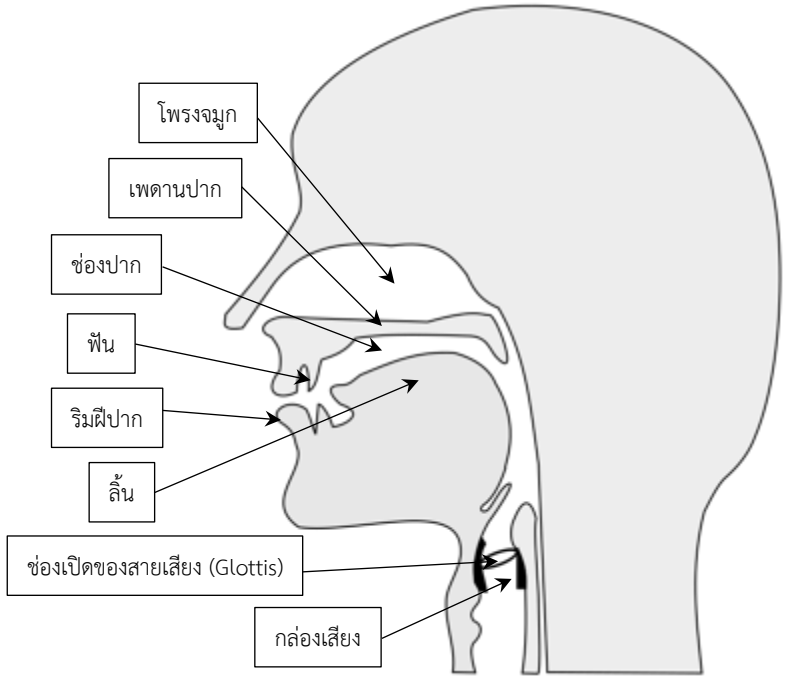
1) งานวิจัยทางด้านการพัฒนาอัลกอริทึมการรู้จำลายเซ็นโดยใช้การเรียนรู้เชิงลึก [Li2021], [Tolosana2021]
2) งานวิจัยทางด้านการป้องกันการโจมตีปลอมแปลงการรู้จำลายเซ็น [Lai2021]

1.6. การรู้จำเสียงพูด (Voice Recognition)

การใช้เสียงเป็นลักษณะเฉพาะหนึ่งในไบโอเมตริกที่ได้รับความสนใจ มนุษย์ใช้เสียงในการสื่อสารระหว่างกัน และเสียงของผู้พูดแต่ละคนมีเอกลักษณ์ และสามารถใช้ในการพิสูจน์ยืนยันตัวบุคคลได้ นอกจากข้อมูลที่ต้องการสื่อสาร เสียงของมนุษย์มีข้อมูลประกอบที่สามารถบ่งบอกเพศ สถานะของอารมณ์ และสุขภาพของผู้พูดด้วย [Benesty2008]

ความเป็นเอกลักษณ์ของเสียงพูดของผู้พูดแต่ละคน ขึ้นอยู่กับสองส่วนหลัก ส่วนแรก คือ โครงสร้างทางกายภาพของบุคคล (Physiological characteristics) และส่วนที่สอง คือ ลักษณะนิสัย (Behavioral characteristics)

ส่วนแรก คือ โครงสร้างทางกายภาพของบุคคล จะพิจารณาส่วนกำเนิดเสียง โดยเฉพาะ บริเวณช่องเสียง (Vocal tract) ทั้งหมดซึ่งประกอบด้วย ริมฝีปาก ฟัน ลิ้น กราม ช่องปาก เพดานปาก ทางเดินจมูก จนไปถึงปอด ซึ่งส่วนต่าง ๆ เหล่านี้ จะเป็นตัวกำหนดลักษณะเฉพาะของเสียงของแต่ละคนที่ไม่เหมือนกัน ดังแสดงในภาพที่ 51



ภาพที่ 51 ส่วนประกอบต่างๆ บริเวณช่องเสียง ที่ทำให้เสียงแต่ละบุคคลมีความเป็นเอกลักษณ์

(ภาพจาก Tavin - Own work [13], CC BY 3.0)

เสียงพูดของมนุษย์เกิดจากลม ที่อัดผ่านช่องเปิดของสายเสียงบริเวณกล่องเสียง (Glottis) หรือลมที่ผ่านช่องเสียง ซึ่งสร้างกลุ่มความถี่สั่นพ้องของช่องเสียง (Formant) เฉพาะตนขึ้นในแต่ละบุคคล กลุ่มความถี่สั่นพ้องของช่องเสียง จะประกอบด้วยความถี่พื้นฐาน (Fundamental frequency) แถบความถี่ (Bandwidth) และความถี่ฮาร์โมนิกต่าง ๆ (Harmonic frequencies) ประกอบกันเป็นเสียงพูดของแต่ละบุคคล ความถี่พื้นฐานของแต่ละบุคคลไม่เหมือนกันขึ้นอยู่กับโครงสร้างช่องเสียงดังกล่าวมาแล้ว โดยทั่วไป ผู้ชายจะมีความถี่พื้นฐานเฉลี่ยของเสียงอยู่ที่ประมาณ 100 เฮิรตซ์ ผู้หญิงจะอยู่ที่ประมาณ 200 เฮิรตซ์ และเด็กจะอยู่ที่ประมาณ 300 เฮิรตซ์ [Benesty2008] ความถี่เหล่านี้อาจใช้แยกเพศได้อย่างหยาบ ๆ ส่วนประกอบอื่น ๆ ทางโครงสร้างจะเป็นตัวกำหนดรูปร่างของคลื่นและความถี่ฮาร์โมนิกต่าง ๆ ซึ่งเป็นส่วนประกอบในรายละเอียดของเสียงแต่ละคน ทำให้สามารถพิสูจน์ยืนยันตัวบุคคลด้วยเสียงได้

[13] https://commons.wikimedia.org/w/index.php?curid=17324330

1.6.1. หลักการทำงานของการรู้จำเสียงพูด

หลักการทำงานของระบบการรู้จำผู้พูดอยู่ที่การจำแนกลักษณะเด่น (Feature) ซึ่งเป็นลักษณะเฉพาะจากเสียงของแต่ละบุคคล โดยระบบจะแยกลักษณะเด่นของเสียงออกเป็นสองประเภท ลักษณะเด่นระดับล่าง (Low-level feature) และลักษณะเด่นระดับบน (High-level feature) [Benesty2008] โดยลักษณะเด่นระดับล่างจะประกอบไปด้วย กลุ่มความถี่สั่นพ้องของช่องเสียง (Formant) แถบความถี่ (Bandwidth) การซ้ำคาบของระดับเสียง (Pitch periodicity) และเวลาการแบ่งส่วนของเสียง (Segmental timing) ส่วนลักษณะเด่นระดับบนจะประกอบไปด้วย การรับรู้คำพูดและความหมาย (Perception of words and their meaning) ความสัมพันธ์ระหว่างถ้อยคำในประโยค หรือวากยสัมพันธ์ (Syntax) จังหวะหรือทำนองเสียงในการพูด หรือสัทสัมพันธ์ (Prosody) ภาษาถิ่น (Dialect) และการใช้ภาษาเฉพาะตน (Idiolect) โดยทั่วไปในเชิงเทคนิค ลักษณะเด่นระดับล่างสามารถตรวจจับได้ง่ายกว่าลักษณะเด่นระดับบน

ภาพที่ 52 โครงสร้างระบบยืนยันตัวบุคคลด้วยเสียงพูด [Benesty2008]

โครงสร้างระบบยืนยันตัวบุคคลด้วยเสียงพูดโดยทั่วไปแล้วเป็นดังภาพที่ 52 ระบบจะรับเสียงจากผู้พูดพร้อมทั้งข้อมูลอ้างอิง เช่น รหัส ชื่อผู้ใช้ระบบ หรือ เลขประจำตัว เพื่อเป็นตัวบ่งชี้ในการดึงแบบจำลองหรือโมเดลของผู้พูดมาใช้ในการเปรียบเทียบ โดยเสียงจากผู้พูดจะถูกประมวลผล ซึ่งประกอบไปด้วยการสุ่มตัวอย่างและแปลงสัญญาณเสียงให้เป็นสัญญาณดิจิทัล ในส่วนนี้จะรวมการกรองกำจัดสัญญาณรบกวนต่าง ๆ ออกไปด้วย จากนั้นสัญญาณดิจิทัลจะถูกวิเคราะห์และสกัดลักษณะเด่นที่สำคัญที่เป็นเอกลักษณ์ของเสียง อาทิเช่น ลักษณะเด่นระดับล่าง และ ลักษณะเด่นระดับบน ดังที่อธิบายไปก่อนหน้า ในส่วนสุดท้ายจะเป็นการเปรียบเทียบความเหมือนของลักษณะเด่นต่าง ๆ เพื่อเปลี่ยนเป็นคะแนนความเหมือน โดยผู้ควบคุมระบบจะเป็นผู้กำหนดว่า ค่าคะแนนความเหมือนควรจะมีค่าเกินค่าที่กำหนดไว้จึงจะถือว่าบุคคลนั้นเป็นบุคคลเจ้าของข้อมูลอ้างอิง

1.6.2. อัลกอริทึมการรู้จำเสียงพูด

การพิสูจน์ยืนยันตัวตนด้วยการใช้เสียงพูด สามารถแบ่งได้เป็นสองประเภท คือ แบบกำหนดข้อความ (Text Dependence) ซึ่งจะต้องมีข้อความกำกับแสดงให้ผู้พูดกล่าวตามข้อความเหล่านั้น และแบบไม่กำหนดข้อความ (Text Independence) จะเป็นการให้ผู้พูดกล่าวคำพูดได้อย่างอิสระ โดยปกติแล้วอัลกอริทึมรู้จำผู้พูดแบบกำหนดข้อความจะมีความแม่นยำสูงกว่าแบบไม่กำหนดข้อความ เนื่องจากข้อความที่กำหนดจะถูกใช้ในการสอนและการรู้จำของระบบ ซึ่งระบบจะเรียนรู้แบบเฉพาะเจาะจงกับข้อความเหล่านี้[14] สำหรับแบบไม่กำหนดข้อความ ระบบจะต้องดึงเอกลักษณ์จากเสียงพูด เพื่อสร้างความแตกต่างระหว่างบุคคล ซึ่งจะมีทั้งการสกัดลักษณะเด่นระดับล่าง และลักษณะเด่นระดับบน ซึ่งทำให้อัลกอริทึมมีความซับซ้อนมากกว่าแบบกำหนดข้อความ โดยปกติการสกัดลักษณะเด่นจะใช้ Mel-Frequency Cepstral Coefficients (MFCC) และ Perceptual Linear Prediction Cepstral Coefficients (PLCC) เป็นหลัก [Sundararajan2018]

อัลกอริทึมรู้จำผู้พูดแบบกำหนดข้อความ จะใช้เทคนิคการจับคู่การเรียงลำดับของสเปคตรัมของสัญญาณเสียงซึ่งมีรูปแบบคำพูดตามข้อความที่กำหนด โดยพื้นฐานแล้วจะใช้วิธี Dynamic Time Warping (DTW) หรือวิธี Hidden Markov Model (HMM) โดยวิธี DTW จะเป็นการจัดเรียงสเปกตรัมโดยตามเวลาที่สามารถยืดหดตามการเปล่งเสียงที่อาจมีความแตกต่างกันทางช่วงเวลาได้ เมื่อสามารถปรับช่วงเวลาให้ตรงกันแล้ว ก็จะสามารถเปรียบเทียบสเปกตรัม

[14] http://www.scholarpedia.org/article/Speaker_recognition

ในแต่ละส่วนของคำพูดได้ ส่วนวิธี HMM จะเป็นการสร้างโมเดลทางด้านสถิติของสเปกตรัมเสียงพูดได้อย่างมีประสิทธิภาพ ทำให้มีประสิทธิภาพสูงกว่าวิธี DTW [15]

อัลกอริทึมรู้จำผู้พูดแบบไม่กำหนดข้อความ จะใช้เทคนิคที่ซับซ้อนกว่าแบบกำหนดข้อความ เช่น วิธี Vector Quantization (VQ) หรือใช้วิธี Gaussian Mixture Models (GMM) เพื่อหาโมเดลการกระจายตัวของข้อมูลของผู้พูด โดยเฉพาะเพื่อที่จะเรียนรู้โมเดล Universal Background Model (UBM) ปัจจุบันเป็นยุคของ Deep Learning ซึ่งเทคนิคต่าง ๆ ทางด้าน Deep Learning ได้นำมาประยุกต์ใช้กับการรู้จำผู้พูด เพื่อพัฒนาประสิทธิภาพของระบบให้ดียิ่งขึ้น โดยเทคนิคต่าง ๆ ที่ใช้ คือ Deep Belief Networks (DBN), Restricted Boltzmann Machines (RBM), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) [Sundararajan2018]

อัลกอริทึมเปิดเผยชุดคำสั่ง (Open Source Algorithms)

อัลกอริทึมที่เปิดเผยชุดคำสั่ง (Open Source Code) สำหรับการรู้จำเสียงพูดให้บุคคลทั่วไปดาวน์โหลดและนำไปใช้งานได้มีดังตารางที่ 7

ตารางที่ 7 รายชื่ออัลกอริทึมที่เปิดเผยชุดคำสั่งสำหรับการรู้จำผู้พูด

รายละเอียด	แหล่งดาวน์โหลด
Paperwithcode เว็บไซต์นี้ได้รวบรวมบทความที่มี Open-Source Code ให้ทางด้านการรู้จำผู้พูดอยู่มากถึง 48 บทความ และมีฐานข้อมูลเสียง 5 ฐานข้อมูล โดยเข้าถึงล่าสุดเมื่อวันที่ 25 ตุลาคม 2564	https://paperswithcode.com/task/speaker-recognition
เว็บไซต์นี้ได้รวบรวม Open Source Code ทางด้าน Speaker Recognition มากถึง 135 โครงการ โดยเข้าถึงล่าสุดเมื่อวันที่ 25 ตุลาคม 2564	https://awesomeopensource.com/projects/speaker-recognition

1.6.3. การนำเทคโนโลยีการรู้จำเสียงพูดไปประยุกต์ใช้งาน

การนำเทคโนโลยีการรู้จำเสียงพูดไปประยุกต์ใช้งาน[16] มีดังต่อไปนี้

1) ในช่วงปี พ.ศ. 2539-2541 (ค.ศ. 1996-1998) ที่บริเวณด่านชายแดนระหว่างสหรัฐอเมริกากับแคนาดา โดยเฉพาะที่ด่าน Scobey–Coronach Border Crossing มีการใช้ระบบรู้จำผู้พูดในการยืนยันตัวบุคค สำหรับผ่านแดนในกรณีที่ไม่มีสิ่งที่ต้องสำแดงในเวลาที่ด่านปิดตอนกลางคืน ซึ่งใช้เฉพาะกับผู้อาศัยในบริเวณแถบนั้น ซึ่งได้ลงทะเบียนไว้กับด่านก่อนล่วงหน้า
2) ในเดือนพฤษภาคม ปี พ.ศ. 2556 (ค.ศ. 2013) ธนาคาร Barclays Wealth ใช้ระบบรู้จำผู้พูดในการยืนยันตัวบุคคลของลูกค้าที่โทรศัพท์เข้ามาโดยการสนทนาปกติภายใน 30 วินาที
3) ธนาคาร Barclays เป็นสถาบันแห่งแรกที่ให้บริการการเงินโดยใช้ระบบรู้จำเสียงพูดเป็นหลักในการยืนยันตัวบุคคลผ่าน Call Center โดยลูกค้าถึง 93% ให้ความพึงพอใจสูงถึงเก้าเต็มสิบจากความรวดเร็ว ความสะดวกในการใช้งานและความปลอดภัย
4) ในเดือนกุมภาพันธ์ ปี พ.ศ. 2559 (ค.ศ. 2016) ธนาคาร HSBC ในประเทศอังกฤษและธนาคาร First Direct ซึ่งเป็นธนาคารสาขาของ HSBC ที่เน้นการให้บริการใช้งานผ่านอินเทอร์เน็ตเป็นหลัก ได้มีระบบบริการลูกค้าให้สามารถเข้าถึงแบบ Online หรือผ่านระบบโทรศัพท์ โดยใช้ลายนิ้วมือหรือเสียงพูดเป็นการยืนยันตัวบุคคล

1.6.4. จุดเด่นของการรู้จำเสียงพูด

การใช้งานระบบรู้จำผู้พูดโดยใช้เสียงพูด มีจุดเด่นหลายข้อ ดังนี้

1) มนุษย์ยอมรับการใช้เสียงในการสื่อสาร ดังนั้นการใช้เสียงเพื่อการรู้จำผู้พูดเป็นสิ่งที่ได้รับการยอมรับในมนุษย์โดยทั่วไป และไม่ว่าชนชาติใด ก็จะมีการสื่อสารด้วยเสียงเป็นสำคัญ
2) การเก็บข้อมูลเสียง สามารถเก็บข้อมูลได้ง่าย ตั้งแต่อุปกรณ์การเก็บเสียงที่มีราคาถูก พื้นที่หน่วยความจำสำหรับการเก็บข้อมูลต่ำ และอัลกอริทึมที่ไม่ซับซ้อน

[15] http://www.scholarpedia.org/article/Speaker_recognition

[16] https://en.wikipedia.org/wiki/Speaker_recognition

3) สามารถนำไปประยุกต์กับการรู้จำผู้พูดในระยะไกล ผ่านเครือข่ายสื่อสารที่มีคุณภาพและมีความปลอดภัยได้เป็นอย่างดี

1.6.5. ข้อจำกัดหรืออุปสรรคของการใช้งานการรู้จำเสียงพูด

การใช้งานระบบรู้จำผู้พูดโดยใช้เสียงพูด มีข้อจำกัดหรืออุปสรรคของการใช้งาน ดังนี้

1) เสียงมีการเปลี่ยนแปลงตามอายุและสุขภาพของแต่ละบุคคล ซึ่งจะมีผลกับประสิทธิภาพระบบรู้จำเสียงตามระยะเวลาการใช้งาน วิธีแก้ปัญหาคือการคอยปรับปรุงโมเดลที่เปลี่ยนแปลงของเสียงหลังจากที่ผ่านการพิสูจน์ยืนยันตัวบุคคล ในส่วนนี้มีข้อควรระวัง คือ ทำให้การรักษาความปลอดภัยทำได้ยากขึ้นถ้ามีการจงใจปรับโมเดลให้ผู้ที่ไม่ใช่เจ้าของสามารถสวมรอยได้[17]
2) ระบบรู้จำผู้พูดไม่เหมาะกับการใช้งานในบริเวณที่มีเสียงรบกวน การเก็บเสียงพูดอาจมีสัญญาณรบกวนขึ้นอยู่กับเสียงต่าง ๆ ในสภาพแวดล้อม หรือเสียงมนุษย์ผู้อื่น ทำให้ประสิทธิภาพของระบบรู้จำผู้พูดลดลง การใช้อัลกอริทึมในการลดสัญญาณรบกวน สามารถเพิ่มความแม่นยำของระบบได้ แต่ในทางกลับกัน อาจลดความแม่นยำของระบบได้เช่นกัน ถ้าเสียงบางส่วนโดนกรองไปพร้อมกับสัญญาณรบกวน
3) ผู้ใช้งานหลาย ๆ คนก็ยังรู้สึกอายที่จะใช้เสียงพูดกับโทรศัพท์ ในขณะที่คนอื่นได้ยินเสียงนั้นด้วย

1.6.6. ความเสี่ยงและข้อควรระวังการใช้งานการรู้จำเสียงพูด

อธิบายความเสี่ยงและข้อควรระวังการใช้งานของการรู้จำเสียงพูด โดยเฉพาะการโจมตีระบบโดยการใช้การปลอมแปลงแบบต่าง ๆ

การใช้เทคโนโลยีรู้จำผู้พูด มีความเสี่ยงและข้อควรระวังการใช้งาน ดังต่อไปนี้

1) เสียงสามารถถูกปลอมแปลงได้โดยง่ายโดยเทคโนโลยี Deep Learning ปัจจุบันสามารถปลอมแปลงเสียงผู้พูดได้อย่างไม่ยาก เช่น ระบบ AI ปัจจุบันสามารถเลียนเสียง หรือทำโคลนนิ่งเสียงได้ภายใน 5 วินาที[18]
2) เสียงสามารถถูกแอบเก็บได้ง่ายโดยใช้สมาร์ทโฟน การนำเสียงมาเล่นซ้ำเป็นเรื่องที่ทำได้ง่าย ทำให้สามารถเข้าระบบการพิสูจน์ยืนยันตัวตน ด้วยการใช้เสียงแบบกำหนดข้อความได้โดยง่าย
3) การใช้ระบบรู้จำผู้พูดจากอุปกรณ์หรือเครือข่ายที่ต่างกัน มีผลทำให้ประสิทธิภาพอาจด้อยลงเนื่องจากระบบสื่อสารที่แตกต่างกัน เช่น การลงทะเบียนโดยใช้โทรศัพท์เครื่องหนึ่ง และยืนยันตัวบุคคลด้วยโทรศัพท์อีกเครื่องหนึ่ง เป็นต้น

1.6.7. แนวโน้มงานวิจัยในปัจจุบันของการรู้จำเสียงพูด

แนวโน้มงานวิจัยที่น่าสนใจที่เกี่ยวข้องกับการรู้จำเสียงพูดในปัจจุบัน มีดังต่อไปนี้

1) งานวิจัยทางด้านการพัฒนาอัลกอริทึมการรู้จำเสียงพูดโดยใช้การเรียนรู้เชิงลึก [Cai2020], [Li2020]
2) งานวิจัยทางด้านการป้องกันการโจมตีปลอมแปลงการรู้จำเสียงพูด [Nautsch2021], [Gomez-Alanis2021], [Chettri2021], [Yang2020]
3) งานวิจัยการรู้จำเสียงผู้พูดด้วยเสียงกระซิบ [Vestman2018], [Kelly2021]
4) งานวิจัยการรู้จำเสียงผู้พูดเพื่อให้ทนต่อเสียงที่เปลี่ยนจากอารมณ์โกรธ [Aldeneh2021]
5) งานวิจัยที่ใช้ทั้งวีดิทัศน์ผู้พูดและเสียงเป็นไบโอเมตริกประกอบกัน [Qian2021]

---

[17] https://en.wikipedia.org/wiki/Speaker_recognition

[18] https://www.youtube.com/watch?v=0sR1rU3gLzQ

1.7. การเปรียบเทียบคุณสมบัติของลักษณะเฉพาะไบโอเมตริกแบบต่างๆ

จากการศึกษาลักษณะเฉพาะไบโอเมตริกในรูปแบบต่างๆ ที่มีการใช้กันทั้ง 6 แบบ คือ ใบหน้า ลายนิ้วมือ ลายม่านตา ลายเส้นเลือด ลายเซ็น และ เสียงพูด สามารถสรุปได้ว่า ไม่มีลักษณะเฉพาะไบโอเมตริกใดที่มีคุณสมบัติสมบูรณ์แบบครบทั้ง 7 ประการ คือ ความเป็นเอกลักษณ์ ความคงทนถาวร ความเป็นลักษณะเฉพาะทั่วไปของมนุษย์ ความสามารถในการตรวจวัดได้ สมรรถนะ ความเป็นที่ยอมรับของผู้ใช้ การปลอมแปลงได้ยาก ดังนั้น สามารถสรุปได้ว่า ลักษณะเฉพาะไบโอเมตริกที่สมบูรณ์แบบนั้นไม่มี ตารางที่ 8 แสดงการเปรียบเทียบลักษณะเฉพาะไบโอเมตริกแบบต่าง ๆ ที่กล่าวมาแล้วข้างต้น รวมทั้งสรุปจุดเด่นและข้อจำกัดของแต่ละลักษณะเฉพาะไบโอเมตริกมาไว้ที่ท้ายตาราง

ตารางที่ 8 การเปรียบเทียบคุณสมบัติของลักษณะเฉพาะไบโอเมตริกแบบต่าง ๆ

	ใบหน้า	ลายนิ้วมือ	ลายม่านตา	ลายเส้นเลือด	ลายเซ็น	เสียง
(1) ความเป็นเอกลักษณ์	ไม่เสมอไป เกี่ยวกับพันธุกรรม และอายุ	มีเอกลักษณ์สูงมาก	มีเอกลักษณ์สูงมาก	มีเอกลักษณ์ ขาดการพิสูจน์ ด้วยฐานข้อมูลขนาดใหญ่	ไม่เสมอไป เกี่ยวกับพฤติกรรม และเวลา	ไม่เสมอไป เกี่ยวกับพันธุกรรม และอายุ
(2) ไม่เปลี่ยนไปตามกาลเวลา	เปลี่ยน	ไม่เปลี่ยน	ไม่เปลี่ยน	ไม่เปลี่ยน	เปลี่ยน	เปลี่ยน
(3) ความเป็นลักษณะเฉพาะทั่วไป ของมนุษย์	ทุกคนมีใบหน้า	มนุษย์ปกติมี ยกเว้นผู้พิการ	มนุษย์ปกติมี ยกเว้นผู้พิการ ตาบอด หรืออุบัติเหตุ	มนุษย์ปกติมี ยกเว้นผู้พิการ อวัยวะส่วนนั้น หรืออุบัติเหตุ	ผู้ที่เขียนหนังสือไม่ได้ ไม่มีลายเซ็น	มนุษย์ปกติมี ยกเว้นผู้พิการ เป็นใบ้ หรืออุบัติเหตุ
(4) ความสามารถในการตรวจวัดได้	สะดวก ใช้กล้องวงจรปิดธรรมดาได้ มีฐานข้อมูลขนาดใหญ่	สะดวก เซนเซอร์ราคาถูก มีฐานข้อมูลขนาดใหญ่	การใช้งานยากต้องมีระยะ ที่พอเหมาะระหว่างดวงตา กับกล้อง มีฐานข้อมูลใหญ่	สะดวก มีฐานข้อมูลจำกัด	สะดวก ระบบยังไม่เป็นที่ยอมรับ มีฐานข้อมูลจำกัด	สะดวก จำกัดการใช้งาน ทางโทรศัพท์ มีฐานข้อมูลจำกัด
(5) สมรรถนะของระบบปัจจุบัน	สูง ประยุกต์ใช้งานได้กว้าง	สูง ประยุกต์ใช้งานได้กว้าง	สูง แต่ราคาแพง	สูง (1:1) แต่ (1:N) ต้องพิสูจน์	ยังไม่ถึงขั้นมีเสถียรภาพ	ยังไม่ถึงขั้นมีเสถียรภาพ
(6) ความเป็นที่ยอมรับของผู้ใช้	ดีมาก ผู้ใช้ยอมรับ ไม่ต้องสัมผัส	ดี ผู้ใช้บางประเทศไม่ยอมรับ ส่วนใหญ่ต้องสัมผัส ซึ่งอาจแพร่โรคได้	ดี แต่ผู้ใช้จำกัดการยอมรับ เนื่องจากต้องใช้แสง NIR ส่องเข้าดวงตา	ดี แต่บางอุปกรณ์ต้องสัมผัส	ผู้ใช้ยอมรับ แต่การใช้งาน ยังไม่ได้ใช้ระบบอัตโนมัติ แต่ใช้คนช่วยพิจารณา	ผู้ใช้ยอมรับ แต่การใช้งานยังคงจำกัด
(7) การปลอมแปลงได้ยาก	ปลอมแปลงได้โดยการผ่าตัด เปลี่ยนแปลง หรือการโจมตี ด้วยหน้ากาก	ปลอมแปลงได้ง่าย ใช้ลายนิ้วมือปลอม หรือ ทำลายลายนิ้วมือไม่ให้ ตรวจจับได้	ปลอมแปลงได้จากการใช้ Contact Len แต่เปลี่ยนแปลงยาก เนื่องจาก เกี่ยวกับอวัยวะที่สำคัญ	ปลอมแปลงได้ยากมาก เนื่องจากเป็นส่วนที่อยู่ภายใต้ ในผิวหนัง	สามารถปลอมแปลงได้	สามารถปลอมแปลงได้โดยใช้ เทคโนโลยี AI
จุดเด่น	ราคาถูก สามารถใช้งานระยะไกล	ราคาถูก นิยมใช้งานมากที่สุด ลายนิ้วมือทั้ง 10 นิ้ว ยากที่จะเหมือนกับอีกบุคคล	มีอัตลักษณ์แตกต่างกันมาก ทั้งสองม่านตา ความแม่นยำสูงมาก 1:N เร็วมาก	อวัยวะภายในยากแก่ การปลอมแปลง และสามารถ ตรวจจับความมีชีวิต ไปด้วยพร้อมกัน	เป็นที่ยอมรับในวงกว้าง ใช้กันมานาน และยังใช้กันอยู่ อย่างแพร่หลายในปัจจุบัน	ใช้งานระยะไกล ผ่านระบบโทรศัพท์ได้ สะดวก
ข้อจำกัด	แสง มุมของใบหน้า เปลี่ยน ตามอารมณ์ แว่นกันแดด ผ้าคลุมหน้า และปัญหา ฝาแฝดร่วมไข่หรือพี่น้อง	สภาพผิวหนัง การวางนิ้ว เสี่ยงต่อการติดเชื้อโรค จากการสัมผัส ตัวเซนเซอร์สกปรก	การเก็บม่านตายาก ขนตา แสง แสงสะท้อน แว่นตาและ คอนแทคเลนส์แบบแฟชั่น	มุมการวางอวัยวะที่ใช้เส้นเลือด อุปกรณ์อาจต้องสัมผัส ส่วนใหญ่ใช้แบบ 1:1	ระบบอัตโนมัติยังไม่น่าเชื่อถือ เท่ากับการใช้คน ความหลากหลายของลายเซ็น ของคนคนเดียวกัน	เทคโนโลยี AI สามารถปลอมเสียงได้และ สามารถให้พูดอะไรก็ได้

การนำเทคโนโลยีไบโอเมตริกไปประยุกต์ใช้งานนั้น ต้องคำนึงถึงคุณสมบัติทั้ง 7 ประการของไบโอเมตริก จากตารางที่ 8 สามารถสรุปลักษณะเฉพาะของไบโอเมตริกต่าง ๆ ที่ใช้กันอยู่ในปัจจุบันได้ว่า ไม่มีลักษณะเฉพาะไบโอเมตริกใดที่มีคุณสมบัติครบสมบูรณ์แบบ ทางเลือกคือต้องใช้ลักษณะเฉพาะไบโอเมตริกแบบผสมผสาน (Biometric Fusion) หรือไบโอเมตริกหลายโมเดล (Multi-model Biometric) ด้วยเหตุผลดังต่อไปนี้

1) เพื่อชดเชยคุณสมบัติที่ยังขาดหรือมีปัญหาของลักษณะเฉพาะไบโอเมตริกอย่างใดอย่างหนึ่งเพียงอย่างเดียว อาทิเช่น การใช้การรู้จำใบหน้า มีปัญหาเรื่องใบหน้าเปลี่ยนแปลงตามอายุ สีหน้าตามอารมณ์ หรือการศัลยกรรม ถ้าใช้ลายนิ้วมือประกอบ จะแก้ไขชดเชยปัญหาต่าง ๆ เหล่านี้ได้
2) เพื่อเพิ่มความแม่นยำของระบบ ให้สามารถยืนยันตัวบุคคล หรือ ระบุตัวบุคคลได้ถูกต้องแม่นยำยิ่งขึ้น
3) เพื่อป้องกันการโจมตีและการปลอมแปลง การมีลักษณะเฉพาะไบโอเมตริกหลายชนิด ทำให้ยากแก่การปลอมแปลง ผู้โจมตีจะต้องมีข้อมูลไบโอเมตริกหลายชนิดเพื่อที่จะโจมตีระบบ ซึ่งไบโอเมตริกบางอย่างยากที่จะได้มา เช่น ลายเส้นเลือด เป็นต้น

การที่จะทำให้ระบบไบโอเมตริกสมบูรณ์นั้น จะต้องประกอบด้วยคุณลักษณะไบโอเมตริกอย่างน้อยสองชนิดขึ้นไป ตัวอย่างเช่น Aadhaar ของประเทศอินเดียใช้คุณลักษณะไบโอเมตริกถึงสามชนิดคือ ใบหน้า ม่านตา และลายนิ้วมือ แต่จากการศึกษาพบว่าจะใช้ลายนิ้วมือเป็นหลักในการยืนยันตัวบุคคล เนื่องจากมีความแม่นยำและมีปัญหาน้อยกว่าใบหน้า ส่วนม่านตานั้น เนื่องจากเครื่องสแกนราคาแพง จึงมีจุดใช้งานที่จำกัด

ข้อเสียของการใช้ลักษณะเฉพาะไบโอเมตริกแบบผสมผสาน คือ

1) ระบบมีค่าใช้จ่ายสูง เนื่องจากมีหลายระบบไบโอเมตริก รวมทั้งค่าใช้จ่ายในการดูแลรักษาระบบเพิ่มขึ้นตามไปด้วย
2) การเก็บข้อมูลไบโอเมตริกหลายโมเดล ทำให้ยุ่งยากและซับซ้อน และมีค่าใช้จ่ายสูง ต้องมีเซนเซอร์หลายแบบ และถ้าเซนเซอร์ราคาแตกต่างกัน ทำให้จำกัดการใช้งาน
3) ต้องแก้ปัญหาถ้าระบบไบโอเมตริกให้ผลที่ขัดแย้งกัน จะต้องใช้มนุษย์มาช่วยในการตัดสินใจ คิดคะแนนความเหมือนสำหรับการยืนยันตัวบุคคลและการระบุตัวบุคคลมีความซับซ้อน

ดังนั้น การพิจารณาใช้เทคโนโลยีไบโอเมตริกมาช่วยในการประยุกต์ใช้งานต่าง ๆ นั้น ต้องคำนึงถึงข้อดี ข้อเสีย ข้อจำกัดหรืออุปสรรคต่าง ๆ ของแต่ละเทคโนโลยีไบโอเมตริก แต่เนื่องจากงานวิจัยทางด้านไบโอเมตริกยังคงก้าวหน้าต่อไปอย่างไม่หยุดยั้ง ทำให้ปัญหาต่าง ๆ ที่เกิดขึ้นในปัจจุบันอาจไม่เป็นปัญหาในอนาคต เนื่องจากเกิดแนวทางการแก้ปัญหาแบบใหม่ ๆ ตามเทคโนโลยีที่เกิดขึ้น และตามความก้าวหน้าของมนุษยชาติ

บทที่ 2

ตัวอย่างการใช้งาน (USED CASES)

บทที่ 2. ตัวอย่างการใช้งาน (Used Cases)

การนำเทคโนโลยีไบโอเมตริกไปประยุกต์ใช้งานนั้นมีความหลากหลายดังที่ได้กล่าวมาแล้วในบทที่ 1 ซึ่งได้กล่าวในแนวทางการนำลักษณะเฉพาะไบโอเมตริกแต่ละชนิดไปประยุกต์ใช้งานที่เหมาะสม สำหรับบทนี้จะเน้นถึงการนำเทคโนโลยีไบโอเมตริกไปประยุกต์ใช้งานสำหรับการยืนยันตัวตน ซึ่งได้มีหลายประเทศต่าง ๆ ในโลกที่นำไปประยุกต์ใช้งาน สำหรับบทนี้ จะเน้นระบบการยืนยันตัวตนที่มีขนาดใหญ่ และประยุกต์ใช้กับคนจำนวนมาก เช่น โครงการ Aadhaar ในประเทศอินเดีย โครงการ National ID ในประเทศออสเตรเลีย โครงการ Schengen ในกลุ่มประเทศสหภาพยุโรป

2.1 โครงการ Aadhaar ในประเทศอินเดีย

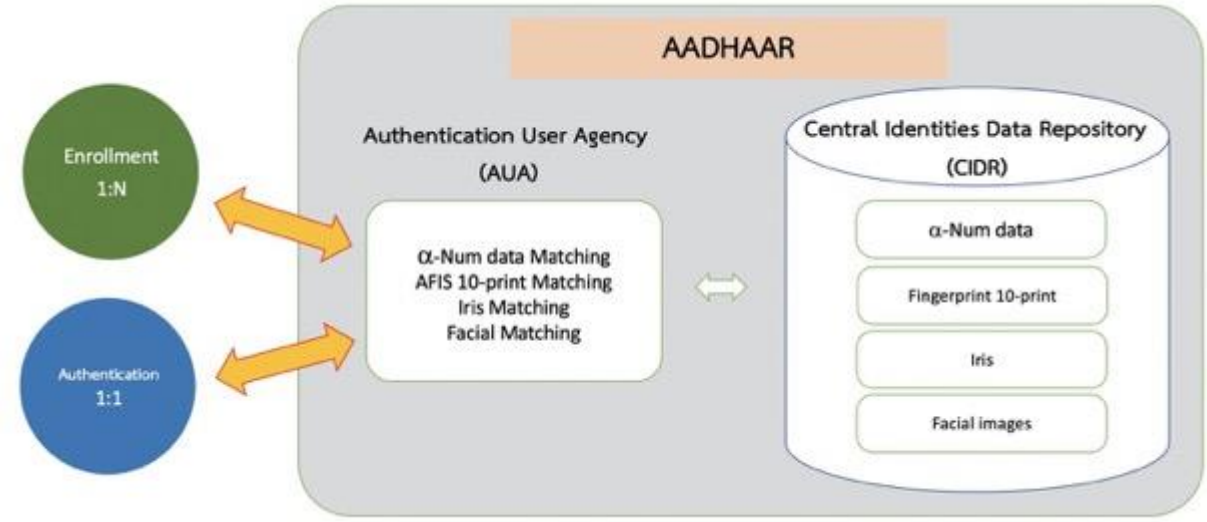
โครงการ Aadhaar เป็นโครงการที่รวบรวมข้อมูลไบโอเมตริกประชาชนที่มีขนาดใหญ่ที่สุดของโลก โดยอยู่ที่ประมาณ 1.4 พันล้านคน จัดทำโดย Unique Identification Authority of India (UIDAI) โดยโครงการนี้เริ่มต้นจากปัญหาของประเทศที่ประชาชนเกือบสองในสามของอินเดียไม่มีบัญชีธนาคาร เนื่องจากประชาชนส่วนใหญ่ขาดเอกสารแสดงตัวตน และการเข้าถึงธนาคารเป็นเรื่องยากเพราะธนาคารมีสาขาไม่เพียงพอ ธนาคารในประเทศอินเดียมี 83,997 สาขา แต่มีเพียง 32,289 สาขาเท่านั้นที่อยู่ในชนบท ซึ่งไม่เพียงพอสำหรับหมู่บ้านกว่า 600,000 หมู่บ้าน [อินเดียแอดฮาร์2561][19]

โครงการ Aadhaar จึงเกิดขึ้นด้วยความร่วมมือระหว่างหน่วยงาน UIDAI และธนาคารภายในประเทศอินเดีย เพื่อทำให้ Aadhaar เป็นอีกหนึ่งเอกสารที่สำคัญที่สามารถใช้ในการเปิดบัญชี และใช้บริการต่าง ๆ จากธนาคาร นอกจากนี้ยังเป็นโอกาสในการแก้ปัญหาทางการเงินสำหรับสถาบันอื่น ๆ เช่น การเสียภาษีเงินได้ การจดทะเบียนซิมโทรศัพท์ การชำระค่าสาธารณูปโภค การมอบทุนการศึกษา หรือการรับสวัสดิการจากภาครัฐ เป็นต้น โดยรายละเอียดข้อมูลต่าง ๆ ในการลงทะเบียนและการเริ่มใช้ในระบบแบบออนไลน์ของ Aadhaar ได้แสดงไว้ในตารางที่ 9 ซึ่งฐานข้อมูลทั้งหมดนี้จะถูกจัดเก็บ รักษาความปลอดภัยและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้ในทางที่ผิดกฎหมายโดย Central Identities Data Repository (CIDR) และรับรองความถูกต้องในการยืนยันตัวตนโดยหน่วยงาน Authentication User Agency (AUA) ภายใต้การดูแลของ UIDAI ดังภาพที่ 53

ตารางที่ 9 ข้อมูลที่เก็บรวบรวมในระบบ Aadhaar [Aadhaar2020]

	ข้อมูล	อธิบายข้อมูลที่เก็บ	เวลาที่เริ่มเก็บ
1	หมายเลข Aadhaar ID	หมายเลข 12 หลัก ไม่ซ้ำกัน	กันยายน พ.ศ. 2553
2	Proof of Identity (PoI)	ชื่อ นามสกุล เพศ	กันยายน พ.ศ. 2553
3	Proof of Address (PoA)	ที่อยู่	กันยายน พ.ศ. 2553
4	Proof of Date of Birth (PoDoB)	วัน เดือน ปี เกิด	กันยายน พ.ศ. 2553
5	(Option)	หมายเลขโทรศัพท์, email	กันยายน พ.ศ. 2553
6	ไบโอเมตริก (หลัก) Fingerprint	ลายนิ้วมือ 10 นิ้ว	กุมภาพันธ์ พ.ศ. 2555
7	ไบโอเมตริก (รอง) Face	ภาพใบหน้า หน้าตรง	กุมภาพันธ์ พ.ศ. 2555
8	ไบโอเมตริก (หลักเพิ่ม) Irises	ภาพลายม่านตา 2 ข้าง	พฤษภาคม พ.ศ. 2556
9	ระบบ One Time Password (OTP)	ใช้สำหรับยืนยันผ่านอุปกรณ์สื่อสาร	พฤษภาคม พ.ศ. 2556

[19]https://www.ditp.go.th/contents_attach/220375/220375.pdf



ภาพที่ 53 โครงสร้างการทำงานของระบบ Aadhaar ของประเทศอินเดีย (ภาพจาก [Aadhaar2020])

ภาพที่ 54 ตัวอย่างลักษณะบัตร Aadhaar ของประเทศอินเดีย
(ภาพได้รับอนุญาตจาก Prof. Anil K. Jain, Michigan State University, USA)

ภาพที่ 55 ตัวอย่างการลงทะเบียนระบบ Aadhaar ของประเทศอินเดียและข้อมูลไบโอเมตริกที่เก็บ
(ภาพได้รับอนุญาตจาก Prof. Anil K. Jain, Michigan State University, USA)

เป้าหมายของโครงการ Aadhaar มีเป้าหมายดังต่อไปนี้

1) เพื่อพิสูจน์ว่าคนคนนั้นมีตัวตนอยู่จริง
2) เพื่อสร้างเครื่องมือที่สามารถยืนยันตัวบุคคล และระบุตัวบุคคลของแต่ละคนได้ และสามารถใช้งานจริงได้ทุกที่
3) เพื่อใช้เทคโนโลยีในการสร้างเลขประจำตัวประชาชนหรือ National ID ที่สามารถเชื่อมต่อเข้าถึงกับการบริการจากภาครัฐและเอกชน รวมถึงการมีสิทธิประโยชน์ส่วนบุคคลต่าง ๆ
4) เพื่อสร้างระบบเลขประจำตัวประชาชนที่ขับเคลื่อนโดยเทคโนโลยีใหม่ จะต้องเป็นมากกว่าการปฏิวัติวิธีที่จะจ่ายเงินสวัสดิการ และเงินสงเคราะห์ต่าง ๆ ได้

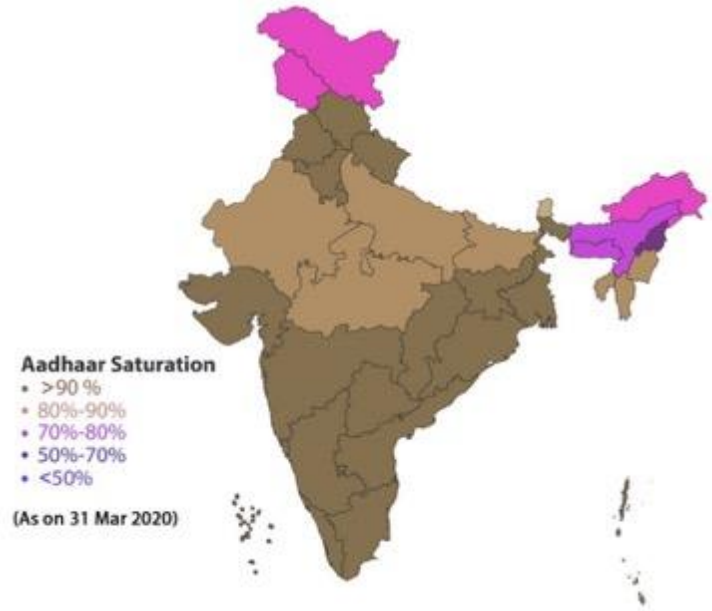
ผู้ที่สามารถลงทะเบียนในระบบ Aadhaar ได้แก่พลเมืองดังต่อไปนี้

1) พลเมืองผู้มีถิ่นฐานที่อยู่ในประเทศอินเดีย
2) ผู้ถือหนังสือเดินทางอินเดีย แม้ไม่ใช่ผู้มีถิ่นฐานที่อยู่ในประเทศอินเดีย
3) บุคคลต่างด้าวที่อยู่ในประเทศอินเดียมากกว่า 182 วัน

หมายเหตุ การลงทะเบียน Aadhaar ถือเป็นหลักฐานการพำนัก แต่ไม่ใช่หลักฐานการเป็นพลเมืองและไม่ได้ให้สิทธิ์ใด ๆ ในการมีภูมิลำเนาในประเทศอินเดีย

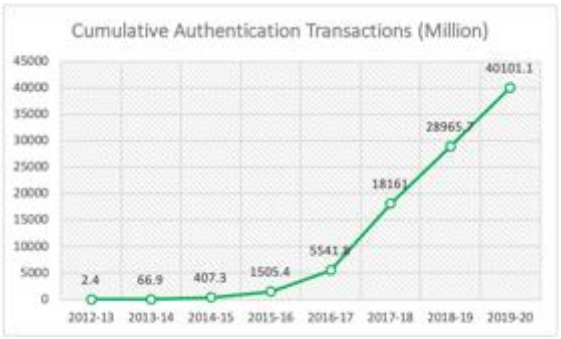
การลงทะเบียน Aadhaar จะใช้การตรวจสอบด้วยการระบุตัวตนด้วยไบโอเมตริกสองชนิด ได้แก่ ลายนิ้วมือ 10 นิ้ว และลายม่านตาสองข้าง (Fingerprint and Iris Identification (1:N)) เพื่อป้องกันการลงทะเบียนซ้ำซ้อนหรือการมี Aadhaar ID ซ้ำซ้อน ซึ่งไม่ต้องการให้มีกรณีนี้เกิดขึ้น

ปัจจุบันประชากรในประเทศอินเดีย มีการลงทะเบียนในระบบ Aadhaar ครอบคลุมเกือบทั้งประเทศ ภาพที่ 56 แสดงสถานะการลงทะเบียนระบบ Aadhaar แต่ละรัฐในประเทศอินเดีย โดยมี 22 รัฐที่มีประชากรลงทะเบียนแล้วมากกว่า 90 เปอร์เซ็นต์ มี 11 รัฐที่มีประชากรลงทะเบียนระหว่าง 70 ถึง 90 เปอร์เซ็นต์ และมีเพียง 3 รัฐที่ยังมีการลงทะเบียนน้อยกว่า 70 เปอร์เซ็นต์ (ข้อมูล ณ วันที่ 31 มีนาคม พ.ศ. 2563) [Aadhaar2020] ปัจจุบันมีศูนย์รับลงทะเบียนและอัปเดตข้อมูล Aadhaar เช่น ธนาคาร ที่ทำการไปรษณีย์ หน่วยงานของรัฐต่าง ๆ มากกว่า 40,000 แห่งทั่วประเทศ และเนื่องจากประชากรในหลายรัฐได้มีการลงทะเบียนในระบบ Aadhaar จนครบถ้วนแล้ว ทำให้ภาครัฐได้เปลี่ยนนโยบายมาเป็นการลงทะเบียนให้แก่เด็กที่มีอายุ 5 ถึง 18 ปี และเด็กอายุต่ำกว่า 5 ปี ตามลำดับ โดยเด็กอายุต่ำกว่า 5 ปี จะมีการบันทึกเฉพาะชื่อ นามสกุล เพศ และภาพใบหน้าของเด็กเท่านั้น โดยอ้างอิงหมายเลข Aadhaar ของผู้ปกครองคนใดคนหนึ่ง



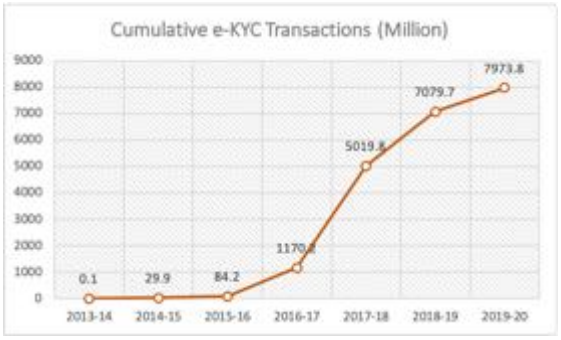
ภาพที่ 56 แสดงสถานะการลงทะเบียนระบบ Aadhaar แต่ละรัฐในประเทศอินเดีย (ภาพจาก [Aadhaar2020])

ตั้งแต่ก่อตั้งหน่วยงาน Authentication User Agency (AUA) มีรายการขอยืนยันตัวตน (Verification) ซึ่งแสดงผลลัพธ์เป็น **“ใช่/ไม่ใช่”** เท่านั้น โดยใช้ในการรับรองการตรวจสอบสิทธิ์ต่าง ๆ แล้วประมาณ 40,101.1 ล้านรายการ (ณ วันที่ 31 มีนาคม พ.ศ. 2563) [Aadhaar2020] สถิติจำนวนครั้งในการยืนยันตัวบุคคลแบบรายปี และแบบสะสมในช่วงตั้งแต่ปี 2012-2020 แสดงไว้ในรูปแบบกราฟในภาพที่ 57 (ก) และ (ข) ตามลำดับ และมีจำนวนรายการในการยืนยันตัวบุคคลเฉพาะการทำธุรกรรมด้านการเงิน e-KYC (Electronic Know Your Customer) แล้วประมาณ 7,973.8 ล้านรายการ (ณ วันที่ 31 มีนาคม พ.ศ. 2563) แจกแจงเป็นแบบรายปีและแบบสะสมในช่วงตั้งแต่ปี พ.ศ. 2555-2563 (ค.ศ. 2012-2020) ได้ดังกราฟในภาพที่ 58 (ก) และ (ข) ตามลำดับ



(ก) แบบรายปี (ข) แบบสะสม

ภาพที่ 57 สถิติจำนวนครั้งในการยืนยันตัวบุคคลในช่วงตั้งแต่ปี 2012-2020 (ภาพจาก [Aadhaar2020])



(ก) แบบรายปี (ข) แบบสะสม

ภาพที่ 58 สถิติจำนวนครั้งในการยืนยันตัวบุคคลเฉพาะการทำธุรกรรมด้านการเงิน Electronic Know Your Customer e-KYC ในช่วงตั้งแต่ปี 2012-2020 (ภาพจาก [Aadhaar2020])

ปัญหาและอุปสรรคของโครงการ Aadhaar มีดังต่อไปนี้

1) ค่าใช้จ่ายในการรวบรวมข้อมูลสูง (เก็บเฉพาะ ชื่อ อายุ เพศ และที่อยู่ที่ติดต่อได้)
2) ปัญหาการทำงานระหว่างรัฐบาลและเอกชน
3) ปัญหาด้านการเก็บภาพลายนิ้วมือ เนื่องจากประชาชนเป็นผู้ใช้แรงงานจำนวนมาก ซึ่งการทำงานหนักทำให้ลายนิ้วมือหาย ไม่สามารถเก็บภาพลายนิ้วมือได้
4) ปัญหาด้านการเก็บภาพลายม่านตา เครื่องอ่านมีราคาแพงต้องสั่งซื้อในปริมาณมากเพื่อให้ได้ราคาที่ถูกลง
5) ปัญหาทางสังคม มีการต่อต้านจากประชาชนบางส่วน เนื่องจากไม่เห็นความจำเป็นในการลงทะเบียน

2.2 โครงการ National ID ในประเทศออสเตรเลีย

Digital Transformation Agency (DTA) เป็นหน่วยงานภาครัฐที่ทำหน้าที่เกี่ยวกับการพิสูจน์ยืนยันและการระบุตัวตนดิจิทัลภายในประเทศออสเตรเลีย ได้เปิดใช้แอปพลิเคชัน (Application) สำหรับสมาร์ทโฟนที่ใช้ชื่อว่า myGov ID ซึ่งพัฒนาโดยสำนักงานสรรพากรของประเทศออสเตรเลีย เพื่อให้บริการจากภาครัฐ ได้แก่ การชำระเงินสวัสดิการสังคม (Centrelink) การดูแลสุขภาพ (Medicare) การคืนภาษีออนไลน์จากสำนักงานสรรพากรออสเตรเลีย การสนับสนุนเด็ก โครงการประกันความทุพพลภาพแห่งชาติ การดูแลผู้สูงอายุ การดูแลทหารผ่านศึก สิ่งอำนวยความสะดวกออนไลน์ และเครือข่ายค้นหางานทำของรัฐบาล นอกจากนี้ myGov ID ยังมีการผสานความร่วมมือกับหน่วยงานอื่น เช่น Australian Post Digital ID เพื่ออำนวยความสะดวกในด้านการจัดส่งเอกสารอิเล็กทรอนิกส์ หลีกเลี่ยงการใช้อีเมลจากหน่วยงานรัฐติดต่อหรือส่งเอกสารส่วนตัวกับผู้ใช้บริการโดยตรง[20]

การลงทะเบียนของแอปพลิเคชัน myGov ID และ Australian Post Digital ID มีรูปแบบการยืนยันตัวตนที่เหมือนกัน โดยมีจุดเด่นคือ ผู้ใช้สามารถทำได้เองแบบออนไลน์ ปลอดภัย ไม่ต้องส่งเอกสารใด ๆ และยังได้รับการรับรองความถูกต้องจากรัฐบาลออสเตรเลีย โดยจะขอยกตัวอย่างขั้นตอนการลงทะเบียนเฉพาะแอปพลิเคชัน myGov ID ดังนี้

1) ผู้ขอรับบริการสามารถดาวน์โหลดแอป myGovID ได้ทาง GooglePlay หรือทาง AppStore
2) กรอกรายละเอียดข้อมูลส่วนตัว ชื่อนามสกุล วันเกิด และที่อยู่ อีเมลส่วนตัว ตามที่แอปพลิเคชันกำหนด
3) ผู้ใช้สามารถเลือกรูปแบบการยืนยันตัวตนเพื่อความปลอดภัยในการเข้าถึงได้ 3 ระดับ ได้แก่
   3.1) **Basic** กรอกข้อมูลส่วนตัว
   3.2) **Standard** ยืนยันตัวตนด้วยการตรวจสอบเอกสารราชการแบบเรียลไทม์ โดยผู้ใช้สามารถใช้ใบขับขี่ออสเตรเลีย (Australia Driver's License) หรือหนังสือเดินทางออสเตรเลีย (Australia Passport) ดังภาพที่ 59 หรือ บัตรสุขภาพออสเตรเลีย (Australia Medicare Card) โดยการแตะบัตรไว้หลังโทรศัพท์มือถือเพื่ออ่านข้อมูลและภาพถ่ายภายในบัตร โดยใช้เทคโนโลยีการสื่อสารแบบ Near-Field Communication (NFC) ซึ่งมีเฉพาะสมาร์ทโฟนบางรุ่นเท่านั้น

ภาพที่ 59 ภาพตัวอย่างใบขับขี่และหนังสือเดินทางประเทศออสเตรเลีย

   3.3) **Strong** ยืนยันตัวตนด้วยไบโอเมตริก โดยแอปพลิเคชันจะให้ผู้ใช้ถ่ายรูปตนเอง และเคลื่อนไหวใบหน้าตามที่กำหนด เพื่อป้องกันการสวมรอยปลอมตัวตน ภาพถ่ายที่ได้จะถูกนำมาพิสูจน์ตัวตนกับภาพใบหน้าที่อ่านจากเอกสารราชการที่กล่าวถึงก่อนหน้าเพื่อยืนยันตัวตน

หมายเหตุ การยืนยันตัวตนแต่ละแบบจะสามารถเข้าถึงการใช้บริการต่าง ๆ ได้แตกต่างกัน ผู้ใช้บริการต้องมีอายุ 15 ปีขึ้นไป

[20] www.myGovID.gov.au

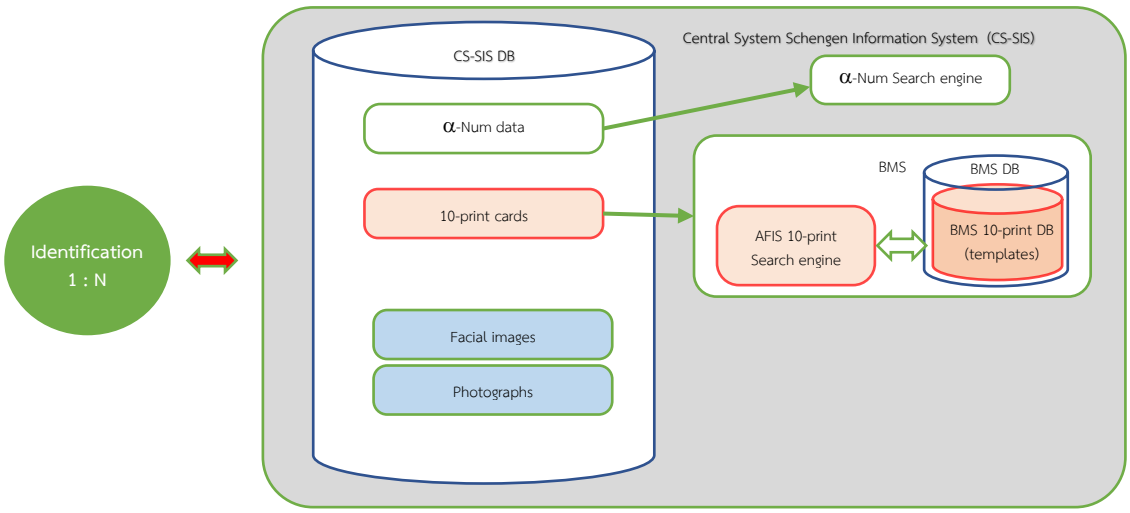
2.3 โครงการ Schengen ในกลุ่มประเทศสหภาพยุโรป

Schengen Information System (SIS) คือ ระบบข้อมูลที่ใช้กันอย่างแพร่หลายและใหญ่ที่สุดในกลุ่มประเทศสมาชิกสหภาพยุโรป โดยมี 2 วัตถุประสงค์หลัก ได้แก่ (1) การบังคับใช้กฎหมาย และ (2) การจัดการชายแดนในยุโรป ระบบมีหน้าที่แบ่งปันข้อมูลแบบเรียลไทม์ ให้แก่หน่วยงานด้านความปลอดภัยระดับชาติที่มีอำนาจควบคุม เช่น ตำรวจ เจ้าหน้าที่ตรวจคนเข้าเมือง และระบบแจ้งเตือนบุคคลหรือวัตถุอื่นที่เกี่ยวข้อง เช่น สมาชิกสหภาพยุโรปทั้ง 26 ประเทศ (Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden และ Switzerland) สำนักงานแจ้งเตือนสหภาพยุโรป SIRENE bureau, EU Agency for large-scale IT systems (eu-LISA) เป็นต้น ซึ่งรูปแบบข้อมูลมีรายละเอียดประกอบด้วย 3 ส่วน ดังนี้

1) ชุดข้อมูลสำหรับระบุตัวบุคคลหรือวัตถุ และหัวข้อการแจ้งเตือน
2) คำชี้แจงว่าทำไมบุคคลหรือวัตถุจึงต้องถูกค้นหา
3) คำแนะนำในการดำเนินการเมื่อพบบุคคลหรือวัตถุ

Schengen Information System (SIS) เริ่มก่อตั้งในปี พ.ศ. 2538 ซึ่งเป็นระบบไอทีขนาดใหญ่ระบบแรกในสหภาพยุโรป ตามด้วยระบบจัดเก็บฐานข้อมูลผู้ขอลี้ภัย (EURODAC) ในปี พ.ศ. 2546 และระบบข้อมูลวีซ่า (VIS) ในปี พ.ศ. 2554 ต่อมาได้เริ่มจัดทำระบบข้อมูลรวมศูนย์ Central Schengen Information System (CS-SIS) นอกจากเก็บข้อมูลที่เป็นตัวอักษรและตัวเลขแล้ว ยังเพิ่มการจัดเก็บข้อมูลไบโอเมตริก เพื่อการแจ้งเตือนที่เกี่ยวข้องกับการระบุตัวตน เช่น การเก็บภาพลายนิ้วมือและภาพใบหน้าของผู้รับการแจ้งเตือน อย่างไรก็ตาม ในช่วงเวลานั้นความแม่นยำเทคโนโลยีในการค้นหาฐานข้อมูลเพื่อระบุตัวบุคคลยังไม่สามารถใช้งานได้ การค้นหาทั้งหมดจึงดำเนินการในรูปแบบการยืนยันตัวบุคคล (Verification) โดยใช้ข้อมูลตัวอักษรและตัวเลข และยืนยันตัวตนด้วยลายนิ้วมือและภาพใบหน้า

ในปี พ.ศ. 2555 คณะกรรมาธิการได้นำเสนอ รายงานเกี่ยวกับความพร้อมใช้งานและความพร้อมของเทคโนโลยีที่จำเป็นซึ่งจะมีการปรึกษารัฐสภายุโรป (A Report on the Availability and Readiness of the Required Technology on which the European Parliament is Consulted)" [Galbally2019] ได้ตัดสินใจใช้ระบบระบุลายนิ้วมืออัตโนมัติ (AFIS) 10 นิ้วเพื่อระบุตัวบุคคล (Fingerprint Identification) ภายในระบบ CS-SIS



ภาพที่ 60 โครงสร้างการเก็บข้อมูลและการประมวลผลของระบบ CS-SIS ในช่วงแรก (ภาพดัดแปลงจาก [Galbally2019])

ภาพที่ 60 แสดงโครงสร้างการประมวลผลและการจัดเก็บฐานข้อมูลของระบบการแจ้งเตือน CS-SIS ในช่วงแรก เป็นการระบุตัวตนด้วยภาพลายนิ้วมือ 10 นิ้ว ได้แก่ มีโครงสร้างแบ่งออกเป็น 3 ส่วน ประกอบด้วย

1) **CS-SIS DB** คือ ส่วนฐานข้อมูลจัดเก็บการแจ้งเตือนด้วยข้อมูลภาพไบโอเมตริกประกอบด้วยภาพลายนิ้วมือต้นฉบับและภาพใบหน้าต้นฉบับ และฐานข้อมูลประเภทตัวอักษรและตัวเลขที่มีการแจ้งเตือน
2) **α-num Search Engine** คือ ส่วนระบบค้นหาข้อมูลประเภทตัวอักษรและตัวเลข

3) **Biometric Matching System (BMS)** คือ ส่วนระบบจับคู่ไบโอเมตริก ซึ่งมี 2 ส่วนย่อยภายใน ได้แก่
   3.1) **ฐานข้อมูล**: ภาพลายนิ้วมือ 10 นิ้ว เฉพาะเทมเพลต (10-print Template DB)
   3.2) **ระบบการระบุตัวตนด้วยไบโอเมตริก**: ระบบการระบุตัวตนด้วยภาพลายนิ้วมือ 10 นิ้ว (AFIS 10-print Search Engine) ในขณะนั้นยังไม่มีการดึงหรือจัดเก็บเทมเพลตจากภาพใบหน้าเนื่องจากข้อบังคับยังไม่อนุญาตให้ใช้ภาพใบหน้าเพื่อระบุตัวตน

ข้อสังเกต รูปแบบโครงสร้างนี้ออกแบบ เพื่อทำให้สามารถเปลี่ยนแปลงผู้ให้บริการระบบระบุตัวตนรายใหม่ได้ โดย BMS สามารถดึงข้อมูลภาพลายนิ้วมือต้นฉบับทั้งหมดกลับจากฐานข้อมูล CS-SIS DB เพื่อสกัดลักษณะเฉพาะและสร้างเทมเพลตด้วยระบบใหม่ได้อีกครั้ง

ในทางปฏิบัติ ผลการจับคู่ไบโอเมตริกจะมี 2 ระดับ คือ

1) **Match** แสดงการจับคู่ที่ได้จากระบบการรู้จำไบโอเมตริกอัตโนมัติ
2) **Hit** แสดงการยืนยันข้อมูลไบโอเมตริกที่ match ได้โดยผู้เชี่ยวชาญ และประกาศแจ้งเตือนบุคคลต้องสงสัย

ต่อมา SIS ได้มอบหมายให้ Joint Research Centre (JRC) [21] ซึ่งเป็นหน่วยงานที่รวบรวมนักวิทยาศาสตร์ให้บริการทางด้านความรู้เพื่อให้คำแนะนำที่เป็นอิสระและสนับสนุนนโยบาย EU เริ่มศึกษาความเป็นไปได้และข้อจำกัดต่าง ๆ เพื่อเตรียมความพร้อมในการใช้ระบบไบโอเมตริกเพื่อระบุตัวตนอัตโนมัติ (Automated Biometric Identification System (ABIS)) กับโครงการ SIS ในปี พ.ศ. 2558 โดยได้ข้อสรุปว่า เทคโนโลยีการรู้จำใบหน้าได้มีการพัฒนาความแม่นยำเพิ่มขึ้นอย่างมากนับตั้งแต่ปี พ.ศ. 2553 (ค.ศ. 2010) ซึ่งเกิดจากการพัฒนาระบบด้วยการเรียนรู้เชิงลึก ตามที่ได้กล่าวไว้ในบทที่ 1.1 จึงเป็นบทสรุปของการศึกษาในปัจจุบันว่า ประสิทธิภาพระบบ ABIS-Face ได้มาถึงระดับที่พร้อมใช้งานร่วมกับระบบ CS-SIS โดยที่ JRC มีข้อเสนอแนะที่สำคัญดังต่อไปนี้

1) ระบบการรู้จำภาพใบหน้าควรแยกฐานข้อมูลภาพใบหน้าออกเป็น 2 ประเภท คือ (1) ภาพบุคคลหน้าตรง และ (2) ภาพใบหน้าอื่น ๆ ซึ่งจะเพิ่มความแม่นยำและความเร็วในการรู้จำภาพใบหน้าได้มากขึ้น
2) ควรใช้ระบบค้นหาภาพใบหน้า ABIS-Face เพียงระบบเดียว เนื่องจากเทคโนโลยีการเรียนรู้เชิงลึกเพื่อรู้จำภาพใบหน้า ควรถูกฝึกสอนด้วยชุดข้อมูลภาพร่วมกัน ซึ่งประกอบด้วย ภาพบุคคลหน้าตรง และภาพใบหน้าอื่น ๆ เพื่อป้องกันปัญหาระบบมีการเรียนรู้ให้เข้ากับภาพเฉพาะในฐานข้อมูล (Overfitting) ยกตัวอย่างเช่น หากภาพที่ใช้ในการเปรียบเทียบแตกต่างจากภาพที่ระบบคาดไว้เล็กน้อย ความแม่นยำจะลดลงอย่างมาก ซึ่งจะทำให้ระบบไม่สามารถทำงานในกรณีที่จำเป็นต้องเปรียบเทียบระหว่างภาพบุคคลหน้าตรงกับภาพใบหน้าอื่น ๆ
3) ควรมีการศึกษาผลกระทบจากระหว่างกลุ่มอายุต่าง ๆ อาทิเช่น เด็ก ผู้ใหญ่ ผู้สูงอายุ ที่มีผลต่อความแม่นยำของระบบการรู้จำใบหน้า โดยมีงานวิจัยที่แสดงให้เห็นว่าความแม่นยำลดลงอย่างมากสำหรับเด็กอายุต่ำกว่า 13 ปี แม้ว่าผลลัพธ์เหล่านี้จะต้องได้รับการยืนยันเพิ่มเติม แต่ในทางปฏิบัติอาจมีการจำกัดอายุสำหรับการใช้เทคโนโลยีการรู้จำใบหน้า หรือต้องมีการพัฒนาอัลกอริทึมเพื่อรับมือกับปัญหานี้โดยเฉพาะ นอกเหนือจากนี้ระบบควรมีการแจ้งเตือนให้อัปเดตภาพใบหน้าล่าสุดทุกครั้งเพื่อลดผลกระทบจากอายุให้มากที่สุด เนื่องจากความแม่นยำของระบบรู้จำใบหน้าจะลดลงเนื่องจากระยะเวลาระหว่างการเก็บภาพใบหน้าทั้งสองที่จะมาเปรียบเทียบกันมีระยะเวลานานมากขึ้น โดยเฉพาะอย่างยิ่งในกรณีของเด็กซึ่งจะมีความแตกต่างได้อย่างมาก แม้ในช่วงเวลาสั้น ๆ ระบบรู้จำใบหน้าที่สามารถเปรียบเทียบได้โดยไม่มีผลต่ออายุจะมีประโยชน์อย่างมาก โดยเฉพาะอย่างยิ่งกรณีบุคคลสูญหาย
4) การสืบค้นบุคคลด้วยภาพใบหน้าควรใช้ภาพสด (Live Image) ที่บุคคลมาปรากฏตัวหน้ากล้องมากกว่าภาพใบหน้าจากภายในหนังสือเดินทาง เนื่องจากภาพถ่ายสดจะมีความละเอียดสูงกว่า และลดช่องโหว่การโจมตีระบบจากการปลอมแปลงหนังสือเดินทาง
5) การชี้วัดคุณภาพภาพใบหน้าเป็นสิ่งสำคัญมากในระบบการรู้จำ เพื่อช่วยเหลือเจ้าหน้าที่เนื่องจากความเหนื่อยล้าในการปฏิบัติงาน โดยเฉพาะอย่างยิ่งในกรณีประตูข้ามแดนอัตโนมัติ (Automatic Border Control (ABC)) ซึ่งไม่ต้องใช้เจ้าหน้าที่ ดังนั้นการชี้วัดคุณภาพภาพใบหน้าจึงควรมีความแม่นยำ ซึ่งอาจแสดงผล

[21] https://ec.europa.eu/info/departments/joint-research-centre_en

ในรูปแบบผลรวมจากค่าปัจจัยต่าง ๆ ที่มนุษย์กำหนดขึ้น เช่น การส่องสว่าง ความคมชัด ตำแหน่งที่จับภาพ พื้นหลัง ท่าทาง การแสดงออกทางสีหน้า แว่นตากันแดด ฯลฯ ข้อมูลเพิ่มเติมสามารถดูได้จากมาตรฐาน ISO/IEC 29794-5:2017 Information Technology – Biometric Sample Quality – Part 5 การแจ้งเตือนภาพใบหน้าที่มีคุณภาพต่ำทำให้ผู้ใช้หรือเจ้าหน้าที่ทราบและสามารถดำเนินการถ่ายภาพซ้ำได้ทันที

6) ในกรณีที่การทำงานมีข้อจำกัดด้านเวลา เช่น การข้ามพรมแดนเจ้าหน้าที่ตรวจคนเข้าเมืองควรใช้เวลาในการดำเนินการตรวจสอบตามระบบให้ครบถ้วนภายในไม่เกิน 30 วินาทีต่อคน ดังนั้น การแสดงรายการภาพใบหน้าบุคคลคล้ายจากระบบค้นหาจึงต้องพิจารณาเฉพาะรายการที่มีคะแนนความเหมือนสูงกว่าค่าระดับอ้างอิงของระบบ ABIS-Face เท่านั้น อาทิเช่น ค่าระดับอ้างอิงของภาพบุคคลหน้าตรง จะอยู่ที่ FPIR = 0.001% @ 1 ล้านข้อมูล

7) ในกรณีที่ต้องการเพิ่มความแม่นยำในการค้นหาภาพบุคคล เช่น การเปรียบเทียบภาพใบหน้าผู้ต้องสงสัยจากสถานีตำรวจ ซึ่งปราศจากข้อจำกัดด้านเวลา ระบบควรสามารถรองรับการใช้ภาพใบหน้าที่มุมเอียง เช่น +90, +45, -45 และ - 90 องศา เพื่อเพิ่มโอกาสในการค้นหาบุคคลผู้ต้องสงสัย

8) การนำเสนอปัญหาด้านความปลอดภัยด้านการโจมตีระบบแบบต่าง ๆ มีดังต่อไปนี้

8.1) การตรวจจับการโจมตีนำเสนอ (Presentation Attack Detection (PAD)) เป็นการโจมตีที่มุ่งการโจมตีเซนเซอร์รับข้อมูลของระบบซึ่งเป็นสองประเภท คือ

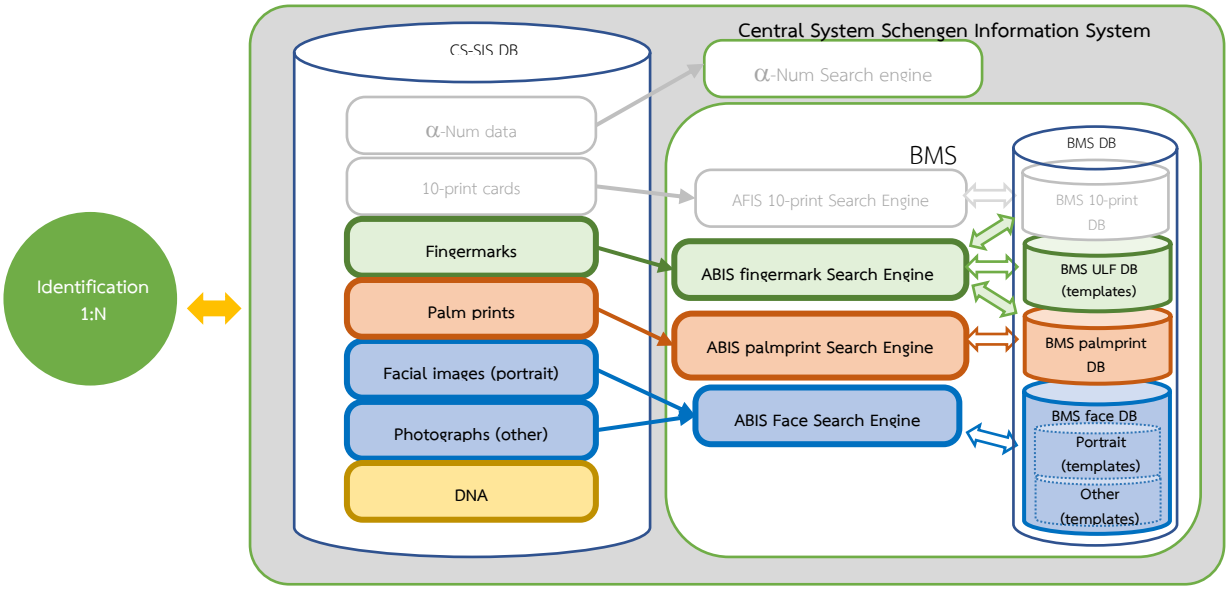
(1) การโจมตีเลียนแบบ มีวัตถุประสงค์เพื่อหลอกให้ระบบคิดว่าเป็นบุคคลเป้าหมาย ในกรณีนี้ผู้โจมตีจะใช้อุปกรณ์หรือแบบจำลองที่ประดิษฐ์ขึ้นเพื่อจำลองลักษณะเฉพาะไบโอเมตริกของบุคคลเป้าหมาย เพื่อให้สามารถเข้าถึงโดยมิชอบด้วยกฎหมาย เช่น การโจมตีด้วยการแต่งหน้า การโจมตีด้วยภาพถ่าย การโจมตีด้วยการฉายภาพวีดิทัศน์ หรือการโจมตีด้วยหน้ากาก

(2) การโจมตีแบบหลบหลีก เป็นความพยายามเพื่อซ่อนตัวตนไม่ให้เป็นที่รู้จัก กรณีนี้มักจะเกิดขึ้นกับการใช้ประตูข้ามแดนอัตโนมัติ (ABC) ซึ่งไม่มีเจ้าหน้าที่ควบคุม แนวทางการปฏิบัติสำหรับป้องกันการโจมตีประเภทนี้สามารถดูรายละเอียดเพิ่มเติมได้ในมาตรฐาน: ISO/IEC 30107-1:2017, Biometric Presentation Attack Detection

8.2) การตรวจจับการโจมตีการหลอมภาพ (Morphing Attack Detection) เมื่อเร็ว ๆ นี้ได้มีการนำเสนอปัญหาด้านความปลอดภัยเกี่ยวกับการดัดแปลงภาพที่เรียกว่า “การหลอมภาพ” (Morphing) เป็นวิธีการแปลงรูปแบบพิเศษที่มีจุดมุ่งหมาย เพื่อรวมภาพใบหน้าจริงของผู้ต้องการลักลอบเข้าระบบกับภาพใบหน้าจริงของบุคคลเป้าหมายเข้าด้วยกัน ซึ่งจะสร้างปัญหาให้กับระบบการรู้จำใบหน้า เนื่องจากภาพสังเคราะห์นี้จะไม่ใช่การระบุตัวตนบุคคลเพียงคน ๆ เดียว แต่กลับสามารถระบุตัวตนกับบุคคลสองคนที่แตกต่างกันได้ การโจมตีระบบประเภทนี้จะสามารถทำได้ในช่วงกระบวนการออกหนังสือเดินทาง ซึ่งในปัจจุบันยังมีหลายประเทศในยุโรปที่ยังกำหนดให้ผู้สมัครจัดเตรียมภาพถ่ายใบหน้ามา เพื่อสแกนเข้าระบบการจัดทำหนังสือเดินทางแบบดิจิทัล ดังนั้น จึงเป็นการเปิดช่องโหว่ให้ผู้สมัครสามารถใช้ภาพใบหน้าสังเคราะห์ที่เกิดจากการหลอม (Morphing) ลงทะเบียนระบบรู้จำใบหน้าได้ ข้อเสนอแนะเพื่อป้องกันการโจมตีประเภทนี้ คือ ควรใช้การลงทะเบียนโดยใช้ภาพสด (Live Image) จากกล้องภายใต้การดูแลของเจ้าหน้าที่ที่มีความชำนาญ

9) การประยุกต์ใช้ภาพใกล้อินฟราเรด (Near Infrared (NIR)) ซึ่งมักจะช่วยให้ภาพใบหน้าชัดเจนกว่าภาพที่ถ่ายด้วยแสงที่มีสเปกตรัมที่มนุษย์มองเห็น (Visual Spectrum (VIS)) กับระบบ CS-SIS ซึ่งภาพใบหน้าส่วนใหญ่จะเป็นภาพใบหน้าที่ถ่ายด้วยแสงที่มนุษย์มองเห็น ให้ระบุรหัสกำกับภาพสำหรับ NIR โดยเฉพาะและควรมีลำดับการสืบค้น ดังต่อไปนี้ (1) ค้นหาภาพด้วยภาพ VIS ให้เปรียบเทียบภาพ VIS-VIS (2) ค้นหาภาพด้วยภาพ NIR ให้เปรียบเทียบภาพ NIR-VIS และ (3) ค้นหาภาพด้วยภาพ NIR ให้เปรียบเทียบ NIR-NIR เป็นลำดับสุดท้าย

10) ยังไม่แนะนำให้รวมเทคโนโลยี 3D ของการรู้จำใบหน้าไว้ในระบบ CS-SIS เนื่องจากในปัจจุบันยังไม่สามารถปรับให้เข้ากับการใช้งานของระบบได้ อย่างไรก็ตาม เทคโนโลยี 3D สามารถนำไปใช้งานเพื่อตรวจจับการลักลอบเข้าระบบ โดยเฉพาะจุดที่ไม่มีเจ้าหน้าที่ดูแลได้ เช่น ประตูข้ามแดนอัตโนมัติ (ABC) ที่สนามบิน



ภาพที่ 61 โครงสร้างการเก็บข้อมูลและการประมวลผลของระบบ CS-SIS ในช่วงที่สอง (ภาพดัดแปลงจาก [Galbally2019])

ภาพที่ 61 แสดงโครงสร้างการประมวลผลและการจัดเก็บฐานข้อมูลของระบบ CS-SIS ในช่วงที่สอง เป็นการเพิ่มการระบุตัวตนด้วยภาพใบหน้า การระบุตัวตนด้วยภาพลายนิ้วมือแฝง ภาพลายฝ่ามือ และรหัสพันธุกรรม ซึ่งใช้ในการสืบสวนกรณีพิเศษ ได้แก่ มีการเปลี่ยนแปลงโครงสร้าง ดังนี้

1) **ส่วน CS-SIS DB**
   - **1.1)** แบ่งภาพฐานข้อมูลภาพใบหน้าออกเป็น 2 ส่วนได้แก่ (1) ฐานข้อมูลภาพใบหน้าตรง (Portrait) และ (2) ฐานข้อมูลภาพใบหน้าอื่น ๆ (Other)
   - **1.2)** เพิ่มการจัดเก็บฐานข้อมูลภาพลายนิ้วมือแฝงต้นฉบับ (Fingermark Image) ภาพลายฝ่ามือต้นฉบับ (Palmprint image) และฐานข้อมูลรหัสพันธุกรรม (DNA)
2) **ส่วนฐานข้อมูลของ Biometric Matching System (BMS) มีการเพิ่มเติมดังนี้**
   - **2.1)** ฐานข้อมูลภาพใบหน้าตรงเฉพาะเทมเพลต (BMS face DB: Portrait Template)
   - **2.2)** ฐานข้อมูลภาพใบหน้าอื่น ๆ เฉพาะเทมเพลต (BMS face DB: Other Template)
   - **2.3)** ฐานข้อมูลภาพลายนิ้วมือแฝงเฉพาะเทมเพลต (BMS Unsolved Latent Files DB: ULF Template)
   - **2.4)** ฐานข้อมูลภาพลายฝ่ามือเฉพาะเทมเพลต (BMS Palmprint DB: Palmprint Template)
3) **ระบบการระบุตัวตนด้วยไบโอเมตริก ของ Biometric Matching System (BMS)** มีการเพิ่มเติม ดังนี้
   - **3.1)** ระบบการระบุตัวตนด้วยภาพใบหน้า (ABIS Face Search Engine) โดยการค้นหาภาพใบหน้าตรงและภาพใบหน้าทั่วไป จะใช้ระบบร่วมกัน
   - **3.2)** ระบบการระบุตัวตนภาพลายนิ้วมือแฝง (ABIS Fingermark Search Engine)
   - **3.3)** ระบบการระบุตัวตนภาพลายฝ่ามือเฉพาะเทมเพลต (ABIS Palmprint DB Search Engine)

   หมายเหตุ การค้นหาข้อมูลภาพลายนิ้วมือแฝงและลายฝ่ามือ อาจมีการดึงข้อมูลจากฐานข้อมูลภาพลายนิ้วมือ 10 นิ้ว มาร่วมด้วย โดยระบบ ABIS จะต้องสกัดลักษณะเฉพาะหรือเทมเพลตจากภาพต้นฉบับลายนิ้วมือ 10 นิ้ว ขึ้นใหม่เนื่องจาก อัลกอริทึมที่ใช้แตกต่างจากระบบ AFIS เดิม

จากรายงานสรุปข้อมูลระบบ CS-SIS ในปี พ.ศ. 2561 (ค.ศ. 2018) มีการตรวจสอบการระบุตัวตนด้วยไบโอเมตริกแล้วทั้งหมดประมาณ 82.2 ล้านรายการ เป็นการแจ้งเตือนเกี่ยวกับบุคคลหรือคนที่ทิ้งวัตถุต้องสงสัยประมาณ 940,000 รายการ โดยประมาณ 25% เป็นการแจ้งเตือนจากการระบุตัวตนด้วยภาพลายนิ้วมือ และประมาณ 30% จากการระบุตัวตนด้วยภาพใบหน้า ตามระเบียบ CS-SIS จะมีการเก็บข้อมูลบุคคลที่ถูกการแจ้งเตือนไว้เพียงช่วงเวลาที่กำหนดเท่านั้น (ระยะเวลาห้าปี) หลังจากนั้นประเทศสมาชิกมีสิทธิ์ที่จะทบทวนถึงความจำเป็น ในการขยายระยะเวลาให้นานขึ้นได้ตามความเหมาะสม

บทที่ 3

ประเด็นที่เกี่ยวข้องการใช้งานไบโอเมตริกกับข้อมูลส่วนบุคคล

บทที่ 3. ประเด็นที่เกี่ยวข้องการใช้งานไบโอเมตริกกับข้อมูลส่วนบุคคล

ประเด็นการใช้งานระบบไบโอเมตริกจะเกี่ยวข้องกับสิทธิส่วนบุคคลเสมอ ข้อมูลไบโอเมตริกเป็นข้อมูลส่วนบุคคล ซึ่งจะต้องได้รับการคุ้มครองตามกฎหมาย แต่การใช้งานระบบไบโอเมตริกอาจมีการก้าวล่วงหรือละเมิดสิทธิส่วนบุคคล ซึ่งจะแสดงในรายละเอียดไว้ในบทนี้

3.1 ประเด็นที่เกี่ยวข้องการใช้งานไบโอเมตริกกับข้อมูลส่วนบุคคลในประเทศไทย

ประเด็นการใช้งานระบบไบโอเมตริกที่เกี่ยวข้องกับสิทธิส่วนบุคคลในประเทศไทย มีกฎหมายที่สำคัญสองฉบับ คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 ซึ่งมีประเด็นสำคัญที่เกี่ยวข้อง ดังนี้

3.1.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ประกาศในราชกิจจานุเบกษาไปเมื่อ 27 พฤษภาคม พ.ศ. 2562 โดยปัจจุบันได้มีมติคณะรัฐมนตรีให้ขยายเวลาบังคับใช้กฎหมายทั้งฉบับออกไปจนถึง วันที่ 1 มิ.ย. พ.ศ. 2565 ซึ่งเจตนารมณ์ของกฎหมายฉบับนี้ก็เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการเก็บรวบรวม การใช้ หรือ การเปิดเผยข้อมูลส่วนบุคคล การป้องกันการละเมิดสิทธิความเป็นส่วนตัว การสร้างความเดือดร้อนรำคาญ การสร้างความเสียหายให้แก่เจ้าของข้อมูล

ประเด็นสำคัญที่เกี่ยวข้องกับการใช้งานระบบไบโอเมตริกและยังไม่ได้มีการกำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลไว้อย่างชัดเจน จึงได้มีการรวบรวมมาจาก [ยุบลชิต2564] ซึ่งมีอยู่ด้วยกัน 3 ประเด็น คือ

1) มาตรา 6 บัญญัติความหมายของ “ข้อมูลส่วนบุคคล” แต่ยังคงมีประเด็น มิได้ให้ความหมายข้อมูลไบโอเมตริก จึงเป็นการคุ้มครองข้อมูลทั่วไป กล่าวคือ ข้อมูลไบโอเมตริกเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับร่างกายที่สามารถเก็บรวบรวมได้ง่ายและเป็นการยากที่เจ้าของจะระวังตัว
2) มาตรา 19 บัญญัติการขอความยินยอมไว้ แต่ยังคงมีประเด็น การเปิดช่องกว้างจนเกินไปในการขอให้ความยินยอมโดยบัญญัติไว้ดังนี้ “เว้นแต่โดยสภาพไม่อาจขอความยินยอมได้” ซึ่งเห็นว่าเป็นการให้ความยินยอม “โดยปริยาย”
3) มาตรา 23 บัญญัติการเก็บรวบรวมและระยะเวลาไว้ แต่ยังคงมีประเด็น การเปิดช่องกว้างจนเกินไปในการกำหนดระยะเวลาการเก็บ โดยบัญญัติไว้ดังนี้ “ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม” อาจทำให้ผู้ให้บริการกำหนดระยะเวลานานเท่าใดก็ได้ตามอำเภอใจ

ทั้งนี้ จากงานวิจัย [ยุบลชิต2564] ให้ข้อเสนอแนะแก้ไขเพิ่มเติมสำหรับการนำไปใช้เพื่อคุ้มครองข้อมูลไบโอเมตริกเป็นการเฉพาะ ดังนี้

1) ให้เพิ่มคำนิยามศัพท์ “ข้อมูลไบโอเมตริก” เพื่อให้เข้าใจความหมายตรงกัน และจำแนกประเภทของข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนไว้อย่างชัดเจนใน มาตรา 6
2) การแจ้งเตือนสิทธิในการขอให้ความยินยอมก่อน ซึ่งมิใช่ความยินยอมโดยปริยายหรือความยินยอมโดยอัตโนมัติ และต้องแจ้งผลกระทบให้เพิ่ม “ก่อน” ถอนความยินยอมใน มาตรา 19 วรรคหก
3) การแจ้งเตือนสิทธิการเข้าถึงข้อมูลส่วนบุคคลได้ตลอดในขณะที่ถูกเก็บรวบรวม หรือประมวลผลข้อมูลยังดำเนินต่อไปไว้ใน มาตรา 30
4) การแจ้งเตือนสิทธิในเรื่องระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล และกำหนดระยะเวลาให้เป็นการที่แน่นอนไว้ได้ภายใน 6 เดือน ในมาตรา 23 (3)
5) เพิ่มบทบัญญัติสิทธิในการแก้ไข (Rights to be rectification) เพื่อให้สิทธิผู้ควบคุมข้อมูลส่วนบุคคลสามารถแก้ไขข้อมูลส่วนบุคคลที่ผิดพลาดได้ตาม มาตรา 29 (2)

.

3.1.2 พระราชบัญญัติข้อมูลข่าวสารทางราชการ ปี พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารทางราชการ ปี พ.ศ. 2540 ได้ประกาศในราชกิจจานุเบกษาไปเมื่อ 10 กันยายน พ.ศ. 2540 โดยวันที่ 9 ธันวาคม พ.ศ. 2540 เป็นวันที่พระราชบัญญัติฉบับนี้มีผลบังคับใช้ตามกฎหมายทั้งฉบับ ซึ่งเจตนารมณ์ของกฎหมายฉบับนี้ ต้องการให้เป็นกลไกตรวจสอบของภาคประชาชน เพื่อความโปร่งใสภาครัฐ และให้ความคุ้มครองข้อมูลส่วนบุคคล รวมทั้ง “สิทธิรับรู้” ไม่ต้องมีส่วนได้เสีย

ประเด็นสำคัญที่เกี่ยวข้องกับการใช้งานระบบไบโอเมตริกในพระราชบัญญัติข้อมูลข่าวสารทางราชการ ได้มีการรวบรวมมาจาก [วศมกไอซีที2554] ซึ่งมีอยู่ด้วยกัน 2 มาตรา คือ

1) มาตรา 24 การแลกเปลี่ยนข้อมูลข่าวสารระหว่างหน่วยงานของรัฐ เช่น กรณีของสถาบันนิติวิทยาศาสตร์ ต้องการพิสูจน์ตัวบุคคลผู้ต้องสงสัยในคดีพิเศษ หรือ กรณีของกรมการกงสุล ต้องการยืนยันข้อมูลลายนิ้วมือของบุคคลในบัตรประจำตัวประชาชนที่นำมากับกรมการปกครองก่อนจะออกเล่มหนังสือเดินทางให้ หรือ กรณีสำนักบริหารแรงงานต่างด้าว กระทรวงแรงงาน ต้องการพิสูจน์ตัวบุคคลแรงงานต่างด้าวที่เข้าประเทศอย่างผิดกฎหมาย ซึ่งข้อมูลอยู่ในฐานข้อมูลของสำนักงานตรวจคนเข้าเมือง
2) มาตรา 25 สิทธิที่จะได้รู้ข่าวสารข้อมูลส่วนบุคคลของตน เช่น สิทธิในการแก้ไขข้อมูลใบหน้าหรือข้อมูลลายนิ้วมือของบุคคลในบัตรประจำตัวประชาชน

ทั้งนี้ ในงานวิจัย [ไอซีที2554] ให้ข้อเสนอแนะเพิ่มเติมสำหรับการนำไปใช้เพื่อคุ้มครองข้อมูลไบโอเมตริกเป็นการเฉพาะ โดยเสนอให้คณะกรรมการข้อมูลข่าวสารของราชการ พิจารณาตีความการแลกเปลี่ยนข้อมูลไบโอเมตริกในกรณีต่าง ๆ ที่เป็นประโยชน์ต่อทางราชการและส่วนรวมว่าสามารถทำได้หรือไม่

3.2 ประเด็นที่เกี่ยวข้องการใช้งานไบโอเมตริกกับสิทธิส่วนบุคคลในต่างประเทศ

ในส่วนนี้จะเป็นการสำรวจประเด็นการใช้งานระบบไบโอเมตริกที่เกี่ยวข้องและมีปัญหากับสิทธิส่วนบุคคลในต่างประเทศที่สำคัญ

3.2.1 สิทธิและกฎหมายที่เกี่ยวข้องกับการใช้งานไบโอเมตริกในประเทศต่าง ๆ

ประเด็นสำคัญของสิทธิและกฎหมายที่เกี่ยวข้องกับการใช้งานไบโอเมตริกในแต่ละประเทศ ทางคณะที่ปรึกษาได้รวบรวมมาจาก [มหาแถลง2564] มาไว้เป็นตัวอย่าง ดังนี้

1) **ประเทศสหรัฐอเมริกา** มีพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริก (Biometric Information Privacy Act 2008: BIPA) ได้มีการประกาศใช้ในมลรัฐอิลลินอยส์ (Illinois) เป็นรัฐแรกในเดือนตุลาคม ปี ค.ศ. 2008 และต่อมามลรัฐวอชิงตัน (Washington) และมลรัฐเท็กซัส (Texas) ได้ผ่านกฎหมายในเรื่องนี้เช่นเดียวกัน โดยมีประเด็นสำคัญ คือ
   1.1) การเก็บ การรวบรวม และการเปิดเผยข้อมูลไบโอเมตริก ต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลโดยชัดแจ้ง
   1.2) ต้องทำลายข้อมูลไบโอเมตริกเมื่อถึงเวลาที่เหมาะสม กล่าวคือ 3 ปี นับแต่วันที่เริ่มเก็บข้อมูล
   1.3) ต้องมีมาตรการรักษาความปลอดภัยในการเก็บข้อมูลไบโอเมตริกอย่างเคร่งครัด
2) **สหภาพยุโรป** มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation: GDPR) ซึ่งมีการกล่าวถึงการใช้งานไบโอเมตริกไว้อยู่ในมาตรา 9 โดยมีหลักห้ามทำการบันทึกหรือประมวลผลข้อมูลไบโอเมตริก เว้นแต่ผู้เป็นเจ้าของข้อมูลจะให้ความยินยอมโดยชัดเจน หรือข้อมูลไบโอเมตริกนั้นจำเป็นสำหรับการปฏิบัติงานความมั่นคงปลอดภัยของสังคม หรือปกป้องคุ้มครองทางสังคม
3) **ประเทศแคนาดา** มีกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection and Electronic Documents Acts) โดยบรรพ 1 มาตรา 5 ข้อ 4.1.4 มีการบังคับใช้ข้อมูลส่วนบุคคลที่อยู่ในครอบครองของเอกชนและเอกสารอิเล็กทรอนิกส์ ซึ่งคล้ายคลึงกับประเทศต่าง ๆ แต่มีประเด็นที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนดอย่างมีประสิทธิภาพ ได้แก่
   3.1) การตั้งหน่วยงานรับเรื่องร้องเรียนหรือร้องขอ
   3.2) การฝึกอบรมลูกจ้าง
   3.3) การสร้างความเข้าใจแก่ผู้ร่วมงานในนโยบายและข้อปฏิบัติของตน

4) **ประเทศเยอรมนี** มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Federal Data Protection Act 2018) โดย มาตรา 1 มีขอบเขตการบังคับใช้แก่หน่วยงานของรัฐระดับสหพันธ์และระดับมลรัฐ และบังคับใช้แก่เอกชนซึ่งเก็บรวบรวม ใช้ หรือดำเนินการเก็บข้อมูลส่วนบุคคล ไม่ว่าด้วยวิธีทางอิเล็กทรอนิกส์หรือไม่ก็ตาม ทั้งนี้ ได้มีการนิยามคำว่า “ดำเนินการ” (Process) หมายถึง การเก็บรักษา การแก้ไขปรับปรุง การยับยั้ง การลบ หรือการเปิดเผยข้อมูลส่วนบุคคล และได้มีการนิยามคำว่า “การเปิดเผยข้อมูล” หมายถึง การเปิดเผยต่อบุคคลที่สาม หรือการส่งผ่านบุคคลที่สาม หรือส่งให้บุคคลที่สามารถเรียกดูได้

นอกจากนี้ มาตรา 15-16 ได้มีบทบัญญัติห้ามให้โอนข้อมูลไปยังประเทศที่ไม่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ยกเว้นการส่งหรือโอนข้อมูลไปในประเทศสหภาพยุโรปสามารถกระทำได้

3.2.2 กรณีศึกษาของปัญหาการใช้งานไบโอเมตริกกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ

คณะที่ปรึกษาฯ ได้สำรวจและรวบรวมกรณีศึกษาของปัญหาการละเมิดสิทธิตามกฎหมายที่ปรากฏอยู่ในสื่อต่าง ๆ ดังนี้

1) **กรณีศึกษาของบริษัท Facebook** [TechCrunch2021] [22] ตามพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริก (Biometric Information Privacy Act 2008: BIPA) ของรัฐอิลลินอยส์ ซึ่งถูกฟ้องเป็นเงิน 650 ล้านดอลล่าสหรัฐ เพราะเหตุว่าใช้โปรแกรม Facial Recognition ที่มีชื่อเรียกว่า “Tagging Features” ไปติดตามใบหน้าของผู้ใช้บริการ Facebook เมื่ออัปโหลดรูปถ่ายของตนเองขึ้นไปบนบริการของ Facebook

หลังจากนั้น บริษัท Facebook ต้องปิดบริการ “Automatic Facial Recognition Tagging Features” ลงในปี ค.ศ. 2019 และเมื่อการพิจารณาคดีขั้นสุดท้ายได้สิ้นสุดลง ผู้อยู่อาศัยในรัฐอิลลินอยส์ จำนวน 1.6 ล้านคน จะได้รับเงินชดเชยจากกรณีดังกล่าว อย่างน้อยคนละ 345 ดอลล่าสหรัฐ

2) **กรณีศึกษาของบริษัท Google** [Robinson&Cole2019] [23] ตามพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริก (Biometric Information Privacy Act 2008: BIPA) ของรัฐอิลลินอยส์ ซึ่ง บริษัท Google ถูกยื่นฟ้อง โดยอ้างว่าละเมิดกฎหมาย BIPA เช่นกัน เนื่องจาก เป็นการรวบรวม จัดเก็บ และใช้งาน ใบหน้าในภาพถ่ายที่อัปโหลดไปยังบริการ Google Photos หลายล้านคนในรัฐอิลลินอยส์ โดยไม่แจ้งให้ทราบและไม่ได้รับความยินยอมเป็นลายลักษณ์อักษร

ทั้งนี้ Google Photos เป็นบริการบนคลาวด์ โดยจะมีการรู้จำใบหน้า เพื่อรู้จำบุคคลและจัดกลุ่มตามบุคคลที่ปรากฏในภาพถ่าย และเก็บเทมเพลตของบุคคลไว้ในฐานข้อมูล

3) **กรณีศึกษาของบริษัท Clearview AI** [น้อยปัญญา2563] [24] ตามพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริก (Biometric Information Privacy Act 2008: BIPA) ซึ่งบริษัท Clearview AI ถูกยื่นฟ้องในศาลนิวยอร์ก 1 คดี ศาลเวอร์จิเนีย 1 คดี และศาลอิลลินอยส์ 2 คดี รวม 4 คดี ในข้อหาละเมิดสิทธิส่วนบุคคล ซึ่งบริการของบริษัท Clearview AI เป็นโปรแกรมหาภาพของบุคคล แม้ภาพนั้นจะอยู่ในโซเชียลส่วนตัว โดยบริการดังกล่าวจะรวบรวมและเข้าถึงรูปภาพจากเว็บโซเชียลต่าง ๆ เช่น Instagram, Twitter, YouTube, Facebook, Venmo, etc. ซึ่งมีกว่า 3,000 ล้านรูปมาเป็นฐานข้อมูล

นอกจากนั้น คณะที่ปรึกษากฎหมายของสหภาพเสรีภาพพลเมืองอเมริกันแห่งอิลลินอยส์ (American Civil Liberties Union of Illinois’ legal adviser, ACLU) ได้ยื่นฟ้องบริษัท Clearview AI หลังจากที่กรมตำรวจชิคาโกได้มีการว่าจ้างบริษัท Clearview AI โดยมีสัญญาสองปี เพื่อใช้เทคโนโลยีการจดจำใบหน้าของบริษัท โดยอ้างว่ามีการละเมิดภายใต้กฎหมาย BIPA ของรัฐ จนทำให้กรมตำรวจต้องบอกเลิกสัญญาดังกล่าว [Garcia2021] [25]

3.2.3 ประเด็นการใช้งานไบโอเมตริกและจริยธรรม

คณะที่ปรึกษาฯ ได้สำรวจและรวบรวมประเด็นที่สำคัญของปัญหาการใช้งานไบโอเมตริกและจริยธรรมในมุมมองต่าง ๆ มาดังนี้

---

[22] https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/

[23] https://www.lexology.com/library/detail.aspx?g=51dd0122-9399-48e9-b6ef-fc357760d387

[24] https://thaipublica.org/2020/03/toppol13/

[25] https://news.wttw.com/2021/03/30/illinois-law-protecting-biometric-privacy-could-be-changed

1) **ประเด็นการใช้งานไบโอเมตริกในผู้สูงวัย (Biometrics for Ageing Society)**

เนื่องจากสัดส่วนของประชากรสูงวัยกำลังมีแนวโน้มเพิ่มมากขึ้น (ตามพระราชบัญญัติผู้สูงอายุ พ.ศ. 2546 มาตรา 3 “ผู้สูงอายุ” หมายความว่า บุคคลซึ่งมีอายุเกินหกสิบปีบริบูรณ์ขึ้นไป) ซึ่งทำให้ในอนาคตการใช้งานไบโอเมตริกจะต้องพบปัญหา [Rebera2012] โดยสามารถรวบรวมมาเป็นประเด็นได้ดังนี้

1.1) คุณภาพของภาพที่ถ่ายได้จากผู้สูงวัยมักจะด้อยกว่าภาพของผู้ที่มีอายุน้อยกว่า ทำให้ผู้สูงวัยประสบปัญหาในการใช้งานมากขึ้น ผู้สูงวัยจะถูกกีดกันการเข้าถึงต่าง ๆ

1.2) ความเสื่อมสภาพของร่างกายผู้สูงวัย ทำให้เทมเพลตที่ใช้ลงทะเบียนเปลี่ยนแปลง เป็นผลให้ประสิทธิภาพของระบบลดลงอย่างมาก ผู้สูงวัยจะไม่สะดวกใช้งาน

โดยผลกระทบต่อผู้สูงวัย อาจประสบกับการกีดกันในหลาย ๆ ด้าน หรือไม่สะดวกในการใช้งาน ทำให้เกิดการแยกตัวออกจากสังคม ซึ่งเป็นภาวะที่น่ากังวลและภาครัฐจะต้องคำนึงถึงประเด็นการใช้งานไบโอเมตริกในผู้สูงวัย ในการออกกฎเกณฑ์ใด ๆ ก็ตาม

2) **ประเด็นการใช้งานไบโอเมตริกในเด็ก (Biometrics Recognition of Children)**

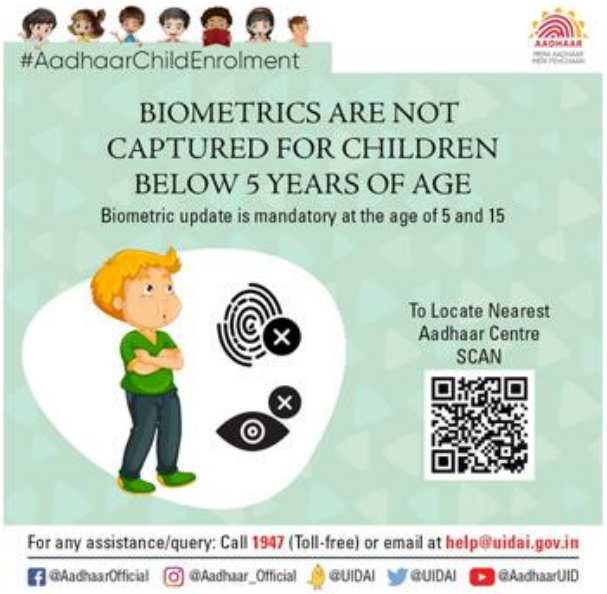
เด็กและเยาวชนได้ถูกคุ้มครองโดยหน่วยงานและกฎหมายหลายฉบับ (ตามพระราชบัญญัติศาลเยาวชนและครอบครัว และวิธีพิจารณาคดีเยาวชนและครอบครัว พ.ศ. 2546 มาตรา 4 “เด็ก” หมายความว่า บุคคลอายุยังไม่เกินสิบห้าปีบริบูรณ์ “เยาวชน” หมายความว่า บุคคลอายุเกินสิบห้าปีบริบูรณ์แต่ยังไม่ถึงสิบแปดปีบริบูรณ์ นอกจากนี้ ตามคำนิยามของ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ (พม.) “เด็ก” หมายถึง บุคคลซึ่งมีอายุต่ำกว่า 18 ปีบริบูรณ์ “เยาวชน” หมายถึง บุคคลซึ่งมีอายุตั้งแต่ 18 ปีบริบูรณ์ถึง 25 ปีบริบูรณ์) ซึ่งในหลายประเทศได้กำหนดข้อจำกัดด้านอายุ สำหรับการใช้งานไบโอเมตริกกับเด็ก [ACE2010] [26], [Pakrasi2021] [27] เช่น

2.1) สหภาพยุโรป มีเกณฑ์อายุ 12 ปี เพื่อใช้ลายนิ้วมือในการทำบัตรประจำตัวประชาชน

2.2) ประเทศโมร็อกโก มีเกณฑ์อายุ 16 ปี เพื่อใช้ลายนิ้วมือในการทำบัตรประจำตัวประชาชน

2.3) ประเทศอาร์เจนตินา จะเริ่มเก็บลายนิ้วมือ ตั้งแต่เด็กเข้าโรงเรียนครั้งแรก

2.4) ประเทศอินเดีย (ในโครงการ Aadhaar) มีเกณฑ์อายุ 5 ปี เพื่อเก็บม่านตาและลายนิ้วมือ โดยก่อนอายุ 5 ปี จะถ่ายเพียงภาพใบหน้าเท่านั้น และจะไม่เก็บลายนิ้วมือและม่านตาตามภาพที่ 62



ภาพที่ 62 โครงการ Aadhaar ประกาศการไม่เก็บลายนิ้วมือและม่านตาของเด็กอายุต่ำกว่า 5 ขวบ (ภาพจาก [Pakrasi2021])

[26] https://aceproject.org/electoral-advice/archive/questions/replies/306802609

[27] https://www.hindustantimes.com/india-news/aadhaar-card-no-fingerprint-eye-scan-for-children-below-5-years-101627353199035.html

ทั้งนี้ นิยามของ สหประชาชาติ “เด็ก” หมายถึง ผู้ที่มีอายุต่ำกว่า 1 ปี ถึง 14 ปี (0 – 14 ปี) “เยาวชน” หมายถึง ผู้ที่มีอายุระหว่าง 15 – 24 ปี

3) การใช้งานไบโอเมตริกกับประเด็นทางจริยธรรม (Ethical Issues with Biometrics)

ประเด็นด้านจริยธรรมของการใช้งานไบโอเมตริกโดยทั่วไป ได้ถูกรวบรวม [Hayes2019] [28] มาดังนี้

3.1) บริษัทผู้ผลิตส่วนมากปฏิเสธที่จะเปิดเผยเทคโนโลยีของตนเองเพื่อการตรวจสอบต่อสาธารณะ ทำให้ยากต่อการเข้าใจถึงระดับอคติ (Bias) ของระบบ ซึ่งจะต้องอาศัยความรับผิดชอบของบริษัทเอง

3.2) อาคารสาธารณะในปัจจุบันมีการติดตั้งกล้องวงจรปิด ซึ่งหากกล้องเหล่านั้นเชื่อมต่อกับบริการรู้จำใบหน้า อาจนำไปสู่ประเด็นเรื่องเสรีภาพในการพูด การชุมนุม และแม้แต่ศาสนา

3.3) ข้อมูลไบโอเมตริกสามารถถูกใช้เพื่อแสดงโฆษณาไปยังกลุ่มลูกค้าเป้าหมาย (Targeted Ads) ดังนั้น หากมีการระบุตัวบุคคลตามสถานที่สาธารณะ อาจนำไปสู่เรื่องการละเมิดสิทธิและเสรีภาพ

3.3 สรุปประเด็นสำคัญที่เกี่ยวข้องการใช้งานไบโอเมตริกกับข้อมูลส่วนบุคคล

ประเทศไทยมีกฎหมายคุ้มครองสิทธิข้อมูลส่วนบุคคล ซึ่งเป็นแนวทางเดียวกันกับหลักสากล แต่ประเทศไทยยังไม่มีกฎหมายเฉพาะเพื่อคุ้มครองสิทธิข้อมูลไบโอเมตริก ซึ่งควรมีการแก้ไขเพื่อกำหนดบทบัญญัติต่าง ๆ ของความคุ้มครองสิทธิข้อมูลไบโอเมตริกให้ชัดเจน เช่น การจัดเก็บ การแก้ไข การยับยั้ง การลบ การเปิดเผยข้อมูล รวมทั้งการเปิดเผยหรือส่งผ่านต่อบุคคลที่สาม

นอกเหนือจากตัวกฎหมายแล้ว ภาครัฐควรเร่งศึกษาถึงการใช้งานที่เหมาะสมกับประชากรในทุกช่วงวัย รวมถึงการผสมผสานข้อมูลไบโอเมตริกให้เข้ากันกับวัฒนธรรมของแต่ละภูมิภาค เช่น การสแกนใบหน้ากับสตรีชาวมุสลิม การพิมพ์นิ้วมือกับเด็กในลักษณะที่แตกต่างกับอาชญากร

[28] https://www.securityinfowatch.com/access-identity/biometrics/article/21072152/ethics-and-biometric-identity

บทที่ 4

ภูมิทัศน์ของมาตรฐานไบโอเมตริก (Biometric Standard Landscape)

บทที่ 4. ภูมิทัศน์ของมาตรฐานไบโอเมตริก (Biometric Standard Landscape)

มาตรฐาน หมายถึง เอกสารเผยแพร่ หรืออยู่ในระหว่างกระบวนการออกเอกสารเผยแพร่ ที่ได้รับการยอมรับในวงกว้าง โดยกำหนดความต้องการและให้ข้อมูลรายละเอียดทางเทคนิค โดยมีเป้าหมายเพื่อการทำงานร่วมกัน แลกเปลี่ยนข้อมูลระหว่างกัน และประเมินประสิทธิภาพการทำงานอย่างเป็นธรรม

มาตรฐานไบโอเมตริก เป็นมาตรฐานที่กำหนดขึ้นเพื่อให้การใช้งานเทคโนโลยีไบโอเมตริกสามารถทำงานร่วมกันได้ สามารถแลกเปลี่ยนข้อมูลระหว่างกัน และสามารถทำงานได้ตามวัตถุประสงค์

วัตถุประสงค์ของการกำหนดมาตรฐานไบโอเมตริก มีดังต่อไปนี้

1) เพื่อการใช้งานไบโอเมตริกแบบบูรณาการ
2) เพื่อรักษาคุณภาพของข้อมูลไบโอเมตริกเมื่อเวลาผ่านไป
3) เพื่อลดความเสี่ยงของผู้ใช้กับผู้ออกแบบระบบ และสามารถปรับปรุงระบบได้โดยไม่ต้องลงทุนซื้อทั้งระบบใหม่
4) เพื่อลดการผูกขาดของบริษัทผู้ขายและส่งเสริมการแข่งขันในตลาดเสรี
5) เพื่อประเมินประสิทธิภาพของระบบไบโอเมตริกอย่างเป็นธรรม

การกำหนดมาตรฐานกลางไบโอเมตริก มีการกำหนดรูปแบบต่าง ๆ ที่สำคัญเพื่อการเชื่อมต่อแบบบูรณาการ แต่มีข้อควรระวัง ดังต่อไปนี้

1) โดยทั่วไปแล้วจุดประสงค์หลักของการกำหนดมาตรฐานคือเพื่อการบูรณาการ แต่การใช้มาตรฐานไม่ได้รับรองการเชื่อมต่อแบบบูรณาการเสมอไป โดยเฉพาะในกรณีที่มาตรฐานไม่สมบูรณ์และมีทางเลือกที่ไม่บังคับ
2) การกำหนดมาตรฐานให้ผลดีและผลเสียทางธุรกิจ มาตรฐานที่ดีอาจสร้างตลาดใหม่ ในทางตรงกันข้ามจะทำให้การแข่งขันในเชิงธุรกิจสูงและลดผลกำไร
3) มาตรฐานมีอายุการใช้งานที่จำกัด เนื่องจากเทคโนโลยีไบโอเมตริกที่เปลี่ยนไป โดยปกติจะพัฒนาทุก 5 ปี โปรดระวังการใช้มาตรฐานที่ล้าสมัย หรือมาตรฐานที่ไม่มีการใช้งานโดยองค์กรใด ๆ

การกำหนดมาตรฐานการใช้งานเทคโนโลยีไบโอเมตริก เริ่มต้นตั้งแต่ปี พ.ศ. 2529 (ค.ศ. 1986) โดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ NIST (National Institute of Standards and Technology)[29] ของประเทศสหรัฐอเมริกา โดยได้กำหนดมาตรฐานไบโอเมตริกเริ่มต้น เกี่ยวกับการเก็บข้อมูลลายนิ้วมือ จากนั้นได้พัฒนากำหนดมาตรฐานไบโอเมตริกเพิ่มเติมมาเรื่อย ๆ จนถึงจุดเปลี่ยนคือสถานการณ์ 911 หรือการโจมตีตึก World Trade Center ที่เมือง New York ประเทศสหรัฐอเมริกา เมื่อ 11 กันยายน พ.ศ. 2544 (ค.ศ. 2001) ทำให้เทคโนโลยีไบโอเมตริกเป็นที่ต้องการและเติบโตอย่างก้าวกระโดด ในช่วงนั้นเป็นจุดกำเนิดของหน่วยงาน กำหนดมาตรฐานไบโอเมตริก INCITS M1 Biometrics[30] ซึ่งจัดตั้งในเดือนพฤศจิกายน พ.ศ. 2544 (ค.ศ. 2001) INCITS ซึ่งเป็นคณะกรรมการภายใต้ ANSI ของประเทศสหรัฐอเมริกา ได้มีการแต่งตั้งคณะกรรมการทางเทคนิคเรียกว่า Technical Committee M1-Biometrics ขึ้น ในปีต่อมาเดือนมิถุนายน พ.ศ. 2545 (ค.ศ. 2002) คณะกรรมการนานาชาติ ISO/IEC JTC1 ได้แต่งตั้งคณะกรรมการกลุ่มย่อย ISO/IEC JTC1 SC37 Biometrics[31] เพื่อกำหนดมาตรฐานทางด้านไบโอเมตริกโดยเฉพาะ โดย INCITS ได้เป็นส่วนหนึ่งในการจัดตั้งและเป็นคณะกรรมการตัวแทนประเทศสหรัฐอเมริกา ทั้งสองหน่วยงานทั้งทำงานคู่ขนานและทำงานผลักดันร่วมกัน ดังนั้นมาตรฐานต่าง ๆ ที่ INCITS กำหนดจึงกลายมาเป็นมาตรฐานไบโอเมตริก ISO ในปัจจุบัน อีกหน่วยงานหนึ่งที่มีส่วนผลักดันเทคโนโลยีไบโอเมตริกในเวลาใกล้เคียงกัน คือ หน่วยงาน OASIS XML Common Biometric Format (XCBF) Technical Committee [32] ซึ่งได้ออกมาตรฐาน XML Common Biometric Format ในเดือนสิงหาคม ปี พ.ศ. 2546 (ค.ศ. 2003) โดย XML (Extensible Markup Language) เป็นภาษาคอมพิวเตอร์ที่ใช้งานสำหรับการกำหนดรูปแบบการเข้ารหัสของข้อมูลรูปแบบที่มนุษย์สามารถอ่านได้และคอมพิวเตอร์สามารถอ่านได้ ซึ่งปัจจุบัน ISO/IEC JTC 1/SC37 ได้มีมาตรฐานครอบคลุม XML ในส่วนที่จำเป็นทั้งหมด ทำให้ OASIS ไม่มีความจำเป็นต้องกำหนดมาตรฐานไบโอเมตริกทางด้าน XML อีก

[29] https://www.nist.gov/

[30] https://www.incits.org/committees/m1

[31] https://www.iso.org/committee/313770.html

[32] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xcbf

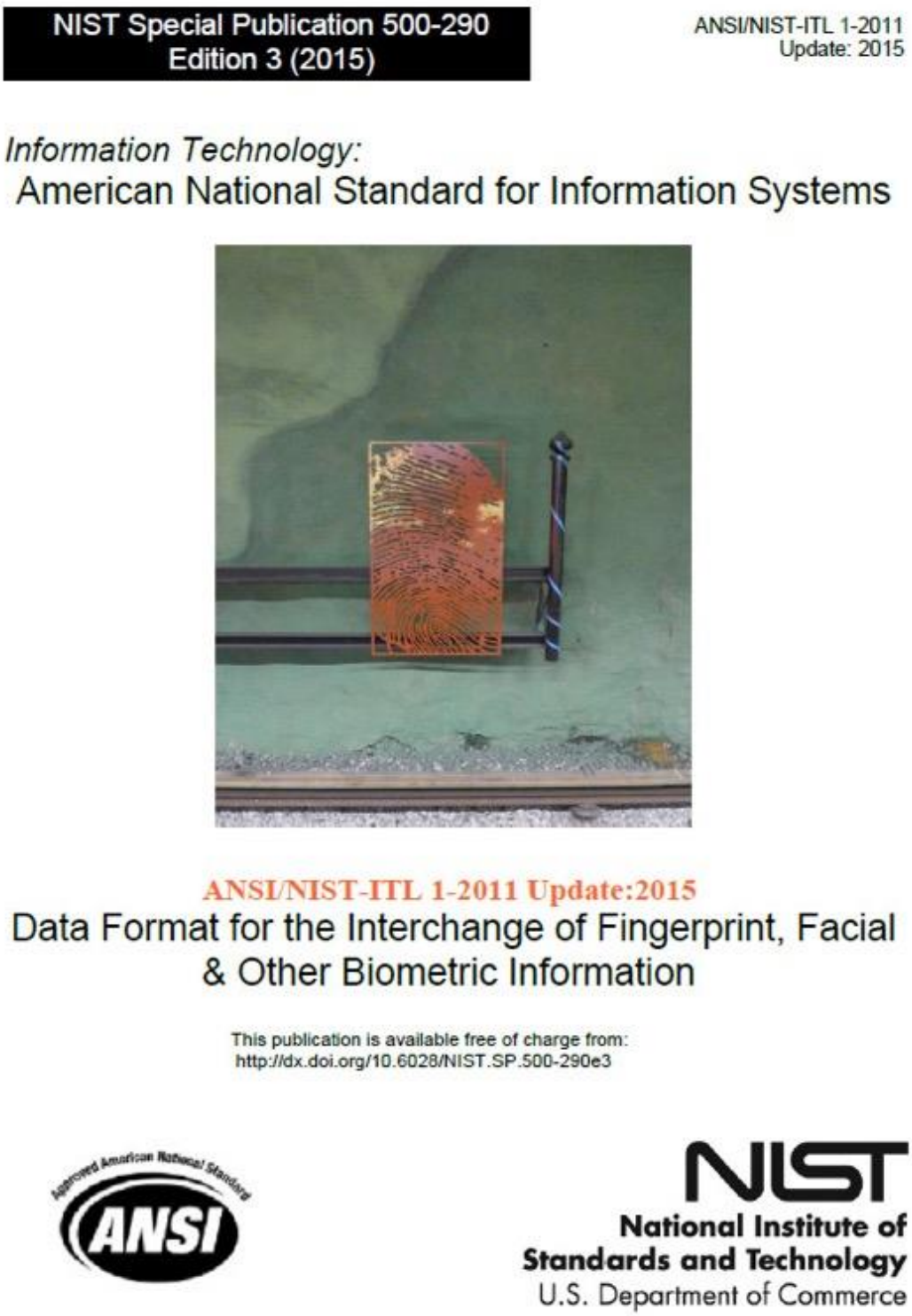
ภูมิทัศน์ของมาตรฐานไบโอเมตริกในปัจจุบัน มีสองมาตรฐานไบโอเมตริกหลักที่สำคัญ คือ มาตรฐาน ISO/IEC JTC 1/SC37 และมาตรฐาน ANSI/NIST-ITL[33] โดยมาตรฐาน ISO จะเกี่ยวข้องกับงานบริการประชาชนโดยทั่วไป อาทิ การใช้ไบโอเมตริกในการควบคุมการเข้าประเทศที่ใช้หนังสือเดินทางที่อ่านได้โดยอัตโนมัติ การควบคุมการเข้าถึง การตรวจสอบผู้มีสิทธิ์ในการทำธุรกรรมต่าง ๆ ที่สำคัญ เช่น การลงคะแนนเสียง การใช้ไบโอเมตริกกับทางสาธารณสุข โดยมีหน่วยงานที่นำมาตรฐาน ISO ไปใช้ อาทิ องค์การบินพลเรือนระหว่างประเทศ (International Civil Aviation Organization (ICAO)) และ องค์การแรงงานระหว่างประเทศ (International Labor Organization (ILO)) ส่วนมาตรฐาน NIST จะเน้นงานทางด้านนิติวิทยาศาสตร์ โดยมีตำรวจสากล (Interpol) และหน่วยงาน FBI ของสหรัฐอเมริกานำไปใช้งาน ทำให้ขยายไปใช้ในหน่วยงานตำรวจและนิติวิทยาศาสตร์อื่น ๆ ในประเทศต่าง ๆ ที่ทำงานเกี่ยวข้องกับหน่วยงานเหล่านี้ สำหรับบทนี้จะเน้นมาตรฐานจากสองหน่วยงานนี้เป็นหลัก

4.1 NIST (National Institute of Standards and Technology)

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ NIST (National Institute of Standards and Technology) ปัจจุบันเป็นสถาบันหนึ่งภายใต้กระทรวงพาณิชย์ (Department of Commerce) ของประเทศสหรัฐอเมริกา มีขอบข่ายงานที่ครอบคลุมศาสตร์ทางด้านฟิสิกส์ เคมีและชีววิทยา นอกจากนี้แล้วยังเป็นสถาบันที่จัดทำเอกสาร ทั้งด้านทฤษฎีและปฏิบัติโดยอาศัยผู้เชี่ยวชาญทั้งในภาครัฐและเอกชนเพื่อนำเสนอต่อ ANSI (American National Standards Institute) และจัดทำเป็นมาตรฐานเพื่อใช้ในประเทศสหรัฐอเมริกา สำหรับมาตรฐานลายนิ้วมือที่จัดทำโดย NIST ที่เป็นลายลักษณ์อักษรเริ่มต้นในปี พ.ศ. 2529 (ค.ศ. 1986) โดยมีรหัส คือ ANSI/NBS-ICST 1-1986 (Fingerprint Identification: Data Format for Information Interchange) และได้รับการปรับปรุงมาเป็นลำดับตามเทคโนโลยีที่เปลี่ยนไปและความสลับซับซ้อนของข้อมูลที่มีมากขึ้นเรื่อย ๆ โดยเรียงลำดับได้ดังนี้ คือ ANSI/NIST-CSL 1-1993 (Data Format for the Interchange of Fingerprint Information), ANSI/NIST-ITL 1a-1997 (Data Format for the Interchange of Fingerprint, Facial & SMT Information), ANSI/NIST-ITL 1-2000 (Data Format for the Interchange of Fingerprint, Facial & Scar Mark & Tattoo (SMT) Information), ANSI/NIST-ITL 1-2007 (Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information – Part 1) และปัจจุบัน คือ ANSI/NIST-ITL 1-2011 (Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information)

อนึ่งในปี พ.ศ. 2550-2551 (ค.ศ. 2007-2008) มีมาตรฐานออกมา 2 ชุด คือ ANSI/NIST-ITL 1-2007 และ ANSI/NIST-ITL 2-2008 (Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information – Part 2: XML Version) มาตรฐานทั้ง 2 ชุดนี้มีเนื้อหาเหมือนกันทุกประการยกเว้นการนำเสนอ กล่าวคือ ANSI/NIST-ITL 1-2007 มีการนำเสนอตามแบบฉบับทั่วไป ANSI/NIST-ITL 2-2008 มีการนำเสนอโดยใช้ภาษา XML (Extensible Markup Language) ทั้งนี้เพื่อให้เป็นไปตาม NIEM-conformance encoding (NIEM: National Information Exchange Model) อย่างไรก็ตามทั้ง ANSI/NIST-ITL 1-2007 และ ANSI/NIST-ITL 2-2008 ก็ถูกแทนที่โดยมาตรฐานล่าสุด คือ ANSI/NIST-ITL 1-2011 และมีการปรับปรุงเพิ่มเติมเมื่อปี ค.ศ. 2013 [NIST-ITL 1-2011 (2013)] (Edition 2) และปี ค.ศ. 2015 [NIST-ITL 1-2011 (2015)] (Edition 3) [NIST-ITL2011] โดยมาตรฐานฉบับล่าสุดดังแสดงในภาพที่ 63

[33] https://www.nist.gov/programs-projects/ansinist-itl-standard



ภาพที่ 63 หน้าปกมาตรฐานฉบับล่าสุด ANSI/NIST-ITL 1-2011 (Update 2015) Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information ของ NIST (ภาพจาก [NIST-ITL2011])

การกำหนดมาตรฐานของ NIST เหมือนกับการกำหนดมาตรฐานโดยทั่วไป กล่าวคือ มาตรฐานใหม่จะไปแทนที่มาตรฐานเก่าเสมอ สิ่งที่กำหนดไว้ดีแล้วในมาตรฐานเก่า ก็จะนำมาสืบสานในมาตรฐานใหม่ โดยมิได้มีการเปลี่ยนแปลง ในกรณีที่มีการปรับปรุงเพิ่มเติมที่มิได้มีนัยสำคัญมาก ก็จะออกมาในรูปแบบบทแทรก บทเฉพาะกาลหรือภาคผนวกเท่านั้น แต่ยังคงมาตรฐานเดิมไว้ การพัฒนามาตรฐานไบโอเมตริกของ NIST เป็นดังตารางที่ 10

ตารางที่ 10 สรุปประวัติการพัฒนามาตรฐานไบโอเมตริกของ NIST

ปี พ.ศ.	Standard	รายละเอียด
2529	ANSI/NBS-ICST 1-1986	ในปี พ.ศ. 2529 หรือ ค.ศ. 1986 NIST ซึ่งในขณะนั้นใช้ชื่อว่า National Bureau of Standards หรือ NBS กำหนดมาตรฐาน ANSI/NBS-ICST 1-1986 ซึ่งเป็นการกำหนดมาตรฐานข้อมูลลายนิ้วมือโดยใช้ข้อมูลมินูเทียร์ (Minutiae) หรือจุดแยกหรือจุดหยุดของเส้นลายนิ้วมือ มาตรฐานนี้เป็นการกำหนดการแลกเปลี่ยนมินูเทียร์และการเก็บข้อมูลมินูเทียร์โดยใช้หน่วยความจำต่ำที่สุด นับว่าเป็นมาตรฐานแรกเริ่มของมาตรฐานไบโอเมตริก
2536	ANSI/NIST-CSL 1-1993	ในปี พ.ศ. 2536 หรือ ค.ศ. 1993 มาตรฐานเดิมได้ถูกปรับปรุงและอนุมัติโดย ANSI เรียกว่า มาตรฐาน “Data Format for the Interchange of fingerprint Information” (ANSI/NIST-CSL 1-1993) โดยยังคงส่วนที่เป็นข้อมูลมินูเทียร์ไว้ แต่เพิ่มส่วนที่เป็นการกำหนดมาตรฐานการแลกเปลี่ยนภาพลายนิ้วมือแทนที่จะเน้นข้อมูลมินูเทียร์ดังมาตรฐานเดิม
2540	ANSI/NIST-ITL 1a-1997	ในปี พ.ศ. 2540 หรือ ค.ศ. 1997 ส่วนมาตรฐานเพิ่มเติมที่เกี่ยวข้องกับการแลกเปลี่ยนมาตรฐานใบหน้าโดยเฉพาะการเก็บใบหน้าเพื่อการระบุตัวอาชญากรและภาพที่เกี่ยวข้องกับแผลเป็นหรือรอยสักได้ถูกเพิ่มเติมเข้าไปในมาตรฐาน เรียกว่า ANSI/NIST-ITL 1a-1997
2541-2543	ANSI/NIST-ITL 1-2000	ในปี พ.ศ. 2541 หรือ ค.ศ. 1998 ได้มีการจัดการประชุม Workshop ทำการปรับปรุงมาตรฐานและส่วนเพิ่มเติม และรวมเป็นเล่มเดียวกัน โดยเน้นส่วนที่เป็น Tagged-field Record และนำเสนอส่วนที่เป็นการแลกเปลี่ยนภาพลายนิ้วมือ ภาพร่องรอยลายนิ้วมือ (Latent) และภาพฝ่ามือ (Palm Print) โดยมาตรฐานนี้เสร็จในปี 2543 หรือ ค.ศ. 2000 เรียกว่า “Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information” เรียกมาตรฐานนี้โดยย่อว่า ANSI/NIST-ITL 1-2000
2548 ถึง 20 เม.ย. 2550	ANSI/NIST-ITL 1-2007	ในปี พ.ศ. 2548 ได้มีการจัดการประชุม Workshop สองครั้ง เพื่อทำการปรับปรุงมาตรฐาน ANSI/NIST-ITL 1-2000 โดยมาตรฐานปรับปรุงใหม่นี้เสร็จวันที่ 20 เมษายน พ.ศ. 2550 เรียกว่า “Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1” เรียกมาตรฐานนี้โดยย่อว่า ANSI/NIST-ITL 1-2007 โดยมีการเปลี่ยนแปลง คือ - กำหนดคุณภาพของภาพและข้อมูลการแบ่งแยกภาพ เพื่อการประมวลภาพ - กำหนดรูปแบบของมินูเทียร์ให้ตรงกับมาตรฐานของ INCITS M1 Minutiae Standard - กำหนดระดับการประยุกต์การถ่ายภาพใบหน้า - กำหนดรูปแบบการแลกเปลี่ยนข้อมูลม่านตา (Iris) - กำหนดรูปแบบการแลกเปลี่ยนข้อมูลไบโอเมตริกอื่น ๆ ที่ไม่ได้อธิบายในมาตรฐานนี้ - กำหนดการใช้รูปแบบ XML เป็นตัวเลือกแทนมาตรฐานนี้
2550 ถึง 12 ส.ค. 2551	ANSI/NIST-ITL 2-2008	จากการปรับปรุงมาตรฐาน ANSI/NIST-ITL 1-2000 เสร็จ คณะกรรมการได้ปรับปรุงส่วนที่สองเรียกว่า “Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Part 2: XML Version.
พ.ย. 2554	ANSI/NIST-ITL 1-2011	มาตรฐานนี้ไม่บังคับให้เข้ารหัสในรูปแบบใด ๆ แต่ในกรณีที่มีการเข้ารหัสทางเลือกที่ไม่ใช่แบบปกติหรือ XML หน่วยงานที่ส่งและรับจะต้องมีรายละเอียดการเข้ารหัสและสมมุติฐาน เพิ่มเติมรายละเอียดข้อมูล DNA ลายฝ่าเท้า (Plantar image) และข้อมูลแทนต้นทาง (Source Representation) เช่น ภาพที่มีหลายลายนิ้วมือแฝง หรือ ภาพและเสียงหรือวีดิทัศน์
ธ.ค. 2556	ANSI/NIST-ITL 1-2011 (Update 2013)	เพิ่มส่วนที่เป็นเสียง (Voice) ข้อมูลเกี่ยวกับฟัน (Dental) และภาพที่ไม่ใช่ภาพสองมิติ
ธ.ค. 2558	ANSI/NIST-ITL 1-2011 (Update 2015)	มีการปรับปรุงแก้ไขส่วนต่างๆ ให้ทันสมัย แต่เป็นการแก้เล็กน้อย แต่ส่วนไบโอเมตริกยังคงเดิม เวอร์ชันนี้เป็นเวอร์ชันปัจจุบัน

มาตรฐานของ NIST มีวัตถุประสงค์เพื่อต้องการให้การแลกเปลี่ยนข้อมูล ระหว่างกระบวนการยุติธรรมหรือระบบ AFIS (Automated Fingerprint Identification Systems) ที่มาจากหลากหลายบริษัท สามารถแลกเปลี่ยนข้อมูลระหว่างกันได้โดยใช้มาตรฐานเดียวกัน และเนื่องจากมาตรฐานล่าสุด ANSI/NIST-ITL 1-2011 (Update 2015) Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information [NIST-ITL2011] ของ NIST กำหนดเกี่ยวกับข้อมูลไบโอเมตริกที่ใช้ในการสืบหาตัวตน และสารสนเทศทางชีวภาพในทางนิติวิทยาศาสตร์ ที่มีหลายมิติดังต่อไปนี้

(1) ภาพลายนิ้วมือแบบละเอียดหรือหยาบ สองระดับหรือระดับเทา (Fingerprint Images)

(2) ข้อมูลลายเซ็น (Signature)

(3) ข้อมูลมินูเทียร์ในภาพลายนิ้วมือ (Minutiae) (ดูรายละเอียดคำอธิบายในบทที่ 1.2)

(4) ภาพถ่ายส่วนต่าง ๆ ของร่างกาย (Body Part Images) รวมทั้งภาพใบหน้า รอยตำหนิ แผลเป็น และรอยสัก (Facial Image & Scar, Mark and Tattoo (SMT))

(5) ข้อมูลเสียงพูด (Voice)
(6) ข้อมูลฟันและปาก (Dental & Oral)
(7) ภาพลายนิ้วมือแฝง (Latent Fingerprint Images)
(8) ภาพลายฝ่ามือ (Palm Print Images)
(9) ภาพผู้ใช้กำหนด (User Defined Image)
(10) ภาพม่านตา (Iris Image)
(11) ข้อมูลดีเอ็นเอ (DNA)
(12) ภาพลายฝ่าเท้า (Plantar Image)
(13) ข้อมูลแทนต้นทาง (Source Representation)
(14) ข้อมูลภาพที่ไม่ใช่สองมิติ (Non-photographic image Data)

โดยมาตรฐานทั้งหมดของ NIST สามารถ Download ได้จาก Website [34] โดยตรงโดยไม่เสียค่าใช้จ่าย มาตรฐาน NIST เป็นมาตรฐานพื้นฐานที่เน้นการใช้งานทางด้านนิติวิทยาศาสตร์ โดยใช้ในหน่วยงาน FBI คือมาตรฐาน FBI's EFTS/EBTS และหน่วยงานตำรวจสากล Interpol ในมาตรฐาน Interpol's INT-I

[34] https://www.nist.gov/publications/data-format-interchange-fingerprint-facial-other-biometric-information-ansinist-itl-1-1

4.2 ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission)

คณะกรรมการ International Organization for Standardization (ISO) ได้ร่วมกับคณะกรรมการของ International Electrotechnical Commission (IEC) จัดตั้งคณะกรรมการร่วม (Joint Technical Committee (JTC)) เรียกว่า ISO/IEC JTC 1 ขึ้นในปี พ.ศ. 2530 (ค.ศ. 1987) ซึ่งเป็นคณะกรรมการที่ใช้ในการร่างมาตรฐานที่เกี่ยวข้องกับเทคโนโลยีข้อมูล (Information Technology) โดยได้ตั้งคณะอนุกรรมการเป็นกลุ่มย่อย ๆ อีก เรียกว่า SubGroup (SG) และเรียงหมายเลขตามการก่อตั้งของแต่ละกลุ่มย่อย ๆ ซึ่งถ้ากลุ่มใดล้มเลิกไป เลขกลุ่มที่กำหนดแล้วจะไม่ถูกใช้อีก ปัจจุบันมีทั้งหมด 22 กลุ่มย่อย โดยมีหัวเรื่องของกลุ่มย่อยดังตารางที่ 11 โดยคณะอนุกรรมการที่ดูแลออกมาตรฐานเกี่ยวข้องกับไบโอเมตริกโดยตรงคือ คณะอนุกรรมการ ISO/IEC JTC 1/ SC37

ตารางที่ 11 คณะอนุกรรมการในกลุ่มย่อย (SubGroup (SG)) ต่าง ๆ ของ ISO/IEC JTC1

#	Subcommittee/Working Group	Title
1	ISO/IEC JTC 1/SC 2	Coded character sets
2	ISO/IEC JTC 1/SC 6	Telecommunications and information exchange between systems
3	ISO/IEC JTC 1/SC 7	Software and systems engineering
4	ISO/IEC JTC 1/SC 17	Cards and personal identification
5	ISO/IEC JTC 1/SC 22	Programming languages, their environments and system software interfaces
6	ISO/IEC JTC 1/SC 23	Digitally Recorded Media for Information Interchange and Storage
7	ISO/IEC JTC 1/SC 24	Computer graphics, image processing and environmental data representation
8	ISO/IEC JTC 1/SC 25	Interconnection of information technology equipment
9	ISO/IEC JTC 1/SC 27	IT Security techniques
10	ISO/IEC JTC 1/SC 28	Office equipment
11	ISO/IEC JTC 1/SC 29	Coding of audio, picture, multimedia and hypermedia information
12	ISO/IEC JTC 1/SC 31	Automatic identification and data capture techniques
13	ISO/IEC JTC 1/SC 32	Data management and interchange
14	ISO/IEC JTC 1/SC 34	Document description and processing languages
15	ISO/IEC JTC 1/SC 35	User interfaces
16	ISO/IEC JTC 1/SC 36	Information technology for learning, education and training
17	**ISO/IEC JTC 1/SC 37**	**Biometrics**
18	ISO/IEC JTC 1/SC 38	Cloud computing and distributed platforms
19	ISO/IEC JTC 1/SC 39	Sustainability, IT and data centres
20	ISO/IEC JTC 1/SC 40	IT service management and IT governance
21	ISO/IEC JTC 1/SC 41	Internet of things and digital twin
22	ISO/IEC JTC 1/SC 42	Artificial intelligence

คณะอนุกรรมการ ISO/IEC JTC 1/ SC37 Biometrics

คณะอนุกรรมการ ISO/IEC JTC 1/ SC37 Biometrics ได้ก่อตั้งขึ้นเมื่อเดือนมิถุนายน พ.ศ. 2545 (ค.ศ. 2002) โดยมีเป้าหมายหลักในการ *"ให้ความสำคัญสูงสุดและให้ความสนใจสูงสุดในการพัฒนามาตรฐานที่เกี่ยวข้องกับไบโอเมตริกทั้งหมดอย่างครอบคลุมครบถ้วน"*

ขอบเขตของคณะอนุกรรมการ ISO/IEC JTC 1/ SC37 Biometrics คือ *"การกำหนดมาตรฐานเทคโนโลยีไบโอเมตริกทั่วไปที่เกี่ยวข้องกับมนุษย์ เพื่อที่จะสนับสนุนการทำงานร่วมกัน การแลกเปลี่ยนข้อมูลระหว่างระบบ และการนำไปประยุกต์ใช้งาน"*

คณะอนุกรรมการ ISO/IEC JTC 1/ SC37 ไม่ได้ทำงานตามลำพัง แต่ได้ติดต่อประสานงานภายใน (Internal Liaisons) ร่วมกับคณะอนุกรรมการชุดอื่นใน ISO/IEC ดังแสดงในตารางที่ 12

ตารางที่ 12 คณะอนุกรรมการกลุ่มย่อยที่ทำงานร่วมกับคณะอนุกรรมการ ISO/IEC JTC 1/ SC37 Biometric ภายในองค์กร ISO/IEC

Subcommittee/ Working Group	Title	To SC37 Liaisons*	From SC37 Liaisons**
IEC/SC 3C	Graphical symbols for use on equipment	✓	✓
ISO/IEC JTC 1	Information technology	✗	✓
ISO/IEC JTC 1/SC 6	Telecommunications and information exchange between systems	✓	✗
ISO/IEC JTC 1/SC 7	Software and systems engineering	✓	✓
ISO/IEC JTC 1/SC 17	Cards and security devices for personal identification	✓	✓
ISO/IEC JTC 1/SC 27	Information security, cybersecurity and privacy protection	✓	✓
ISO/IEC JTC 1/SC 31	Automatic identification and data capture techniques	✗	✓
ISO/IEC JTC 1/SC 35	User interfaces	✓	✗
ISO/IEC JTC 1/SC 38	Cloud computing and distributed platforms	✓	✗
ISO/IEC JTC 1/SC 42	Artificial intelligence	✓	✓
ISO/TC 68/SC 2	Financial Services, security	✓	✓
ISO/TC 68/SC 8	Reference data for financial services	✗	✓
ISO/TC 272	Forensic sciences	✓	✓
ISO/TC 292	Security and resilience	✓	✗
ISO/TC 307	Blockchain and distributed ledger technologies	✓	✓

หมายเหตุ

- **To SC37 Liaisons*** หมายถึง คณะอนุกรรมการ ISO/IEC JTC 1/ SC37 สามารถเข้าถึงข้อมูลเอกสารต่าง ๆ รวมทั้งร่างมาตรฐานของคณะกรรมการหรือคณะอนุกรรมการกลุ่มอื่น ๆ ใน ISO/IEC นั้น ๆ ได้ ถ้ามีเครื่องหมาย "✓" ในช่องนี้ และไม่สามารถเข้าถึงข้อมูลเอกสารต่าง ๆ ของกรรมการชุดอื่น ๆ ได้ถ้ามีเครื่องหมาย "✗" ในช่องนี้
- **From SC37 Liaisons**** หมายถึง คณะกรรมการหรือคณะอนุกรรมการกลุ่มอื่น ๆ ใน ISO/IEC สามารถเข้าถึงข้อมูลเอกสารต่าง ๆ รวมทั้งร่างมาตรฐานของคณะอนุกรรมการ ISO/IEC JTC 1/ SC37 ได้ ถ้ามีเครื่องหมาย "✓" ในช่องนี้ และไม่สามารถเข้าถึงข้อมูลเอกสารของคณะอนุกรรมการ ISO/IEC JTC 1/ SC37 ได้ ถ้ามีเครื่องหมาย "✗" ในช่องนี้

นอกจากการทำงานร่วมกันของคณะกรรมการภายในองค์กร ISO และ IEC แล้ว คณะอนุกรรมการ ISO/IEC JTC 1/ SC37 ยังติดต่อประสานงานและทำงานร่วมกับองค์กรอื่นๆ ภายนอก (Organizations in Liaison) ดังแสดงในตารางที่ 13

ตารางที่ 13 องค์กรภายนอกต่าง ๆ ที่ทำงานร่วมกับคณะอนุกรรมการ ISO/IEC JTC 1/ SC37 Biometric

Organizations	Title	Category
FIDO Alliance	The FIDO (Fast IDentity Online) Alliance	A
IATA	International Air Transport Association	A
IBIA - Biometric	International Biometrics + Identity Association	A
EC - European Commission	European Commission	C
FRONTEX	FRONTEX	C
Interpol	Interpol	C

หมายเหตุ

- **Category A**: เป็นองค์กรสนับสนุนการทำงานของคณะกรรมการทางเทคนิคหรือคณะอนุกรรมการ โดยมีการเชิญเข้าประชุมและส่งเอกสารที่เกี่ยวข้องให้รับทราบและพิจารณา และจะส่งตัวแทนผู้เชี่ยวชาญเข้าร่วมใน Working Group (WG) ด้วย
- **Category C**: องค์กรที่ประสานงานที่มีส่วนร่วมในระดับ Working Group

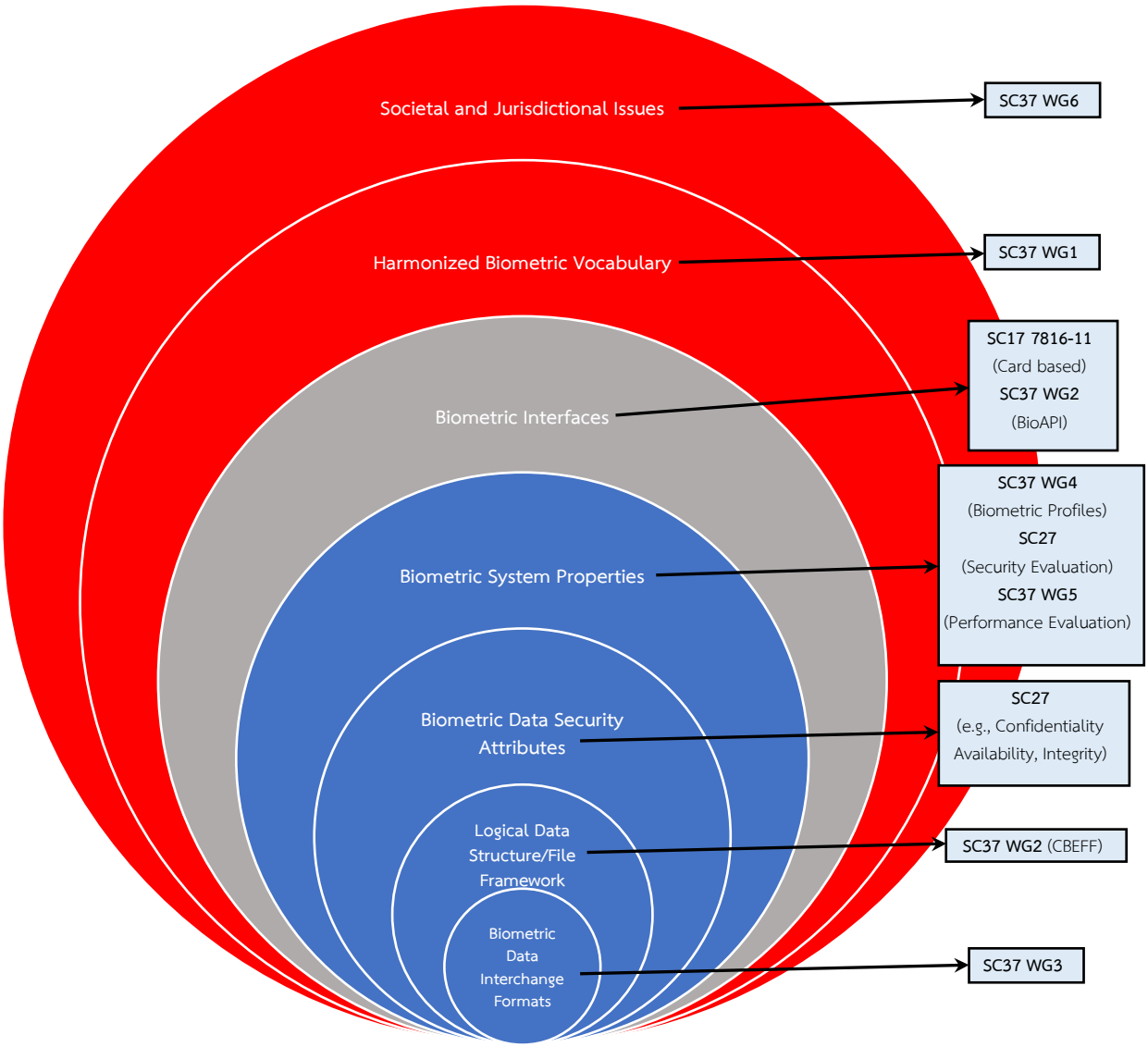
คณะอนุกรรมการ ISO/IEC JTC 1/ SC37 มีสมาชิกมาจากประเทศต่าง ๆ ทั่วโลก โดยประเทศที่เป็นสมาชิกจะส่งตัวแทนประเทศ (National Body) เข้าร่วมประชุมทำงานกำหนดมาตรฐาน ซึ่งจะมีการประชุมปีละสองครั้ง คือ เดือนมกราคม และเดือนกรกฎาคม ของทุกปี โดยสมาชิกจะมีอยู่สองประเภท ได้แก่

1) **สมาชิกผู้มีส่วนร่วม (Participating Member)** โดยมีหน้าที่เข้าร่วมประชุม ทำงาน ให้ความเห็น และลงคะแนน ปัจจุบันมีตัวแทนจาก 28 ประเทศ โดยมีตัวแทนจากประเทศสหรัฐอเมริกาเป็นเลขาธิการ ภาพที่ 64 แสดงสมาชิกผู้มีส่วนร่วมด้วยสีฟ้าขุ่น และเลขาธิการเป็นสีน้ำเงินเข้ม
2) **สมาชิกผู้สังเกตการณ์ (Observing Member)** ปัจจุบันมีทั้งหมด 21 ประเทศ ซึ่งรวมทั้งประเทศไทยด้วย โดยประเทศไทยได้เข้าร่วมเป็นสมาชิกตั้งแต่ปี พ.ศ. 2552 (ค.ศ. 2009) จนถึงปัจจุบัน ภาพที่ 64 แสดงสมาชิกผู้สังเกตการณ์ด้วยสีส้ม

ภาพที่ 64 ประเทศที่เข้าร่วมเป็นสมาชิกของคณะอนุกรรมการ ISO/IEC JTC 1/ SC37 ในปัจจุบัน (ตุลาคม พ.ศ. 2564) (ภาพจาก [35])

ในคณะกรรมการ ISO/IEC JTC 1/ SC37 Biometrics ได้แบ่งกลุ่มย่อยทั้งหมด 6 กลุ่ม เรียกว่าคณะทำงาน (Working Group (WG)) โดยมี WG1, WG2, WG3, WG4, WG5, และ WG6 โดยแต่ละกลุ่มจะมีหน้าที่เฉพาะกลุ่ม ซึ่งสามารถแสดงด้วยแผนภาพชั้นของหัวหอม (Onion Layer) ดังภาพที่ 65

[35] https://www.iso.org/committee/313770.html?view=participation



ภาพที่ 65 แผนภาพชั้นหัวหอมของคณะทำงานหกกลุ่ม (WG1-6) ในคณะอนุกรรมการ ISO/IEC JTC 1/SC37

โดยแต่ละกลุ่มคณะทำงาน (Working Group (WG)) สามารถกำหนดเป้าหมาย แจกแจงหน้าที่ และตัวอย่างมาตรฐานที่ได้กำหนดออกมาแล้วดังต่อไปนี้

4.2.1 คณะทำงานกลุ่มที่ 1 ประมวลคำศัพท์ไบโอเมตริก (WG1: Harmonized Biometric Vocabulary)

เป้าหมายหลักของคณะทำงานกลุ่มที่ 1 หรือ WG1 คือ *"ทำให้ภาษากลมกลืนและถูกต้อง"* (Getting the language harmonized and correct)

หน้าที่ของคณะทำงานกลุ่มที่ 1 (WG1)

1) สร้างเอกสารเกี่ยวกับคำศัพท์และคำนิยามเพื่อใช้งานกับมาตรฐาน SC37 ทั้งหมด
2) กำหนดกระบวนการสำหรับการให้การยอมรับหรือการพัฒนาคำศัพท์และคำนิยามที่อ้างอิงไว้ในมาตรฐาน ISO/IEC ตามความเหมาะสม
3) ระบุต้นกำเนิดของคำศัพท์และคำนิยามสำหรับความเป็นไปได้ในการใช้งานในรายการคำศัพท์สำหรับ SC37
4) ลดความกำกวมในคำศัพท์และคำนิยามในมาตรฐาน SC37 ซึ่งเกิดจากความแตกต่างทางวัฒนธรรม

ตัวอย่างมาตรฐานที่กำหนดโดยคณะทำงานกลุ่มที่ 1 (WG1)

1) ISO/IEC 2382-37: Information Technology — Vocabulary — Part 37: Biometrics

4.2.2 คณะทำงานกลุ่มที่ 2 ส่วนต่อประสานเชิงเทคนิคไบโอเมตริก (WG2: Biometric Technical Interfaces)

เป้าหมายหลักของคณะทำงานกลุ่มที่ 2 หรือ WG2 คือ *"ทำให้อุปกรณ์สามารถคุยกันได้"* (Getting equipment to talk together)

หน้าที่ของคณะทำงานกลุ่มที่ 2 (WG2)

1) กำหนดมาตรฐานสำหรับทุกการเชื่อมต่อและการทำงานร่วมกันระหว่างอุปกรณ์ไบโอเมตริกและระบบย่อย
2) การผนวกรวมของความเป็นไปได้ในการใช้กลไกรักษาความปลอดภัยเพื่อที่จะป้องกันข้อมูลที่เก็บและข้อมูลที่ส่งผ่านกันระหว่างระบบ
3) แบบจำลองอ้างอิงสำหรับสถาปัตยกรรมและปฏิบัติการของระบบไบโอเมตริก
4) มาตรฐานที่จำเป็นเพื่อที่จะสนับสนุนระบบที่มีการรวมกันของอุปกรณ์จากหลากหลายบริษัทและการประยุกต์ใช้งาน

ตัวอย่างมาตรฐานที่กำหนดโดยคณะทำงานกลุ่มที่ 2 (WG2)

1) ISO/IEC 19784-X: Information Technology — Biometric application programming interface (BioAPI)
2) ISO/IEC 19785-X: Information Technology — Common Biometric Exchange Formats Framework (CBEFF)
3) ISO/IEC 24709-X: Information Technology — Conformance testing for the biometric application programming interface (BioAPI)
4) ISO/IEC 30106-X: Information Technology — Object oriented BioAPI

4.2.3 คณะทำงานกลุ่มที่ 3 การแลกเปลี่ยนข้อมูลไบโอเมตริก (WG3: Biometric Data Interchange)

เป้าหมายหลักของคณะทำงานกลุ่มที่ 3 หรือ WG3 คือ *"ทำให้อุปกรณ์เข้าใจซึ่งกันและกัน"* (Getting equipment to understand each other)

หน้าที่ของคณะทำงานกลุ่มที่ 3 (WG3)

1) การกำหนดมาตรฐานสำหรับ เนื้อหา ความหมาย และการแทน สำหรับรูปแบบข้อมูลไบโอเมตริก ซึ่งกำหนดให้เฉพาะเจาะจงกับแต่ละเทคโนโลยีไบโอเมตริก
2) กำหนดมาตรฐานโครงสร้างข้อมูลไบโอเมตริกโดยทั่วไป
3) กำหนดเครื่องหมายหรือสัญลักษณ์และรูปแบบการส่งผ่าน เพื่อที่จะทำให้แพลตฟอร์มเป็นอิสระ และแยก transfer syntax ออกจากนิยามเนื้อหา

ตัวอย่างมาตรฐานที่กำหนดโดยคณะทำงานกลุ่มที่ 3 (WG3)

1) ISO/IEC 19794-X: Information Technology — Biometric data interchange formats
2) ISO/IEC 29109-X: Information Technology — Conformance testing methodology for biometric data interchange formats
3) ISO/IEC 29794-X: Information Technology — Biometric sample quality
4) ISO/IEC 30107-X: Information Technology — Biometric presentation attack detection
5) ISO/IEC 39794-X: Information Technology — Extensible biometric data interchange formats

4.2.4 คณะทำงานกลุ่มที่ 4 สถาปัตยกรรมการทำงานของไบโอเมตริกและโพรไฟล์ที่เกี่ยวข้อง (WG4: Biometric Functional Architecture and Related Profiles)

เป้าหมายหลักของคณะทำงานกลุ่มที่ 4 หรือ WG4 คือ *"ทำให้เข้ากับวัตถุประสงค์"* (Making it fit the purpose)

หน้าที่ของคณะทำงานกลุ่มที่ 4 (WG4)

1) สถาปัตยกรรมการทำงานของไบโอเมตริกและโพรไฟล์ที่เกี่ยวข้อง ซึ่งรวมมาตรฐานไบโอเมตริกและมาตรฐานที่เกี่ยวข้องในแนวทางที่สอดคล้องกันพร้อมด้วยบล็อกการทำงานของระบบไบโอเมตริก
2) โพรไฟล์ที่ระบุมาตรฐานที่มีความสัมพันธ์กับไบโอเมตริกอย่างตรงประเด็น

ตัวอย่างมาตรฐานที่กำหนดโดยคณะทำงานกลุ่มที่ 4 (WG4)

1) ISO/IEC 24713-X: Information Technology — Biometric profiles for interoperability and data interchange

4.2.5 คณะทำงานกลุ่มที่ 5 การทดสอบและการรายงานผลไบโอเมตริก (WG5: Biometric Testing and Reporting)

เป้าหมายหลักของคณะทำงานกลุ่มที่ 5 หรือ WG5 คือ *"ทำอย่างไรจึงตรวจสอบได้ว่าระบบสามารถทำงานได้"* (How to check it works)

หน้าที่ของคณะทำงานกลุ่มที่ 5 (WG5)

1) การทดสอบและการรายงานระเบียบวิธีและการวัดผลครอบคลุมเทคโนโลยีไบโอเมตริก ระบบ และ ส่วนประกอบ
2) ร่างการทำงานสำหรับโครงงานผ่านการเห็นชอบที่เกี่ยวข้องกับการทดสอบและการรายงานผลไบโอเมตริก

ตัวอย่างมาตรฐานที่กำหนดโดยคณะทำงานกลุ่มที่ 5 (WG5)

1) ISO/IEC 19795-X: Information Technology — Biometric performance testing and reporting
2) ISO/IEC 29197: Information Technology — Evaluation methodology for environmental influence in biometric system performance

4.2.6 คณะทำงานกลุ่มที่ 6 มุมมองทางสังคมและการข้ามเขตอำนาจ (WG6: Cross-Jurisdictional and Societal Aspects)

เป้าหมายหลักของคณะทำงานกลุ่มที่ 6 หรือ WG6 คือ *"ทำให้ได้รับการยอมรับ"* (Making it acceptable)

หน้าที่ของคณะทำงานกลุ่มที่ 6 (WG6)

1) สนับสนุนการออกแบบและการทำให้เกิดผลในทางปฏิบัติของเทคโนโลยีไบโอเมตริก ทางด้านความสามารถในการเข้าถึง สุขภาพและความปลอดภัย และสนับสนุนความต้องการที่ถูกกฎหมาย
2) สร้างการยอมรับของข้อพิจารณาทางสังคมและอำนาจทางกฎหมาย เกี่ยวกับข้อมูลส่วนบุคคล

ตัวอย่างมาตรฐานที่กำหนดโดยคณะทำงานกลุ่มที่ 6 (WG6)

1) ISO/IEC 24779-X: IT — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems
2) ISO/IEC TR 24714-X: IT — Biometrics — Jurisdictional and societal considerations for commercial applications
3) ISO/IEC TR 30110: IT — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children

ขั้นตอนวิธีการกำหนดมาตรฐาน

การกำหนดมาตรฐาน เริ่มจากการยื่นข้อเสนอ (Project Proposal) มาเป็นร่างมาตรฐาน (Draft Standard) ซึ่งขั้นตอนนี้จะแยกย่อยออกเป็น ร่างทำงาน (Working Draft) ร่างคณะกรรมการ (Committee Draft) ร่างมาตรฐาน (Draft International Standard) และร่างสุดท้าย (Final Draft International Standard) ซึ่งเกิดจากการเขียน แก้ไข และข้อเสนอแนะของคณะกรรมการวนไปจนกว่าจะได้รับการลงความเห็นยอมรับจากคณะกรรมการทั้งหมด จากนั้น จะเข้าสู่การอนุมัติโดยสมาชิก (Member Body Approval) และออกพิมพ์เป็นมาตรฐาน (Published Standard) ในขั้นตอนสุดท้าย

การกำหนดมาตรฐานไบโอเมตริกในปัจจุบัน จะเป็นหน้าที่หลักของ ISO/IEC JTC1/SC37 โดยเน้นการใช้งานทั่วไปทางการบริหารอัตลักษณ์ (Identity Management) โดยมีเป้าหมายการใช้งานควบคุมการเข้าออกระหว่างประเทศ (Border Control) และทางด้านนิติวิทยาศาสตร์ตามมาในอนาคตอันใกล้ ปัจจุบันมีมาตรฐานที่สำเร็จสมบูรณ์ทั้งหมด 137 มาตรฐานในปัจจุบัน (ตรวจสอบเมื่อ 12 พฤศจิกายน 2564) ซึ่งแสดงอยู่ในตารางที่ 14 และมาตรฐานที่กำลังอยู่ในระหว่างการพิจารณาอีก 22 มาตรฐานสรุปอยู่ในตารางที่ 15 ซึ่งรายละเอียดสามารถดูได้จาก[36]

[36] https://www.iso.org/committee/313770/x/catalogue/p/1/u/0/w/0/d/0

ตารางที่ 14 มาตรฐาน ISO/IEC JTC1/ SC37 Biometric ทั้งหมดที่ออกมาในปัจจุบัน (137 มาตรฐาน ตรวจสอบเมื่อ 12 พฤศจิกายน พ.ศ. 2564)

#	ISO/IEC #	Title
1	ISO/IEC 2382-37:2017	IT — Vocabulary — Part 37: Biometrics
2	ISO/IEC 19784-1:2018	IT — Biometric application programming interface — Part 1: BioAPI specification
3	ISO/IEC 19784-2:2007	IT -- Biometric application programming interface -- Part 2: Biometric archive function provider interface
4	ISO/IEC 19784-2:2007/COR 1:2011	IT — Biometric application programming interface — Part 2: Biometric archive function provider interface — Technical Corrigendum 1
5	ISO/IEC 19784-2:2007/COR 2:2013	IT — Biometric application programming interface — Part 2: Biometric archive function provider interface — Technical Corrigendum 2
6	ISO/IEC 19784-4:2011	IT — Biometric application programming interface — Part 4: Biometric sensor function provider interface
7	ISO/IEC 19784-4:2011/COR 1:2013	IT — Biometric application programming interface — Part 4: Biometric sensor function provider interface — Technical Corrigendum 1
8	ISO/IEC 19785-1:2020	IT — Common Biometric Exchange Formats Framework — Part 1: Data element specification
9	ISO/IEC 19785-2:2006	IT — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority
10	ISO/IEC 19785-2:2006/AMD 1:2010	IT — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority — Amendment 1: Additional registrations
11	ISO/IEC 19785-3:2020	IT — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications
12	ISO/IEC 19785-4:2010	IT — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications
13	ISO/IEC 19785-4:2010/COR 1:2013	IT — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications — Technical Corrigendum 1
14	ISO/IEC 19794-1:2006	IT — Biometric data interchange formats — Part 1: Framework
15	ISO/IEC 19794-1:2011	IT — Biometric data interchange formats — Part 1: Framework
16	ISO/IEC 19794-1:2011/AMD 1:2013	IT — Biometric data interchange formats — Part 1: Framework — Amendment 1: Conformance testing methodology
17	ISO/IEC 19794-1:2011/AMD 2:2015	IT — Biometric data interchange formats — Part 1: Framework — Amendment 2: Framework for XML encoding
18	ISO/IEC 19794-2:2005	IT — Biometric data interchange formats — Part 2: Finger minutiae data
19	ISO/IEC 19794-2:2005/AMD 1:2010	IT — Biometric data interchange formats — Part 2: Finger minutiae data — Amendment 1: Detailed description of finger minutiae location, direction, and type
20	ISO/IEC 19794-2:2005/COR 1:2009	IT — Biometric data interchange formats — Part 2: Finger minutiae data — Technical Corrigendum 1
21	ISO/IEC 19794-2:2005/AMD 1:2010/COR 2:2014	IT — Biometric data interchange formats — Part 2: Finger minutiae data — Amendment 1: Detailed description of finger minutiae location, direction, and type — Technical Corrigendum 2
22	ISO/IEC 19794-2:2011	IT — Biometric data interchange formats — Part 2: Finger minutiae data
23	ISO/IEC 19794-2:2011/AMD 1:2013	IT — Biometric data interchange formats — Part 2: Finger minutiae data — Amendment 1: Conformance testing methodology and clarification of defects
24	ISO/IEC 19794-2:2011/COR 1:2012	IT — Biometric data interchange formats — Part 2: Finger minutiae data — Technical Corrigendum 1
25	ISO/IEC 19794-2:2011/AMD 2:2015	IT — Biometric data interchange formats — Part 2: Finger minutiae data — Amendment 2: XML encoding and clarification of defects
26	ISO/IEC 19794-3:2006	IT — Biometric data interchange formats — Part 3: Finger pattern spectral data
27	ISO/IEC 19794-4:2005	IT — Biometric data interchange formats — Part 4: Finger image data
28	ISO/IEC 19794-4:2005/COR 1:2011	IT — Biometric data interchange formats — Part 4: Finger image data — Technical Corrigendum 1
29	ISO/IEC 19794-4:2011	IT — Biometric data interchange formats — Part 4: Finger image data
30	ISO/IEC 19794-4:2011/AMD 1:2013	IT — Biometric data interchange formats — Part 4: Finger image data — Amendment 1: Conformance testing methodology and clarification of defects
31	ISO/IEC 19794-4:2011/COR 1:2012	IT — Biometric data interchange formats — Part 4: Finger image data — Technical Corrigendum 1
32	ISO/IEC 19794-4:2011/AMD 2:2015	IT — Biometric data interchange formats — Part 4: Finger image data — Amendment 2: XML encoding and clarification of defects
33	ISO/IEC 19794-5:2005	IT — Biometric data interchange formats — Part 5: Face image data
34	ISO/IEC 19794-5:2011	IT — Biometric data interchange formats — Part 5: Face image data
35	ISO/IEC 19794-5:2011/AMD 1:2014	IT — Biometric data interchange formats — Part 5: Face image data — Amendment 1: Conformance testing methodology and clarification of defects
36	ISO/IEC 19794-5:2011/AMD 2:2015/COR 1:2016	IT — Biometric data interchange formats — Part 5: Face image data — Amendment 2: XML encoding and clarification of defects — Technical Corrigendum 1

#	ISO/IEC #	Title
37	ISO/IEC 19794-5:2011/AMD 2:2015	IT — Biometric data interchange formats — Part 5: Face image data — Amendment 2: XML encoding and clarification of defects
38	ISO/IEC 19794-6:2005	IT — Biometric data interchange formats — Part 6: Iris image data
39	ISO/IEC 19794-6:2011	IT — Biometric data interchange formats — Part 6: Iris image data
40	ISO/IEC 19794-6:2011/AMD 1:2015	IT — Biometric data interchange formats — Part 6: Iris image data — Amendment 1: Conformance testing methodology and clarification of defects
41	ISO/IEC 19794-6:2011/COR 1:2012	IT — Biometric data interchange formats — Part 6: Iris image data — Technical Corrigendum 1
42	ISO/IEC 19794-6:2011/AMD 2:2016	IT — Biometric data interchange formats — Part 6: Iris image data — Amendment 2: XML encoding and clarification of defects
43	ISO/IEC 19794-7:2014	IT — Biometric data interchange formats — Part 7: Signature/sign time series data
44	ISO/IEC 19794-7:2014/AMD 1:2015	IT — Biometric data interchange formats — Part 7: Signature/sign time series data — Amendment 1: XML encoding
45	ISO/IEC 19794-7:2021	IT — Biometric data interchange formats — Part 7: Signature/sign time series data
46	ISO/IEC 19794-8:2006	IT — Biometric data interchange formats — Part 8: Finger pattern skeletal data
47	ISO/IEC 19794-8:2006/COR 1:2011	IT — Biometric data interchange formats — Part 8: Finger pattern skeletal data — Technical Corrigendum 1
48	ISO/IEC 19794-8:2011	IT — Biometric data interchange formats — Part 8: Finger pattern skeletal data
49	ISO/IEC 19794-8:2011/AMD 1:2014	IT — Biometric data interchange formats — Part 8: Finger pattern skeletal data — Amendment 1: Conformance testing methodology
50	ISO/IEC 19794-8:2011/COR 1:2012	IT — Biometric data interchange formats — Part 8: Finger pattern skeletal data — Technical Corrigendum 1
51	ISO/IEC 19794-9:2007	IT — Biometric data interchange formats — Part 9: Vascular image data
52	ISO/IEC 19794-9:2011	IT — Biometric data interchange formats — Part 9: Vascular image data
53	ISO/IEC 19794-9:2011/AMD 1:2013	IT — Biometric data interchange formats — Part 9: Vascular image data — Amendment 1: Conformance testing methodology
54	ISO/IEC 19794-9:2011/COR 1:2012	IT — Biometric data interchange formats — Part 9: Vascular image data — Technical Corrigendum 1
55	ISO/IEC 19794-9:2011/AMD 2:2015	IT — Biometric data interchange formats — Part 9: Vascular image data — Amendment 2: XML Encoding and clarification of defects
56	ISO/IEC 19794-10:2007	IT — Biometric data interchange formats — Part 10: Hand geometry silhouette data
57	ISO/IEC 19794-11:2013	IT — Biometric data interchange formats — Part 11: Signature/sign processed dynamic data
58	ISO/IEC 19794-11:2013/AMD 1:2014	IT — Biometric data interchange formats — Part 11: Signature/sign processed dynamic data — Amendment 1: Conformance test assertions
59	ISO/IEC 19794-13:2018	IT — Biometric data interchange formats — Part 13: Voice data
60	ISO/IEC 19794-14:2013	IT — Biometric data interchange formats — Part 14: DNA data
61	ISO/IEC 19794-14:2013/AMD 1:2016	IT — Biometric data interchange formats — Part 14: DNA data — Amendment 1: Conformance testing and clarification of defects
62	ISO/IEC 19794-15:2017	IT — Biometric data interchange format — Part 15: Palm crease image data
63	ISO/IEC 19795-1:2021	IT — Biometric performance testing and reporting — Part 1: Principles and framework
64	ISO/IEC 19795-2:2007	IT — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation
65	ISO/IEC 19795-2:2007/AMD 1:2015	IT — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation — Amendment 1: Testing of multimodal biometric implementations
66	ISO/IEC TR 19795-3:2007	IT — Biometric performance testing and reporting — Part 3: Modality-specific testing
67	ISO/IEC 19795-4:2008	IT — Biometric performance testing and reporting — Part 4: Interoperability performance testing
68	ISO/IEC 19795-5:2011	IT — Biometric performance testing and reporting — Part 5: Access control scenario and grading scheme
69	ISO/IEC 19795-6:2012	IT — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation
70	ISO/IEC 19795-7:2011	IT — Biometric performance testing and reporting — Part 7: Testing of on-card biometric comparison algorithms
71	ISO/IEC TS 19795-9:2019	IT — Biometric performance testing and reporting — Part 9: Testing on mobile devices
72	ISO/IEC 20027:2018	IT — Guidelines for slap ten print fingerprint capture
73	ISO/IEC 21472:2021	IT — Scenario evaluation methodology for user interaction influence in biometric system performance
74	ISO/IEC TR 22116:2021	IT — A study of the differential impact of demographic factors in biometric recognition system performance
75	ISO/IEC 24708:2008	IT — Biometrics — BioAPI Interworking Protocol

#	ISO/IEC #	Title
76	ISO/IEC 24709-1:2017	IT — Conformance testing for the biometric application programming interface (BioAPI) — Part 1: Methods and procedures
77	ISO/IEC 24709-2:2007	IT — Conformance testing for the biometric application programming interface (BioAPI) — Part 2: Test assertions for biometric service providers
78	ISO/IEC 24709-3:2011	IT — Conformance testing for the biometric application programming interface (BioAPI) — Part 3: Test assertions for BioAPI frameworks
79	ISO/IEC 24713-1:2008	IT — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles
80	ISO/IEC 24713-2:2008	IT — Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports
81	ISO/IEC 24713-3:2009	IT — Biometric profiles for interoperability and data interchange — Part 3: Biometrics-based verification and identification of seafarers
82	ISO/IEC TR 24714-1:2008	IT — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance
83	ISO/IEC TR 24722:2015	IT — Biometrics — Multimodal and other multibiometric fusion
84	ISO/IEC TR 24741:2018	IT — Biometrics — Overview and application
85	ISO/IEC 24779-1:2016	IT — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 1: General principles
86	ISO/IEC 24779-4:2017	IT — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 4: Fingerprint applications
87	ISO/IEC 24779-5:2020	IT — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 5: Face applications
88	ISO/IEC 24779-9:2015	IT — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 9: Vascular applications
89	ISO/IEC 29109-1:2009	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 1: Generalized conformance testing methodology
90	ISO/IEC 29109-1:2009/COR 1:2010	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 1: Generalized conformance testing methodology — Technical Corrigendum 1
91	ISO/IEC 29109-2:2010	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 2: Finger minutiae data
92	ISO/IEC 29109-4:2010	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 4: Finger image data
93	ISO/IEC 29109-4:2010/COR 1:2011	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 4: Finger image data — Technical Corrigendum 1
94	ISO/IEC 29109-5:2019	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 5: Face image data
95	ISO/IEC 29109-6:2011	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 6: Iris image data
96	ISO/IEC 29109-7:2011	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 7: Signature/sign time series data
97	ISO/IEC 29109-8:2011	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 8: Finger pattern skeletal data
98	ISO/IEC 29109-9:2011	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 9: Vascular image data
99	ISO/IEC 29109-10:2010	IT — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 10: Hand geometry silhouette data
100	ISO/IEC 29120-1:2015	IT — Machine readable test data for biometric testing and reporting — Part 1: Test reports
101	ISO/IEC 29141:2009	IT — Biometrics — Tenprint capture using biometric application programming interface (BioAPI)
102	ISO/IEC TR 29144:2014	IT — Biometrics — The use of biometric technology in commercial Identity Management applications and processes
103	ISO/IEC TR 29156:2015	IT — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
104	ISO/IEC 29159-1:2010	IT — Biometric calibration, augmentation and fusion data — Part 1: Fusion information format
105	ISO/IEC 29164:2011	IT — Biometrics — Embedded BioAPI
106	ISO/IEC TR 29189:2015	IT — Biometrics — Evaluation of examiner assisted biometric applications
107	ISO/IEC TR 29194:2015	IT — Biometrics — Guide on designing accessible and inclusive biometric systems
108	ISO/IEC TR 29195:2015	Traveller processes for biometric recognition in automated border control systems
109	ISO/IEC TR 29196:2018	IT — Guidance for biometric enrolment
110	ISO/IEC 29197:2015	IT — Evaluation methodology for environmental influence in biometric system performance

#	ISO/IEC #	Title
111	ISO/IEC TR 29198:2013	IT — Biometrics — Characterization and measurement of difficulty for fingerprint databases for technology evaluation
112	ISO/IEC 29794-1:2016	IT — Biometric sample quality — Part 1: Framework
113	ISO/IEC 29794-4:2017	IT — Biometric sample quality — Part 4: Finger image data
114	ISO/IEC TR 29794-5:2010	IT — Biometric sample quality — Part 5: Face image data
115	ISO/IEC 29794-6:2015	IT — Biometric sample quality — Part 6: Iris image data
116	ISO/IEC 30106-1:2016	IT — Object oriented BioAPI — Part 1: Architecture
117	ISO/IEC 30106-1:2016/AMD 1:2019	IT — Object oriented BioAPI — Part 1: Architecture — Amendment 1: Additional specifications and conformance statements
118	ISO/IEC 30106-2:2020	IT — Object oriented BioAPI — Part 2: Java implementation
119	ISO/IEC 30106-3:2020	IT — Object oriented BioAPI — Part 3: C# implementation
120	ISO/IEC 30106-4:2019	IT — Object oriented BioAPI — Part 4: C++ implementation
121	ISO/IEC 30107-1:2016	IT — Biometric presentation attack detection — Part 1: Framework
122	ISO/IEC 30107-2:2017	IT — Biometric presentation attack detection — Part 2: Data formats
123	ISO/IEC 30107-3:2017	IT — Biometric presentation attack detection — Part 3: Testing and reporting
124	ISO/IEC 30107-4:2020	IT — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices
125	ISO/IEC 30108-1:2015	IT — Biometric Identity Assurance Services — Part 1: BIAS services
126	ISO/IEC TR 30110:2015	IT — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children
127	ISO/IEC TR 30125:2016	IT — Biometrics used with mobile devices
128	ISO/IEC 30136:2018	IT — Performance testing of biometric template protection schemes
129	ISO/IEC 30137-1:2019	IT — Use of biometrics in video surveillance systems — Part 1: System design and specification
130	ISO/IEC 30137-4:2021	IT — Use of biometrics in video surveillance systems — Part 4: Ground truth and video annotation procedure
131	ISO/IEC 39794-1:2019	IT — Extensible biometric data interchange formats — Part 1: Framework
132	ISO/IEC 39794-4:2019	IT — Extensible biometric data interchange formats — Part 4: Finger image data
133	ISO/IEC 39794-5:2019	IT — Extensible biometric data interchange formats — Part 5: Face image data
134	ISO/IEC 39794-6:2021	IT — Extensible biometric data interchange formats — Part 6: Iris image data
135	ISO/IEC 39794-9:2021	IT — Extensible biometric data interchange formats — Part 9: Vascular image data
136	ISO/IEC 39794-16:2021	IT — Extensible biometric data interchange formats — Part 16: Full body image data
137	ISO/IEC 39794-17:2021	IT — Extensible biometric data interchange formats — Part 17: Gait image sequence data

ตารางที่ 15 มาตรฐาน ISO/IEC JTC1/ SC37 Biometric ที่กำลังอยู่ในช่วงพัฒนา (22 มาตรฐาน เมื่อ 12 พฤศจิกายน พ.ศ. 2564)

#	ISO/IEC #	Title
1	ISO/IEC FDIS 2382-37	IT — Vocabulary — Part 37: Biometrics
2	ISO/IEC WD 5152	Biometric performance estimation methodologies using statistical model
3	ISO/IEC 19785-2	IT — Common Biometric Exchange Formats Framework — Part 2: Biometric registration authority
4	ISO/IEC WD 19785-4	IT — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications
5	ISO/IEC DIS 19794-14	IT — Biometric data interchange formats — Part 14: DNA data
6	ISO/IEC WD 19795-10	IT — Biometric performance testing and reporting — Part 10: Quantifying biometric system performance variation across demographic groups
7	ISO/IEC CD TR 20322.3	IT - Cross jurisdictional and societal aspects of implementation of biometric technologies - Biometrics and elderly people
8	ISO/IEC WD TS 21419	IT — Cross jurisdictional and societal aspects of implementation of biometric technologies — Use of biometrics for identity management in healthcare
9	ISO/IEC WD TS 22604	Biometric recognition of subjects in motion in access related systems
10	ISO/IEC WD TS 24358	Face-aware capture subsystem specifications
11	ISO/IEC DIS 24714	Biometrics — Cross-Jurisdictional and Societal Aspects of Biometrics — General Guidance
12	ISO/IEC CD 24741	IT — Biometrics — Overview and application
13	ISO/IEC DIS 29120-1	IT — Machine readable test data for biometric testing and reporting — Part 1: Test reports
14	ISO/IEC WD 29794-1	IT — Biometric sample quality — Part 1: Framework
15	ISO/IEC AWI 29794-4	IT — Biometric sample quality — Part 4: Finger image data

#	ISO/IEC #	Title
16	ISO/IEC WD 29794-5	IT — Biometric sample quality — Part 5: Face image data
17	ISO/IEC AWI 30107-1	IT — Biometric presentation attack detection — Part 1: Framework
18	ISO/IEC DIS 30107-3	IT — Biometric presentation attack detection — Part 3: Testing and reporting
19	ISO/IEC WD 30107-4	IT — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices
20	ISO/IEC WD 30108-2	IT — Biometric Identity Assurance Services — Part 2: REST-based implementation
21	ISO/IEC CD 39794-2.3	IT — Extensible biometric data interchange formats — Part 2: Finger minutiae data
22	ISO/IEC PRF TR 49794	IT – Transition examples from ISO/IEC 19794 First Edition to ISO/IEC 39794 for ID documents

4.3 ข้อสรุปและข้อเสนอแนะเกี่ยวกับมาตรฐานไบโอเมตริก

มาตรฐานไบโอเมตริกสากลปัจจุบันที่นิยมใช้กันอยู่มีสองมาตรฐาน คือ มาตรฐานไบโอเมตริก ISO/IEC JTC 1/SC37 ซึ่งใช้กับงานบริการประชาชน และ มาตรฐานไบโอเมตริก ANSI/NIST-ITL ที่ใช้กับงานทางด้านนิติวิทยาศาสตร์ การใช้งานมาตรฐานไบโอเมตริก จำเป็นต้องมีความเข้าใจวัตถุประสงค์และเป้าหมายของแต่ละมาตรฐานอย่างชัดเจน มีข้อควรระวังและข้อเสนอแนะดังต่อไปนี้

1) การกำหนดมาตรฐานเป็นเรื่องที่ต้องให้ความระมัดระวังเป็นอย่างมาก เนื่องจากอาจให้ทั้งผลดีผลเสียต่อส่วนรวม รวมทั้งปัญหาต่าง ๆ ที่ติดตามมาในอนาคตถ้าขาดความรอบคอบหรือรู้เท่าไม่ถึงการณ์ในการกำหนดมาตรฐาน
2) มาตรฐานที่เกี่ยวกับ Information Technology (IT) ต้องมีการปรับปรุงให้ทันสมัยอยู่เสมอ เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็ว มาตรฐานมีโอกาสล้าสมัยได้โดยง่าย และจะทำให้เป็นอุปสรรคในการทำตามมาตรฐาน ถ้ามาตรฐานนั้นล้าสมัย
3) การกำหนดมาตรฐานเพื่อบังคับใช้ จะเหมาะกับการใช้มาตรฐานสำหรับระบบที่ยังไม่เกิดขึ้น แต่ถ้ามีระบบแล้วและจะกำหนดมาตรฐานมากำกับ จะต้องมีช่วงเวลาเปลี่ยนผ่านและต้องมีงบประมาณสนับสนุนการเปลี่ยนผ่านด้วย

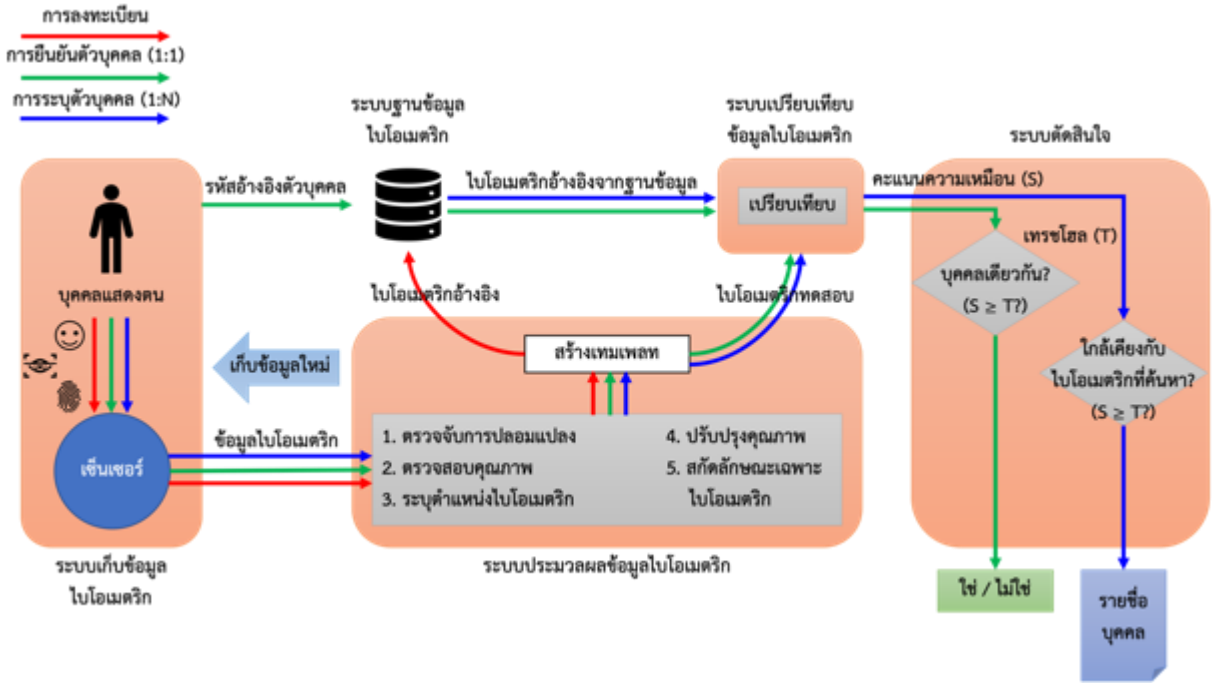
บทที่ 5

แนวทางการวัดสมรรถนะของระบบไบโอเมตริกและผลิตภัณฑ์ไบโอเมตริก

บทที่ 5. แนวทางการวัดสมรรถนะของระบบไบโอเมตริกและผลิตภัณฑ์ไบโอเมตริก

ความต้องการใช้งานระบบไบโอเมตริกสำหรับประยุกต์ใช้ในงานต่าง ๆ ถูกตั้งความหวังไว้สูงมาก ตั้งแต่เทคโนโลยีเริ่มพัฒนาจนถึงเทคโนโลยีไบโอเมตริกในปัจจุบัน ในช่วงแรกระบบไบโอเมตริกไม่สามารถตอบสนองความต้องการในงานประยุกต์บางอย่าง อาทิ งานด้านการควบคุมด่านชายแดนของประเทศต่าง ๆ ทั่วโลก เนื่องจากเทคโนโลยียังไม่พร้อมในการใช้งานสำหรับการดูแลประชากรเข้าออกระหว่างประเทศที่มีจำนวนประชากรมากได้ แต่ในปัจจุบันและอนาคต ปัญหาต่าง ๆ ที่เกิดขึ้นกำลังถูกแก้ไขและปรับปรุงจนถึงขั้นที่ใช้งานได้จริง ตามวัตถุประสงค์ของการนำไปประยุกต์ใช้

ระบบไบโอเมตริกโดยทั่วไปสามารถแบ่งการทำงานออกเป็น 3 ลักษณะ ได้แก่ การลงทะเบียน การยืนยันตัวบุคคล และการระบุตัวบุคคล [Jain2011], [ISO/IEC_19795-1] โดยอาศัยการทำงานร่วมกันระหว่างระบบย่อยต่าง ๆ ได้แก่ ระบบเก็บข้อมูลไบโอเมตริก ระบบประมวลผลข้อมูลไบโอเมตริก ฐานข้อมูลไบโอเมตริก ระบบเปรียบเทียบข้อมูลไบโอเมตริก และระบบตัดสินใจ ซึ่งภาพรวมของระบบและความแตกต่างการทำงานแต่ละลักษณะแสดงได้ดังภาพที่ 66 (โดยรายละเอียดของระบบย่อยแต่ละระบบอาจมีความแตกต่างกันตามไบโอเมตริกที่ใช้โดยสามารถอ้างอิงได้จากบทที่ 1)



ภาพที่ 66 ภาพรวมระบบไบโอเมตริก

โดยแต่ละลักษณะมีรายละเอียดการทำงานดังต่อไปนี้

1) **การลงทะเบียน (Enrollment)** เป็นการสร้างเทมเพลตไบโอเมตริก อ้างอิงสำหรับบุคคลแต่ละคน เพื่อลงทะเบียนในฐานข้อมูล โดยบุคคลที่ต้องการลงทะเบียนจะแสดงตนที่ระบบเก็บข้อมูลไบโอเมตริก จากนั้นระบบประมวลผลข้อมูลไบโอเมตริกจะตรวจสอบและประมวลผลข้อมูล เพื่อสร้างเทมเพลตและส่งไปลงทะเบียนในระบบฐานข้อมูลไบโอเมตริก หากตรวจพบการปลอมแปลงหรือข้อมูลมีคุณภาพต่ำ ระบบจะปฏิเสธการลงทะเบียนและให้บุคคลส่งข้อมูลไบโอเมตริกเข้ามาใหม่
2) **การยืนยันตัวบุคคล (Verification)** เป็นการเปรียบเทียบไบโอเมตริกแบบหนึ่งต่อหนึ่ง (1:1) เพื่อพิสูจน์ว่าบุคคลที่แสดงตนที่ระบบเก็บข้อมูลไบโอเมตริก เป็นคนเดียวกันกับบุคคลตามรหัสอ้างอิงตัว บุคคล โดยบุคคลที่ต้องการยืนยันตัวตน จะแสดงตนที่ระบบเก็บข้อมูลไบโอเมตริกพร้อมกับให้รหัสอ้างอิงตัวบุคคล ซึ่งรหัสอ้างอิงนี้อาจมาในรูปแบบ สมาร์ตการ์ด (Smart Card) อาร์เอฟไอดี (RFID) บาร์โค้ด (Barcode) พินโค้ด (Pin code) หรือรหัสผ่าน (Password) โดยระบบจะดึงข้อมูลเทมเพลตไบโอเมตริก อ้างอิงจากระบบฐานข้อมูลไบโอเมตริกตามรหัสอ้างอิง เพื่อใช้เปรียบเทียบกับเทมเพลตไบโอเมตริกทดสอบที่ได้จากการแสดงตน ซึ่งผลลัพธ์การเปรียบเทียบจากระบบเปรียบเทียบข้อมูลไบโอเมตริกจะได้เป็นคะแนนความเหมือน (Similarity Score) จากนั้นระบบตัดสินใจจะให้ผลลัพธ์เป็น “ใช่” (Yes หรือ Match) เมื่อคะแนนความเหมือนมากกว่าหรือเท่ากับค่าเทรชโฮล (Threshold)

(ค่าระดับความปลอดภัยหรือ ค่าขีดเริ่มเปลี่ยน) และให้ผลเป็น “ไม่ใช่” เมื่อคะแนนความเหมือนน้อยกว่าค่าเทรชโฮล การทำงานลักษณะนี้มักใช้ในงานการให้สิทธิ์ในการใช้งานเฉพาะส่วนบุคคลนั้น ๆ เช่น การเข้าใช้พื้นที่ การข้ามแดน การทำธุรกรรมทางการเงิน เป็นต้น

3) **การระบุตัวบุคคล (Identification)** เป็นการเปรียบเทียบไบโอเมตริกแบบหนึ่งต่อหลาย (1:N) เพื่อระบุตัวบุคคลจากข้อมูลไบโอเมตริก โดยระบบจะสร้างเทมเพลตไบโอเมตริกทดสอบ จากข้อมูลไบโอเมตริกที่ได้จากระบบเก็บข้อมูลไบโอเมตริก จากนั้นระบบเปรียบเทียบข้อมูลไบโอเมตริกจะเปรียบเทียบเทมเพลตทดสอบ กับเทมเพลตทั้งหมดในระบบฐานข้อมูลไบโอเมตริกและให้ผลลัพธ์เป็นคะแนนความเหมือนของทุกคู่การเปรียบเทียบ จากนั้นระบบตัดสินใจจะให้ผลลัพธ์เป็น รายการบุคคล (Candidate List) ที่เรียงลำดับรายการจากคะแนนความเหมือนซึ่งเรียงจากมากไปน้อย (อันดับที่ 1 คือ คะแนนสูงที่สุด) โดยคะแนนความเหมือนต้องมีค่ามากกว่าหรือเท่ากับค่าเทรชโฮล และมีจำนวนรายการไม่เกินที่กำหนด การทำงานลักษณะนี้มักใช้ในงานการติดตามคนร้าย หรือใช้ตรวจสอบบุคคลก่อนการลงทะเบียนเพื่อป้องกันการลงทะเบียนซ้ำ เป็นต้น

ระบบไบโอเมตริกเป็นระบบอิเล็กทรอนิกส์ จึงได้รับความคาดหวังจากคนทั่วไปว่าจะมีความถูกต้องสูง คือไม่มีความผิดพลาดหรือมีต่ำมาก แต่ไบโอเมตริก (ใบหน้า ลายนิ้วมือ ลายม่านตา หรือไบโอเมตริกอื่น ๆ) มีความผิดพลาดในทางปฏิบัติด้วยสาเหตุต่าง ๆ มากมาย เช่น ความเปลี่ยนแปลงของแสงในการถ่ายภาพใบหน้า เส้นลายนิ้วมือที่ผิดปกติจากความผิดพลาดของเครื่องสแกน หรือสภาพผิวหนัง เป็นต้น จึงไม่มีทางที่จะมีความถูกต้องถึง 100% ซึ่งเป็นสิ่งแรกที่ผู้ใช้ระบบไบโอเมตริกต้องยอมรับความจริงข้อนี้

5.1 การวัดสมรรถนะของระบบไบโอเมตริก

การวัดสมรรถนะของระบบไบโอเมตริกสามารถวัดแยกตามลักษณะการทำงาน และการนำเข้าข้อมูล โดยลักษณะการทำงานจะเกี่ยวข้องกับระบบตัดสินใจโดยแบ่งเป็น การยืนยันตัวบุคคล และการระบุตัวบุคคล ในขณะที่การนำเข้าข้อมูลจะเกี่ยวข้องกับระบบเก็บข้อมูลไบโอเมตริก และระบบประมวลผลข้อมูลไบโอเมตริก ซึ่งมีรายละเอียดดังนี้

5.1.1 การวัดสมรรถนะของระบบไบโอเมตริกแบบการยืนยันตัวบุคคล

ในการทำงานลักษณะนี้ระบบจะให้ผลลัพธ์การเปรียบเทียบไบโอเมตริกแบบหนึ่งต่อหนึ่ง (1:1) เป็น “ใช่” (ใช่บุคคลเดียวกัน) หรือ “ไม่ใช่” (ไม่ใช่บุคคลเดียวกัน) โดยพิจารณาจากคะแนนความเหมือนระหว่างสองไบโอเมตริก โดยระบบจะให้ผลเป็น “ใช่” เมื่อคะแนนความเหมือนมากกว่าหรือเท่ากับค่าเทรชโฮล และให้ผลเป็น “ไม่ใช่” เมื่อคะแนนความเหมือนน้อยกว่าค่าเทรชโฮล ซึ่งคะแนนความเหมือนของสองไบโอเมตริกที่มาจากบุคคลเดียวกันคือคะแนนแท้ (Genuine Score) และคะแนนความเหมือนของสองไบโอเมตริกที่มาจากคนละบุคคลคือ คะแนนเทียม (Imposter Score) โดยการตัดสินคะแนนแท้เป็น “ไม่ใช่” และคะแนนเทียมเป็น “ใช่” จากค่าเทรชโฮลที่กำหนดถือเป็นความผิดพลาดของระบบ โดยความสัมพันธ์ของคะแนนแท้ คะแนนเทียม ค่าเทรชโฮล และความผิดพลาดของระบบแสดงได้ดังภาพที่ 67 ซึ่งการบ่งชี้สมรรถนะของระบบไบโอเมตริกที่ทำงานลักษณะนี้สามารถพิจารณาจากอัตราความผิดพลาดดังต่อไปนี้

1) **อัตราการจับคู่ผิดพลาด (False Match Rate (FMR))** คือ อัตราที่คะแนนเทียมมีค่ามากกว่าหรือเท่ากับค่าเทรชโฮล (อัตราการยอมรับตัวปลอม) หรืออัตราส่วนของผู้ที่สามารถเข้าระบบได้โดยที่ไม่ใช่เจ้าของไบโอเมตริกนั้นกับผู้ที่เข้าระบบได้ทั้งหมด ซึ่งคำนวณได้จากสมการที่ (2)

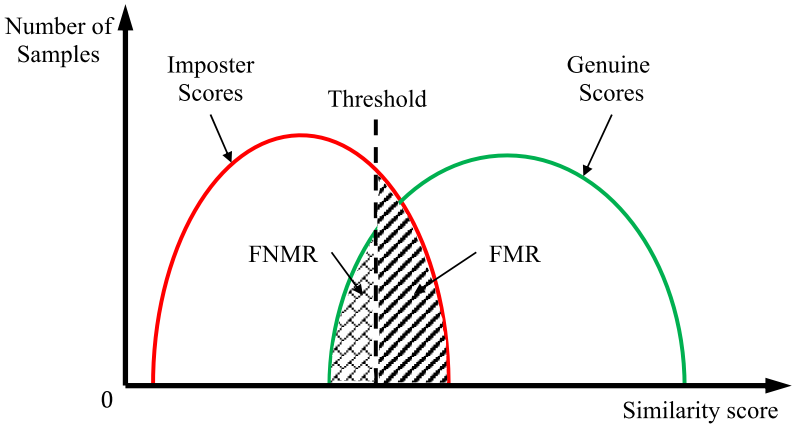
$$FMR(T) = \frac{1}{N}\sum_{i=1}^{N} H(v_i - T) \quad (2)$$

เมื่อ T คือ ค่าเทรชโฮล N คือ จำนวนคะแนนเทียมทั้งหมด $H(x)$ คือ ฟังก์ชันขั้นบันไดหนึ่งหน่วย (Unit step function) โดย $H(0) = 1$ และ v คือ คะแนนเทียม

2) **อัตราการไม่จับคู่ผิดพลาด (False Non-Match Rate (FNMR))** คือ อัตราที่คะแนนแท้มีค่าน้อยกว่าค่าเทรชโฮล (อัตราการปฏิเสธตัวจริง) หรืออัตราส่วนของผู้ที่ไม่สามารถเข้าระบบได้โดยที่เป็นเจ้าของไบโอเมตริกนั้นกับผู้ที่ไม่สามารถเข้าระบบได้ทั้งหมด ซึ่งคำนวณได้จากสมการที่ (3)

$$FNMR(T) = 1 - \frac{1}{N}\sum_{i=1}^{N} H(u_i - T) \quad (3)$$

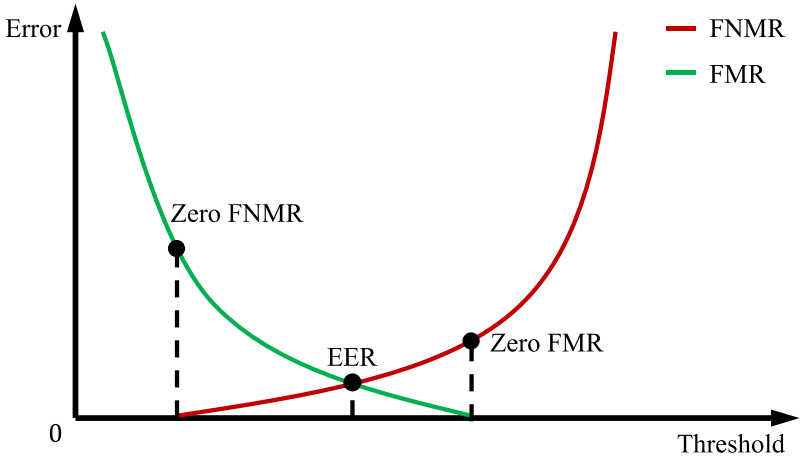
เมื่อ T คือ ค่าเทรชโฮล N คือ จำนวนคะแนนแท้ทั้งหมด $H(x)$ คือ ฟังก์ชันขั้นบันไดหนึ่งหน่วย (Unit step function) โดย $H(0) = 1$ และ u คือ คะแนนแท้



ภาพที่ 67 ความสัมพันธ์ของคะแนนแท้ (Genuine score) คะแนนเทียม (Imposter score) อัตราการไม่จับคู่ผิดพลาด (FNMR) และอัตราการจับคู่ผิดพลาด (FMR) ที่ค่าเทรชโฮลที่กำหนด

สมรรถนะของระบบอาจบ่งชี้โดยสรุปได้จากดัชนีชี้วัด ดังต่อไปนี้

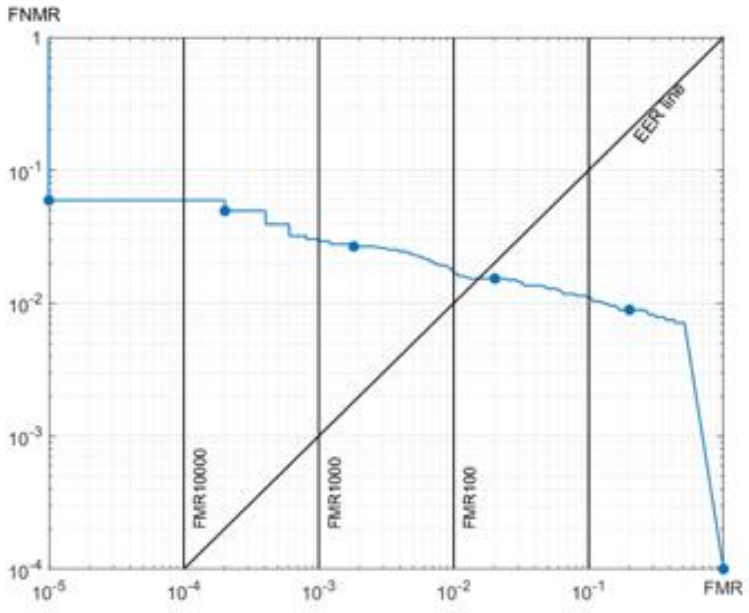
1) **อัตราความผิดพลาดที่เท่ากัน (Equal Error Rate (EER))** คือ ค่าความผิดพลาด ที่ตำแหน่งค่าเทรชโฮลทำให้อัตราการจับคู่ผิดพลาด (FMR) เท่ากับอัตราการไม่จับคู่ผิดพลาด (FNMR) ($FMR(T) = FNMR(T)$) (ภาพที่ 68) โดยถ้าระบบใดมีค่าอัตราความผิดพลาดที่เท่ากันต่ำกว่าอีกระบบ จะสามารถตัดสินได้ว่าระบบนั้นมีความแม่นยำมากกว่า
2) **อัตราการไม่จับคู่ผิดพลาดเป็นศูนย์ (Zero FNMR)** คือ ค่าความผิดพลาด ที่ตำแหน่งค่าเทรชโฮลทำให้อัตราการไม่จับคู่ผิดพลาดเป็นศูนย์ (ภาพที่ 68)
3) **อัตราการจับคู่ผิดพลาดเป็นศูนย์ (Zero FMR)** คือ ค่าความผิดพลาด ที่ตำแหน่งค่าเทรชโฮลทำให้อัตราการจับคู่ผิดพลาดเป็นศูนย์ (ภาพที่ 68)



ภาพที่ 68 ดัชนีชี้วัด อัตราความผิดพลาดที่เท่ากัน (EER) อัตราการไม่จับคู่ผิดพลาดเป็นศูนย์ (Zero FNMR) อัตราการจับคู่ผิดพลาดเป็นศูนย์ (Zero FMR) บนเส้นโค้ง FMR และ FNMR

ในทางปฏิบัติแล้วการพิจารณาสมรรถนะของระบบ เพื่อเปรียบเทียบสมรรถนะของแต่ละระบบ จะพิจารณาจากค่าของอัตรา FMR และอัตรา FNMR ที่ตั้งไว้ตามวัตถุประสงค์การนำระบบไปใช้ ดังนั้น การรายงานสมรรถนะของระบบมักรายงานในรูปแบบของกราฟ เส้นโค้งการแลกเปลี่ยนการตรวจจับที่ผิดพลาด (Detection-Error Tradeoff (DET) curve) โดยจะรายงานสมรรถนะของระบบไบโอเมตริกที่ค่าเทรชโฮลต่าง ๆ ของระบบ ซึ่งสามารถสร้างโดยการลงจุดโดยใช้ค่า $FMR(T)$ กับค่า $FNMR(T)$ เพื่อกำหนดพิกัดสองมิติในกราฟ ซึ่งการเปลี่ยนค่าเทรชโฮล T แต่ละค่า

จะสร้างจุดหนึ่งจุดบนเส้นโค้ง DET โดยที่กำหนดให้ $FNMR(T)$ อยู่ในแนวแกนตั้งและ $FMR(T)$ อยู่ในแนวแกนนอน ดังภาพที่ 69



ภาพที่ 69 ตัวอย่างเส้นโค้งการแลกเปลี่ยนการตรวจจับที่ผิดพลาด (Detection-Error Tradeoff (DET) curve)

5.1.2 การวัดสมรรถนะของระบบไบโอเมตริกแบบการระบุตัวบุคคล

ในการทำงานลักษณะนี้ระบบจะให้ผลลัพธ์การเปรียบเทียบลักษณะเฉพาะไบโอเมตริกแบบหนึ่งต่อหลาย (1:N) เป็นรายการบุคคล ที่เรียงลำดับรายการจากคะแนนความเหมือนซึ่งเรียงจากมากไปน้อย (อันดับที่ 1 คือคะแนนสูงที่สุด) โดยคะแนนความเหมือนต้องมีค่ามากกว่าหรือเท่ากับค่าเทรชโฮล T และมีความยาวรายการไม่เกิน L รายการ ซึ่งผู้เชี่ยวชาญหรือพนักงานอาจตรวจสอบรายการบุคคลทั้งหมด หรืออาจตรวจสอบเพียงรายการคะแนนสูงสุดลำดับ (Rank) R แรก ($R \leq L$) โดยจะขึ้นกับนโยบาย หรือข้อกำหนดของการประยุกต์ใช้ระบบ การวัดสมรรถนะสามารถแบ่งตามลักษณะการใช้งานได้เป็น 2 ชนิด คือ

1) **ฐานข้อมูลเปิด (Open-set)** คือ ระบบที่มีการค้นหาเพื่อระบุตัวบุคคลที่ไม่ได้ลงทะเบียนในฐานข้อมูล (Nonmated Search) เช่น การป้อนข้อมูลไบโอเมตริกของบุคคลทั่วไปที่ไม่ได้ลงทะเบียนในฐานข้อมูลรายชื่อบุคคลเฝ้าระวัง (Watch-list) แล้วระบบอาจตอบผลลัพธ์กลับมาเป็นรายการบุคคลจากฐานข้อมูลรายชื่อบุคคลเฝ้าระวัง หรืออาจตอบผลลัพธ์กลับมาเป็นไม่พบรายการ เป็นต้น การบ่งชี้สมรรถนะของระบบไบโอเมตริกที่ทำงานในลักษณะนี้สามารถพิจารณาจากอัตราความผิดพลาดดังต่อไปนี้

   (1) อัตราความผิดพลาดบวกจากการระบุตัวบุคคลผิด (False Positive Identification Rate (FPIR)) คือ อัตราความผิดพลาดจากการค้นหาด้วยไบโอเมตริกของบุคคลที่ไม่ได้ลงทะเบียนในระบบ (Nonmated Search) ที่ผลลัพธ์รายการบุคคลมีหนึ่งรายการหรือมากกว่า ซึ่งคำนวณได้จากสมการที่ (4)

$$FPIR(N,T) = \frac{\#\mathrm{NM}_{C\geq 1}}{\#\mathrm{NM}} \tag{4}$$

   เมื่อ N คือ จำนวนบุคคลทั้งหมดในฐานข้อมูล T คือ ค่าเทรชโฮล $\#\mathrm{NM}_{C\geq 1}$ คือ จำนวนครั้งการค้นหาแบบ Nonmated Search ที่ผลลัพธ์รายการบุคคลมีหนึ่งรายการหรือมากกว่า โดยแต่ละรายการมีคะแนนมากกว่าหรือเท่ากับค่าเทรชโฮล และ $\#\mathrm{NM}$ คือ จำนวนครั้งการค้นหาแบบ Nonmated Search ทั้งหมด

   (2) อัตราความผิดพลาดลบจากการระบุตัวบุคคลผิด (False Negative Identification Rate (FNIR) หรือ Miss Rate) คือ อัตราความผิดพลาดจากการค้นหาด้วยไบโอเมตริกของบุคคลที่ลงทะเบียนในระบบ (Mated Search) ที่ผลลัพธ์รายการบุคคลที่ใช้ค้นหาอยู่นอกลำดับ R หรือมีคะแนนน้อยกว่าค่าเทรชโฮล นอกจากนั้น

ยังรวมถึงกรณีที่ระบบล้มเหลว เช่น ไม่สามารถสร้างเทมเพลต (Template) จากข้อมูลไบโอเมตริกคุณภาพต่ำได้ และอัลกอริทึมหรือซอฟต์แวร์ล้มเหลว (Crash) เป็นต้น ซึ่งอัตรา FNIR คำนวณได้จากสมการที่ (5)

$$FNIR(N,R,T) = \frac{\#\mathrm{M}_{r>R}}{\#\mathrm{M}} \tag{5}$$

เมื่อ N คือ จำนวนบุคคลทั้งหมดในฐานข้อมูล R คือ จำนวนลำดับรายการบุคคลที่พิจารณา T คือ ค่าเทรชโฮล $\#\mathrm{M}_{r>R}$ คือ จำนวนครั้งการค้นหาแบบ Mated Search ที่ผลลัพธ์รายการบุคคลที่ใช้ค้นหาอยู่นอกลำดับ R หรือมีคะแนนน้อยกว่าค่าเทรชโฮล และ $\#\mathrm{M}$ คือ จำนวนครั้งการค้นหาแบบ Mated Search ทั้งหมด

สำหรับการใช้งานจริงของระบบอาจมีข้อมูลไบโอเมตริกของหนึ่งบุคคลมากกว่าหนึ่งไบโอเมตริก แต่ระบบเก็บข้อมูลแยกเป็นคนละบุคคล ซึ่งอาจเกิดจากการลงทะเบียนผิดพลาด ซ้ำซ้อน หรือการสวมสิทธิ์ เพื่อวัดสมรรถนะของระบบในการระบุตัวบุคคลในกรณีนี้ ข้อมูลไบโอเมตริกแต่ละรายการ (K_i) ของบุคคลเดียวกันจะถูกเก็บแยกเสมือนเป็นคนละบุคคลในฐานข้อมูลทดสอบ และวัดอัตรา $FNIR$ สองกรณี คือ อัตราความผิดพลาดที่ผลลัพธ์รายการบุคคลที่ใช้ค้นหารายการใดรายการหนึ่งอยู่นอกลำดับ R ($FNIR_{any}$) และอัตราความผิดพลาดที่ผลลัพธ์รายการบุคคลที่ใช้ค้นหาทุกรายการอยู่นอกลำดับ R ($FNIR_{all}$) โดยสามารถคำนวณได้จากสมการที่ (6) และ (7) ตามลำดับ

$$FNIR_{any}(N,R,T) = 1 - \frac{\#\mathrm{M}_{any\ of\ K_i \le R}}{\#\mathrm{M}} \tag{6}$$

$$FNIR_{all}(N,R,T) = 1 - \frac{\#\mathrm{M}_{all\ of\ K_i \le R}}{\#\mathrm{M}} \tag{7}$$

เมื่อ N คือ จำนวนบุคคลทั้งหมดในฐานข้อมูล R คือ จำนวนลำดับรายการบุคคลที่พิจารณา T คือ ค่าเทรชโฮล $\#\mathrm{M}_{any\ of\ K_i \le R}$ คือ จำนวนครั้งการค้นหาแบบ Mated Search ที่ผลลัพธ์รายการบุคคลที่ใช้ค้นหารายการใดรายการหนึ่งในฐานข้อมูลอยู่ในลำดับ R หรือสูงกว่า และมีคะแนนมากกว่าหรือเท่ากับค่าเทรชโฮล $\#\mathrm{M}_{all\ of\ K_i \le R}$ คือ จำนวนครั้งการค้นหาแบบ Mated Search ที่ผลลัพธ์รายการบุคคลที่ใช้ค้นหาทุกรายการในฐานข้อมูลอยู่ในลำดับ R หรือสูงกว่า และมีคะแนนมากกว่าหรือเท่ากับค่าเทรชโฮล และ $\#\mathrm{M}$ คือจำนวนครั้งการค้นหาแบบ Mated Search ทั้งหมด

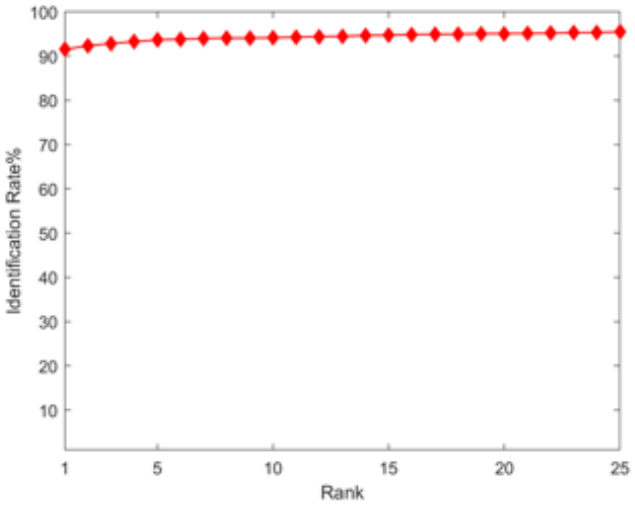
การรายงานสมรรถนะของระบบแบบฐานข้อมูลเปิดสามารถรายงานในรูปแบบของกราฟ DET ได้ โดยที่กำหนดให้ $FNIR$ อยู่ในแนวแกนตั้งและ $FPIR$ อยู่ในแนวแกนนอน

2) **ฐานข้อมูลปิด (Closed-set)** คือ ระบบที่มีการค้นหาเพื่อระบุตัวตนของบุคคลเฉพาะบุคคลที่ลงทะเบียนในฐานข้อมูล (Mated search) การใช้งานในกรณีนี้ระบบจะตอบผลลัพธ์เป็นรายการบุคคลที่เรียงลำดับรายการจากคะแนนความเหมือนจากมากไปน้อย โดยตั้งค่าเทรชโฮลเป็นศูนย์ $T = 0$ การบ่งชี้สมรรถนะของระบบไบโอเมตริกที่ทำงานในลักษณะนี้สามารถพิจารณาจากอัตราความถูกต้อง ดังต่อไปนี้

(1) อัตราการระบุตัวบุคคล (Identification Rate) คือ อัตราความถูกต้องจากการค้นหาด้วยไบโอเมตริกของบุคคลที่ลงทะเบียนในระบบ (Mated Search) ที่ผลลัพธ์รายการบุคคลที่ใช้ค้นหาอยู่ในลำดับ R หรือสูงกว่าโดยจะรายงานในรูปแบบของกราฟ เส้นโค้งการจับคู่ลักษณะเฉพาะสะสม (Cumulative Match Characteristic (CMC) curve) ซึ่งสามารถคำนวณได้จากสมการที่ (8)

$$CMC(N,R) = 1 - FNIR(N,R,0) \tag{8}$$

เมื่อ N คือ จำนวนบุคคลทั้งหมดในฐานข้อมูล R คือ จำนวนลำดับรายการบุคคลที่พิจารณา และ $FNIR(N,R,0)$ คือ อัตราที่ผลลัพธ์รายการบุคคลที่ใช้ค้นหาอยู่นอกลำดับ R ตัวอย่างกราฟ CMC แสดงได้ดังภาพที่ 70



ภาพที่ 70 ตัวอย่างเส้นโค้งการจับคู่ลักษณะเฉพาะสะสม (Cumulative Match Characteristic (CMC) curve)

5.1.3 การวัดสมรรถนะของระบบไบโอเมตริกในการนำเข้าข้อมูล

นอกจากสมรรถนะด้านความแม่นยำในการรู้จำตัวบุคคลแล้ว ระบบไบโอเมตริกยังเผชิญกับความผิดพลาดจากการนำเข้าข้อมูล ซึ่งสามารถบ่งชี้ได้จากอัตราความผิดพลาด ดังต่อไปนี้

1) **อัตราความผิดพลาดจากการเก็บข้อมูลไบโอเมตริก (Failure to Acquire Rate (FTA))** คือ อัตราความผิดพลาดที่ระบบไม่สามารถสร้างลักษณะเฉพาะชีวมิติที่ใช้ในการเปรียบเทียบได้ ซึ่งอาจเกิดจากความผิดพลาดของการทำงานของซอฟต์แวร์หรือฮาร์ดแวร์ หรือบุคคลไม่สามารถแสดงไบโอเมตริกได้ เนื่องจากข้อจำกัดทางการแพทย์ เช่น มีผ้าพันแผลที่นิ้ว มีผ้าปิดตาจากการผ่าตัดดวงตา รวมถึงระบบประมวลผลข้อมูลไบโอเมตริกไม่สามารถระบุตำแหน่งไบโอเมตริก (segmentation fail) หรือไม่สามารถสกัดลักษณะเฉพาะไบโอเมตริก (feature extraction fail) ได้ หรือลักษณะเฉพาะไบโอเมตริกที่สกัดได้มีคุณภาพต่ำกว่าความต้องการของระบบ
2) **อัตราความผิดพลาดจากการลงทะเบียนไบโอเมตริก (Failure to Enroll Rate (FTE))** คือ อัตราความผิดพลาดที่ระบบไม่สามารถสร้างและเก็บข้อมูลไบโอเมตริกอ้างอิงลงในฐานข้อมูลได้ ซึ่งอาจเกิดจากบุคคลไม่สามารถแสดงไบโอเมตริกได้ เนื่องจากข้อจำกัดทางการแพทย์หรือข้อมูลไบโอเมตริกคุณภาพต่ำ

5.1.4 แนวทางการประเมินสมรรถนะของระบบไบโอเมตริก

แนวทางการประเมินสมรรถนะของระบบไบโอเมตริกที่ดี คือ การอาศัยหน่วยงานอิสระ (Independent Third Party) ในการออกแบบ บริหารจัดการ และวิเคราะห์การทดสอบ [Jain2011] โดยสามารถแบ่งการประเมินออกเป็น 3 ระดับ [ISO/IEC_19795-1] โดยมีรายละเอียดดังต่อไปนี้

1) **การประเมินระดับเทคโนโลยี (Technology Evaluation)** คือ การทดสอบเพื่อเปรียบเทียบสมรรถนะของอัลกอริทึมที่ทำงานในระบบย่อยต่าง ๆ โดยใช้เทคโนโลยี (ฮาร์ดแวร์ และซอฟต์แวร์) และชุดข้อมูลทดสอบเดียวกัน ซึ่งชุดข้อมูลทดสอบอาจเป็นข้อมูลที่เก็บระหว่างการทดสอบ หรืออาจเป็นชุดข้อมูลที่จัดเตรียมไว้ก่อนหน้า (Offline Data) ก็ได้ ในบางการทดสอบอาจมีการให้ตัวอย่างข้อมูลทดสอบ แก่ผู้พัฒนาเพื่อใช้ในการพัฒนาหรือปรับแต่งอัลกอริทึมก่อนดำเนินการทดสอบ แต่ในการทดสอบจริงจะใช้ชุดข้อมูลทดสอบที่ไม่ได้เปิดเผยแก่ผู้พัฒนา โดยการทดสอบจะดำเนินการแบบปิด (Offline Test) คือ การทดสอบที่มีการเก็บข้อมูลไบโอเมตริกล่วงหน้าโดยจะทำการลงทะเบียนและหรือเปรียบเทียบไบโอเมตริกในภายหลัง ซึ่งการทดสอบระดับเทคโนโลยีนี้สามารถทดสอบซ้ำได้ เนื่องจากชุดข้อมูลทดสอบไม่เปลี่ยนแปลง
2) **การประเมินระดับการจำลองประยุกต์ใช้งาน (Scenario Evaluation)** คือ การทดสอบเพื่อเปรียบเทียบสมรรถนะของระบบไบโอเมตริกต่าง ๆ โดยจำลองสภาพแวดล้อมการประยุกต์ใช้งานจริงเพื่อประเมินสมรรถนะของระบบแบบครบวงจร (End-To-End) ในแต่ละระบบทดสอบ จะมีอุปกรณ์สำหรับเก็บข้อมูลไบโอเมตริกของตัวเอง ซึ่งจะทำให้แต่ละระบบได้ชุดข้อมูลที่แตกต่างกันเล็กน้อย ดังนั้น ในการเปรียบเทียบระบบหลายระบบจึงต้องมีการควบคุมกระบวนการเก็บข้อมูลให้ระบบทดสอบทุกระบบอยู่ในสภาพแวดล้อมเหมือนกัน

และใช้ผู้ทดสอบชุดเดียวกัน โดยการทดสอบสามารถดำเนินการแบบเปิด (Online Test) หรือแบบปิด (Offline Test) ก็ได้ ขึ้นกับความต้องการของการทดสอบ โดยการทดสอบแบบเปิด คือ การทดสอบที่เก็บข้อมูลไบโอเมตริกและทำการลงทะเบียนและหรือเปรียบเทียบไบโอเมตริกทันที ซึ่งการทดสอบระดับการจำลองประยุกต์ใช้งานนี้สามารถทดสอบซ้ำได้ หากสามารถควบคุมสภาพแวดล้อมและผู้ทดสอบให้เหมือนกัน

3) **การประเมินระดับปฏิบัติการ (Operational Evaluation)** คือ การทดสอบเพื่อวัดสมรรถนะของระบบไบโอเมตริกในการประยุกต์ใช้งานจริง ซึ่งมักจะเป็นการทดสอบแบบเปิด (Online Test) เพื่อให้สอดคล้องกับสภาพแวดล้อมและกลุ่มเป้าหมายที่ใช้งานจริงของระบบ ซึ่งการทดสอบลักษณะนี้ไม่สามารถทดสอบซ้ำได้ เนื่องจากไม่สามารถรู้หรือระบุความแตกต่างของสภาพแวดล้อม ในการปฏิบัติการของระบบได้ นอกจากนั้นการระบุตัวตนและพฤติกรรมของผู้ทดสอบทำได้ยาก โดยเฉพาะในกรณีที่ไม่มีผู้ดูแลการทดสอบ (Test Administrator) ผู้สังเกตการณ์การทดสอบ (Test Observer) หรือเจ้าหน้าที่ในการปฏิบัติการ (Operational Personnel) มาควบคุม

ตารางที่ 16 แสดงความแตกต่างของการประเมินสมรรถนะของระบบไบโอเมตริกในแต่ละระดับ ตามหัวข้อต่าง ๆ ของการประเมิน ดังต่อไปนี้

ตารางที่ 16 ความแตกต่างของการประเมินสมรรถนะของระบบไบโอเมตริกแต่ละระดับ

หัวข้อ	การประเมินระดับเทคโนโลยี	การประเมินระดับการจำลองประยุกต์ใช้งาน	การประเมินระดับปฏิบัติการ
สิ่งที่ทำการทดสอบ	อัลกอริทึมที่ทำงานในระบบย่อยต่าง ๆ	ระบบไบโอเมตริก	ระบบไบโอเมตริก
อัตลักษณ์ของชุดข้อมูลทดสอบ (Ground Truth)	รู้ แต่อาจมีความผิดพลาด ซึ่งเกิดจากการเก็บและการรวมข้อมูล	รู้ แต่อาจมีความผิดพลาด ซึ่งเกิดจากการเก็บและความผิดพลาดจากพฤติกรรมของผู้ทดสอบ	ขึ้นอยู่กับการควบคุมและอุปกรณ์ที่ใช้ในการสร้างชุดข้อมูลทดสอบ
การควบคุมพฤติกรรมของผู้ทดสอบ โดยผู้ดูแลการทดสอบ	ควบคุมได้ในกระบวนการเก็บข้อมูลไบโอเมตริก	ควบคุมได้ ยกเว้นไม่ได้มีการระบุให้ควบคุม	ควบคุมไม่ได้
การตอบสนองกลับทันที (Real-Time Feedback) ของผู้ทดสอบในการใช้ระบบ	ไม่มี	มี	มี
การทำการทดสอบซ้ำ	ได้ เนื่องจากชุดข้อมูลทดสอบเหมือนเดิม	ได้ หากมีการควบคุมสถานการณ์การทดสอบและกลุ่มผู้ทดสอบให้เหมือนเดิม	ไม่ได้
การควบคุมสภาพแวดล้อมในการทดสอบ	ควบคุมได้ในกระบวนการเก็บข้อมูลไบโอเมตริก	ควบคุมได้	ควบคุมไม่ได้
การบันทึกปฏิสัมพันธ์ของผู้ทดสอบ	บันทึกได้ในกระบวนการเก็บข้อมูลไบโอเมตริก	บันทึกได้	บันทึกได้ระหว่างการลงทะเบียนหรือระหว่างการยืนยันหรือการระบุตัวบุคคล
การรายงานผลการทดสอบ	เปรียบเทียบประสิทธิภาพของอัลกอริทึมที่ทำงานในระบบย่อยต่าง ๆ โดยใช้ตัวบ่งชี้ประสิทธิภาพต่าง ๆ	เปรียบเทียบระบบไบโอเมตริกโดยใช้ตัวบ่งชี้ประสิทธิภาพต่างๆ และประสิทธิภาพในการจำลองการประยุกต์ใช้งาน	วัดประสิทธิภาพในสภาพแวดล้อมระดับปฏิบัติการ
ตัวบ่งชี้ประสิทธิภาพ	อัตราความผิดพลาดของกระบวนการต่างๆ ในระบบ ซึ่งวัดสำหรับแต่ละกระบวนการ	อัตรา FMR, FNMR, FTA, FTE และอัตราการรองรับภาระงาน (End-To-End Throughput Rate)	อัตราการรองรับภาระงาน ความน่าเชื่อถือของอัตรา FMR และ FNMR ของการทดสอบระดับปฏิบัติการ
ข้อจำกัด	ต้องเก็บชุดข้อมูลทดสอบให้สอดคล้องกับการนำไปประยุกต์ใช้	การปฏิบัติงานและอุปกรณ์ของระบบต้องสอดคล้องกับการนำไปประยุกต์ใช้	การปฏิบัติงานและอุปกรณ์ของระบบต้องสอดคล้องกับการนำไปประยุกต์ใช้
ผู้ทดสอบ	เก็บข้อมูลไว้ล่วงหน้า	ทดสอบสด	ทดสอบสด

5.1.5 การกำหนดจำนวนข้อมูลทดสอบ

ตามมาตรฐาน ISO/IEC 19795-1:2021 [ISO/IEC_19795-1] นิยามไว้ว่า จำนวนชุดข้อมูลทดสอบมีผลกับความแม่นยำของประสิทธิภาพที่วัดได้ หากใช้ข้อมูลทดสอบมากความแม่นยำในการวัดประสิทธิภาพก็จะมากตาม แต่หากต้องการกำหนดจำนวนอย่างน้อยในการทดสอบสามารถกำหนดได้จาก กฎของ 3 (Rule of 3) และกฎของ 30 (Rule of 30) โดยรายละเอียดแต่ละกฎมี ดังนี้

1) **กฎของ 3 (Rule of 3)** คือ กฎที่กำหนดค่าความผิดพลาดที่ต่ำที่สุดจากข้อมูลทดสอบ ที่มีการกระจายตัวเหมือนกันอิสระ (Independent Identical Distributed (i.i.d.)) n จำนวน ซึ่งกำหนดให้ค่าความผิดพลาดน้อยกว่าหรือเท่ากับ p ที่ความเชื่อมั่น 95% และให้ค่าความผิดพลาดเท่ากับ 0 ที่ความเชื่อมั่น 5% โดย

$$p \approx \frac{3}{n} \tag{9}$$

เมื่อ n จำนวนข้อมูลทดสอบ

ตัวอย่างเช่น มีชุดข้อมูลทดสอบจำนวน 300 ($n = 300$) ซึ่งจากการทดสอบมีค่าความผิดพลาดเท่ากับ 0 จากกฎของ 3 ทำให้บอกได้ว่าความผิดพลาดที่ต่ำที่สุดที่เป็นไปได้ของระบบนี้มีค่าน้อยกว่าหรือเท่ากับ $p = \frac{3}{300} = 1\%$ ที่ความเชื่อมั่น 95% เป็นต้น

จากกฎดังกล่าว สามารถหาจำนวนข้อมูลทดสอบได้โดยการกำหนดค่าความผิดพลาดเป้าหมายของระบบ เช่น กำหนดอัตรา FMR = 0.1% จะต้องใช้จำนวนข้อมูลคะแนนเทียมเท่ากับ $n = \frac{3}{p} = \frac{3}{0.1\%} = 3{,}000$

และกำหนดอัตรา FNMR = 3% จะต้องใช้จำนวนข้อมูลคะแนนแท้เท่ากับ $n = \frac{3}{p} = \frac{3}{3\%} = 100$

2) **กฎของ 30 (Rule of 30)** คือ กฎที่กำหนดจากการแจกแจงแบบทวินาม (Binomial Distribution) โดยกำหนดให้ค่าความผิดพลาดที่แท้จริงเท่ากับ $\pm 30\%$ ของค่าความผิดพลาดที่วัดได้ (ต้องมีความผิดพลาดอย่างน้อยจำนวน 30 จากจำนวนข้อมูลทดสอบทั้งหมด) ที่ความเชื่อมั่น 90% เช่น

จากข้อมูลคะแนนแท้จำนวน	$3{,}000$
มีการตัดสินผิดพลาดว่าไม่ใช่คนเดียวกันจำนวน	30
ค่าความผิดพลาดที่วัดได้คือ	$\frac{30}{3000} = 1\%$

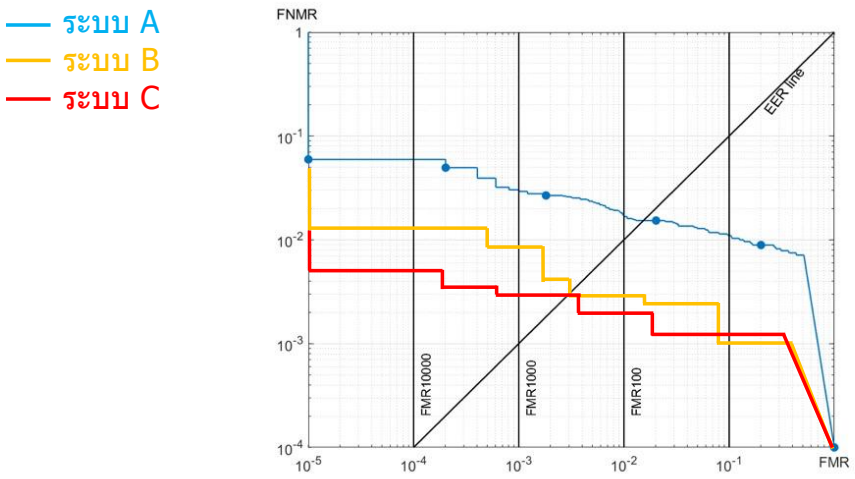
ดังนั้นจากกฎของ 30 ทำให้บอกได้ว่าค่าความผิดพลาดที่แท้จริง จะอยู่ในช่วง 0.7% ถึง 1.3% ที่ความเชื่อมั่น 90%

จากกฎดังกล่าว สามารถหาจำนวนข้อมูลทดสอบได้โดยการกำหนดค่าความผิดพลาดเป้าหมายของระบบ เช่น กำหนดอัตรา FMR = 0.1% จะต้องใช้จำนวนข้อมูลคะแนนเทียมเท่ากับ $n = \frac{30}{p} = \frac{30}{0.1\%} = 30{,}000$

และกำหนดอัตรา FNMR = 3% จะต้องใช้จำนวนข้อมูลคะแนนแท้เท่ากับ $n = \frac{30}{p} = \frac{30}{3\%} = 1{,}000$

5.2 การเปรียบเทียบระบบไบโอเมตริก

ในทางการค้าของระบบรู้จำตัวบุคคลอัตโนมัติด้วยไบโอเมตริก บริษัทส่วนใหญ่จะใช้อัตรา FMR (FAR) และ FNMR (FRR) เป็นตัวโฆษณาประสิทธิภาพของระบบ และค่าที่อ้างอิงมักจะเป็น FMR อยู่ที่ 0.001% หรือ 1/100,000 และจะมี FNMR อยู่ที่น้อยกว่า 1% ทั้งนี้ สังเกตว่าที่บริษัทอ้าง จะไม่พูดถึงว่าใช้ฐานข้อมูลกลางหรือมาตรฐานใด ๆ แต่จะใช้ฐานข้อมูลของตนเอง ซึ่งสามารถปรับค่าอัตราความผิดพลาดได้ต่ำมาก และอาจไม่พูดถึงอัตรา FTA หรือ FTE เลย ดังนั้น การเปรียบเทียบประสิทธิภาพของระบบต้องอ้างอิงกับผลการทดสอบที่มีการกำหนดปัจจัยต่าง ๆ ในการทดสอบที่ทำให้ระบบที่ถูกทดสอบมีความเท่าเทียมกัน ซึ่งการเปรียบเทียบประสิทธิภาพของระบบการยืนยันตัวตนจะพิจารณาจากอัตรา FMR และ FNMR ที่ทดสอบด้วยชุดข้อมูลที่ใกล้เคียงกับการประยุกต์ใช้งานจริง เช่น ระบบยืนยันตัวตนด้วยใบหน้าจากหนังสือเดินทาง เปรียบเทียบกับใบหน้าของผู้ถือหนังสือเดินทาง ชุดข้อมูลทดสอบก็ต้องใช้ภาพใบหน้าที่มีลักษณะเฉพาะเหมือนกับที่ได้จากหนังสือเดินทาง และภาพใบหน้าที่ถ่ายได้จากผู้ถือหนังสือเดินทางที่จุดแสดงตน เป็นต้น ตัวอย่างการเปรียบเทียบประสิทธิภาพแสดงได้ดังภาพที่ 71



ภาพที่ 71 กราฟ DET แสดงประสิทธิภาพของระบบไบโอเมตริกสำหรับการยืนยันตัวบุคคล A B และ C

จากกราฟหากพิจารณาในภาพรวมจะเห็นว่าระบบ C มีประสิทธิภาพโดยรวมสูงกว่าระบบ A และ B ซึ่งหากกำหนดประสิทธิภาพขั้นต่ำของระบบที่ต้องการใช้ที่ FMR น้อยกว่าหรือเท่ากับ 1% (น้อยกว่า 10^{-2}) ระบบที่ควรเลือกใช้ คือ ระบบ C แต่หากกำหนดที่ FMR เท่ากับ 10% ระบบที่ควรเลือกใช้คือระบบ B เป็นต้น อย่างไรก็ตามในการเปรียบเทียบเพื่อเลือกซื้อระบบไบโอเมตริก นอกจากประสิทธิภาพแล้วยังต้องคำนึงถึงปัจจัยอื่น ๆ ที่เกี่ยวข้องด้วย [อารีกุล2557] ซึ่งอาจรวมถึงปัจจัย ดังต่อไปนี้

1) **ภาวการณ์ปฏิบัติการ (Modes of Operation)** ลักษณะการทำงานของระบบที่ต้องการ เช่น การยืนยันตัวบุคคล การระบุตัวบุคคล หรือทั้งสองลักษณะ
2) **เวลาการตอบสนอง (Response Time)** ในการประยุกต์ใช้งานที่เวลาเป็นตัวแปรที่สำคัญ เช่น มีผู้ใช้งานจำนวนมาก มีคิวยาว ระบบเหล่านี้ต้องตอบสนองอย่างรวดเร็ว และมีวิธีการรองรับปัญหาในกรณีที่เกิดเหตุขัดข้องทางเทคนิค เช่น บุคคลไม่สามารถยืนยันตัวตนด้วยไบโอเมตริกที่กำหนดได้ แต่เป็นเจ้าของไบโอเมตริกจริง ระบบอาจต้องมีทางเลือกอื่นในการยืนยันตัวบุคคล เช่น เปิดช่องให้เจ้าหน้าที่เข้าตรวจสอบและยืนยันด้วยไบโอเมตริกชนิดอื่น หรืออาจใช้ร่วมกับเอกสารที่น่าเชื่อถืออื่น ๆ เป็นต้น เพื่อให้ภาระงานของระบบยังคงอยู่ในระดับที่ยอมรับได้
3) **ขนาดของฐานข้อมูล (Size of Database)** การประยุกต์ใช้งานระบบแต่ละประเภทอาจมีความต้องการการใช้งานขนาดฐานข้อมูลไม่เท่ากัน ซึ่งขนาดฐานข้อมูลจะมีผลกระทบทั้งประสิทธิภาพ และค่าใช้จ่ายในการดูแลรักษา เช่น ประสิทธิภาพของระบบการระบุตัวบุคคลจากการทดสอบด้วยชุดข้อมูลทดสอบอาจลดลงตามขนาดฐานข้อมูลที่ใหญ่ขึ้นทั้งในแง่เวลาในการค้นหา และอัตราความผิดพลาดต่าง ๆ ดังนั้น การเลือกระบบต้องคำนึงถึงประสิทธิภาพที่ระบบรับประกันตามขนาดฐานข้อมูลด้วย
4) **เงื่อนไขในการดำเนินการ (Conditions of Operation)** ในการเลือกใช้ระบบจำเป็นต้องคำนึงถึงสภาพแวดล้อมในการใช้งาน เช่น ระบบทำงานอยู่ภายในอาคารหรือภายนอกอาคาร ในบริเวณนั้นมีฝุ่น อุณหภูมิ ความชื้น หรืออยู่ใกล้ทะเลหรือไม่ ซึ่งปัจจัยเหล่านี้ส่งผลต่อการทำงานของอุปกรณ์อิเล็กทรอนิกส์ หากได้รับผลกระทบจากสภาพแวดล้อมอาจต้องใช้อุปกรณ์ที่สามารถทนต่อสภาพแวดล้อมดังกล่าวได้
5) **ผู้ใช้งาน (Anticipated Users)** การกำหนดกลุ่มเป้าหมายผู้ใช้งานเป็นสิ่งจำเป็นสำหรับการเลือกใช้ระบบไบโอเมตริกที่เหมาะสมซึ่ง เพศ อายุ อาชีพ โรค ฯลฯ มีความเกี่ยวข้องกับการเปลี่ยนแปลงข้อมูลไบโอเมตริกของแต่ละบุคคล เช่น เพศชายวัยรุ่นอาจใช้แรงกระทำกับเซนเซอร์มากกว่าเพศหญิงหรือบุคคลสูงอายุ ทำให้การเลือกเซนเซอร์แต่ละกลุ่มเป้าหมายอาจต่างกัน เป็นต้น ในขณะที่อาชีพที่ทำอาจทำให้ข้อมูลไบโอเมตริกเปลี่ยนแปลงได้ เช่น การทำงานแรงงานโดยไม่ใส่ถุงมือในการคัดแยกผลผลิตทางการเกษตร หรืออุตสาหกรรมประมงที่ทำให้มือแช่น้ำหรือมีความชื้นตลอดวัน ส่งผลให้ลายนิ้วมือถูกทำลาย หรือโรคบางอย่าง เช่น โรคเรื้อนก็สามารถทำลายลายนิ้วมือได้เช่นกัน ดังนั้น ในกรณีนี้จึงไม่ควรเลือกใช้ลายนิ้วมือเป็นไบโอเมตริก
6) **สถานที่ติดตั้ง (Installation Location)** การเลือกระบบไบโอเมตริกอาจต้องคำนึงถึงสถานที่ติดตั้งทั้งในแง่ข้อจำกัดของสถานที่และความขัดแย้งของบุคคลในสถานที่ เช่น ระบบไบโอเมตริกสำหรับกล้องวงจรปิด

ต้องติดตั้งในสถานที่ปิด เนื่องจากผู้ใช้งานอาจรู้สึกเสียผลประโยชน์จากการมีระบบ และหากรู้มุมกล้องอาจเปลี่ยนพฤติกรรมเพื่อหลบเลี่ยงระบบ เป็นต้น

7) **พฤติกรรมของผู้ใช้งาน (User's Behaviors)** ผู้ใช้งานอาจให้ความร่วมมือ หรือไม่ให้ อาจขึ้นกับการยอมรับการใช้งานของไบโอเมตริกที่กำหนด หรือการได้ประโยชน์หรือเสียประโยชน์จากการใช้งานระบบ เช่น ยอมรับการใช้ลายนิ้วมือ กับใบหน้า แต่ไม่ยอมรับการใช้ลายม่านตา เนื่องจากความกังวลเรื่องอันตรายจากการสแกนลายม่านตา การใช้ลายนิ้วมือในการบันทึกเวลาเข้าออกงานแทนการใช้บัตรบันทึกเวลา ทำให้ผู้ใช้งานบางคนเสียประโยชน์จากการบันทึกเวลาแทนกันด้วยบัตรบันทึกเวลา ซึ่งอาจทำให้ผู้ใช้งานพยายามทำลายความน่าเชื่อถือของระบบ เช่น การวางนิ้วไม่เหมาะสม หรือทำลายเซนเซอร์เพื่อหลบเลี่ยงการใช้ระบบ เป็นต้น

8) **ความเสถียรของเทคโนโลยี (Technology Stability)** การเลือกใช้งานระบบไบโอเมตริกควรคำนึงถึงความเสถียรของเทคโนโลยี เนื่องจากสามารถใช้เป็นตัวบ่งชี้ความน่าเชื่อถือของระบบได้ หากเป็นเทคโนโลยีใหม่ที่พึ่งเริ่มต้น เช่น การรู้จำตัวบุคคลจากลายเส้นเลือด เป็นเทคโนโลยีที่ยังมีการทดสอบและใช้งานน้อยจึงยังไม่น่าเชื่อถือ ในขณะที่การรู้จำตัวบุคคลจากภาพใบหน้า หรือลายนิ้วมือ หรือลายม่านตา มีการใช้งานมานานและมีการทดสอบกับฐานข้อมูลขนาดใหญ่ จึงมีความน่าเชื่อถือมากและถือได้ว่าเป็นเทคโนโลยีที่มีการพัฒนาจนถึงขั้นที่เสถียรแล้ว

5.3 การใช้ผลการประเมินสมรรถนะสากลโดยหน่วยงานที่มีความน่าเชื่อถือ

ในปัจจุบันมีหน่วยงานที่ทำหน้าที่ประเมินสมรรถนะของระบบไบโอเมตริกในระดับเทคโนโลยีอยู่หลายหน่วยงาน โดยมีผู้พัฒนา (Developer) และผู้ขาย (Vendor) หลายรายเข้าร่วมประเมิน และเปิดเผยผลการประเมิน ซึ่งผู้ซื้อ (Buyer) หรือผู้ที่ต้องการใช้งานสามารถใช้ผลการประเมินเหล่านี้ อ้างอิงในการเลือกใช้ระบบไบโอเมตริกได้ โดยหน่วยงานที่ทำหน้าที่ประเมินสมรรถนะ ได้แก่

1) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology (NIST)) เป็นหน่วยงานของกระทรวงพาณิชย์ ประเทศสหรัฐอเมริกา
2) การแข่งขันการยืนยันตัวบุคคลด้วยลายนิ้วมือ (Fingerprint Verification Competition (FVC)) จัดโดยห้องปฏิบัติการระบบไบโอเมตริก (Biometric system laboratory) ของมหาวิทยาลัยโบโลญญา (University of Bologna) ประเทศอิตาลี
3) การแข่งขันการตรวจจับการปลอมแปลงไบโอเมตริก (Liveness Detection Competition Series (LivDet)) จัดโดยมหาวิทยาลัยคลาร์กสัน (Clarkson University) ประเทศสหรัฐอเมริกา ร่วมกับสถาบันวิจัยและมหาวิทยาลัยอื่น ๆ โดยปัจจุบันจัดแข่งขันไบโอเมตริก 3 ประเภท คือ ลายนิ้วมือ ลายม่านตา และใบหน้า หน่วยงานเหล่านี้ มีผลการประเมินที่เปิดเผย ดังนี้

5.3.1 การประเมินสมรรถนะการรู้จำใบหน้า ลายนิ้วมือ ลายม่านตา โดย NIST

NIST ได้เปิดทำการทดสอบผลิตภัณฑ์การรู้จำตัวบุคคลด้วยใบหน้า ลายนิ้วมือ และลายม่านตา ซึ่งเป็นการทดสอบแบบต่อเนื่อง (Ongoing) ซึ่งไม่กำหนดวันสิ้นสุดการทดสอบและมีการปรับปรุง (Update) ผลการทดสอบให้เป็นปัจจุบันเสมอ ซึ่งการทดสอบแต่ละประเภทมีดังต่อไปนี้

1) การทดสอบผลิตภัณฑ์การรู้จำตัวบุคคลด้วยใบหน้า (Face Recognition Vendor Test (FRVT)) โดยแบ่งการทดสอบย่อยออกเป็น 4 ประเภท ได้แก่
   (1) การทดสอบการรู้จำใบหน้าแบบการยืนยันตัวบุคคล (FRVT 1:1) [Grother2021a]
   (2) การทดสอบการรู้จำใบหน้าแบบการระบุตัวบุคคล (FRVT 1:N) [Grother2021b]
   (3) การทดสอบการตรวจจับการปลอมแปลงภาพใบหน้าแบบการผสมใบหน้า (FRVT MORPH) [Ngan2020]
   (4) การทดสอบการประเมินคุณภาพของภาพใบหน้า (FRVT Quality) [Grother2020]
2) การทดสอบผลิตภัณฑ์การรู้จำตัวบุคคลด้วยลายนิ้วมือ โดยแบ่งการทดสอบย่อยออกเป็น 4 ประเภท ได้แก่

(1) การประเมินเทมเพลต ลายนิ้วมือเฉพาะสำหรับการยืนยันตัวบุคคล (Proprietary Fingerprint Template Evaluation (PFT)) [37]

(2) การประเมินการใช้งานและการแลกเปลี่ยนข้อมูลมินูเทียร์ (MINEX) [38]

(3) การประเมินการรู้จำลายนิ้วมือแฝงสำหรับการระบุตัวบุคคล (Evaluation of Latent Fingerprints Technologies (ELFT)) [39]

(4) การประเมินการตัดแยกลายนิ้วมือจากภาพแบบวางตบสี่นิ้ว (Slapseg) [40]

3) การทดสอบผลิตภัณฑ์การรู้จำตัวบุคคลด้วยลายม่านตา

ในการประเมินการใช้งานและการแลกเปลี่ยนข้อมูลลายม่านตา (Iris Exchange (IREX) 10) [41] ปัจจุบันเปิดการทดสอบเฉพาะการทำงานแบบการระบุตัวบุคคล (1:N)

5.3.2 การประเมินสมรรถนะการรู้จำลายนิ้วมือโดย FVC Ongoing

มหาวิทยาลัยโบโลญญาจัดการแข่งขันอัลกอริทึมการรู้จำตัวบุคคลด้วยลายนิ้วมือแบบต่อเนื่อง (FVC-Ongoing) ซึ่งในการแข่งขันสามารถแบ่งการทดสอบออกเป็น 5 ประเภท[42] ได้แก่

1) การทดสอบอัลกอริทึมการยืนยันตัวบุคคลด้วยลายนิ้วมือ (Fingerprint Verification)
2) การทดสอบอัลกอริทึมการยืนยันตัวบุคคลด้วยเทมเพลตมินูเทียร์ตามมาตรฐาน ISO (Fingerprint Matching ISO)
3) การทดสอบอัลกอริทึมการทำดัชนีลายนิ้วมือ (Fingerprint Indexing)
4) การทดสอบอัลกอริทึมการตรวจจับทิศทางลายนิ้วมือ (Fingerprint Orientation Extraction)
5) การทดสอบอัลกอริทึมการสร้างเทมเพลตปกป้องข้อมูลลายนิ้วมือ สำหรับการยืนยันตัวบุคคล (Secure Template Fingerprint Verification)

5.3.3 การประเมินสมรรถนะการตรวจจับการปลอมแปลงโดยมหาวิทยาลัยต่างๆ

มหาวิทยาลัยคลาร์กสันร่วมกับสถาบันวิจัยและมหาวิทยาลัยอื่น ๆ ในการจัดการแข่งขันการตรวจจับการปลอมแปลงไบโอเมตริก ซึ่งการแข่งขันไม่ได้ถูกจัดอย่างต่อเนื่อง โดยการแข่งขันล่าสุดแต่ละประเภทสามารถจำแนกตามไบโอเมตริกที่ใช้ ดังนี้

1) การแข่งขันการตรวจจับการปลอมแปลงภาพใบหน้า 2021 (LivDet Face 2021) [Purnapatra2021]
2) การแข่งขันการตรวจจับการปลอมแปลงลายนิ้วมือ 2021 (LivDet 2021 Fingerprint Liveness Detection Competition – Into The Unknown) [Casula2021]
3) การแข่งขันการตรวจจับการปลอมแปลงลายม่านตา 2020 (LivDet Iris 2020) [Das2020]

---

[37] https://pages.nist.gov/pft/results/pftiii

[38] https://www.nist.gov/itl/iad/image-group/minutiae-interoperability-exchange-minex-iii

[39] https://pages.nist.gov/elft/elft_1_x/results/

[40] https://pages.nist.gov/slapseg/results/slapsegiii/

[41] https://pages.nist.gov/IREX10/

[42] https://biolab.csr.unibo.it/FVCOnGoing/UI/Form/Benchmarks.aspx

เอกสารอ้างอิงภาษาไทย

[ทูลแสงงาม 2549] พีรณัฐ ทูลแสงงาม ขั้นตอนวิธีการดึงลักษณะเด่นและทำการเปรียบเทียบเพื่อใช้รู้จำลายม่านตามนุษย์ วิทยานิพนธ์ปริญญาโท มหาวิทยาลัยเกษตรศาสตร์ 2549.

[น้อยปัญญา2563] ทพพล น้อยปัญญา “การสแกนใบหน้าของบุคคลกำลังเป็นปัญหา” Thaipublica, 9 มีนาคม 2020 สืบค้นเมื่อ 10 ต.ค. 2564 จาก https://thaipublica.org/2020/03/toppol13/

[มหาแถลง2564] ทัชชภร มหาแถลง “มาตรการในการคุ้มครองข้อมูลชีวมาตรตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” งานประชุมวิชาการระดับชาติ มหาวิทยาลัยรังสิต ประจำปี 2564 หน้าที่ 336-348. เม.ย. 2564.

[ยุบลชิต2564] เมธิชา ยุบลชิต “การคุ้มครองข้อมูลชีวมาตรภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร ปีที่ 14 ฉบับที่ 1 หน้าที่ 49-71 ม.ค.-มิ.ย. 2564.

[โหราพงศ์2549] กิตติพล โหราพงศ์ ขั้นตอนวิธีการรู้จำม่านตาและการพัฒนาซอฟต์แวร์ระบบไบโอเมตริก วิทยานิพนธ์ปริญญาโท มหาวิทยาลัยเกษตรศาสตร์ 2549.

[อารีกุล2557] วุฒิพงศ์ อารีกุล การประมวลลายนิ้วมือดิจิทัล ม.เกษตรศาสตร์ 2557.

[อินเดียแอดฮาร์2561] การปฏิวัติข้อมูลด้านอัตลักษณ์ของอินเดียด้วยเลข 12 หลัก ตอนที่ 4 รายงานสถานการณ์เศรษฐกิจการค้าอินเดีย สำนักงานส่งเสริมการค้าในต่างประเทศ ณ กรุงนิวเดลี 5 มีนาคม พ.ศ. 2561 https://www.ditp.go.th/contents_attach/220375/220375.pdf

[ไอซีที2554] คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ “โครงการศึกษาและเสนอแนะกรอบแนวทางการแลกเปลี่ยนข้อมูลไบโอเมตริกระหว่างหน่วยงานภาครัฐ” สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. กย. 2554.

Reference

[Aadhaar2020] ANNUAL REPORT, Unique Identification Authority of India, 2019-2020 https://uidai.gov.in/images/AADHAR_AR_2019_20_ENG_approved.pdf

[ACE2010] ACE Facilitators, “Age limit for biometric identification,” ACE Electoral Knowledge Network, November 22. 2010 สืบค้นเมื่อ 10 ต.ค. 2564 จาก https://aceproject.org/electoral-advice/archive/questions/replies/306802609

[Ahonen2006] T. Ahonen, A. Hadid and M. Pietikainen, “Face description with local binary patterns: Application to face recognition,” IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 28, pp. 2037-2041, 2006.

[Aldeneh2021] Z. Aldeneh and E. Mower Provost, “You're Not You When You're Angry: Robust Emotion Features Emerge by Recognizing Speakers,” IEEE Transactions on Affective Computing, June 2021.

[Atanasiu2010] A. Atanasiu, M.I. Mihailescu, "Biometric passports (ePassports)," in the 8th International Conference onCommunications/IEEE Xplore, Jul 2010, pp. 443-446.

[Auksorius2020] E. Auksorius, K. B. Raja, B. Topcu, R. Ramachandra, C. Busch and C. A. Boccara. Compact and Mobile Full-Field Optical Coherence Tomography Sensor for Subsurface Fingerprint Imaging. IEEE Access, 8, pp.15194-15204. 2020.

[Azom2015] V. Azom, A. Adewumi, and J. Tapamo, “Face and Iris biometrics person identification using hybrid fusion at feature and score-level,” In 2015 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech), pp. 207-212, Nov 2015.

[Barnes2011] J. G. Barnes. Chapter 1 History. Fingerprint Source Book, Washington, DC, USA: Office of Justice Programs, pp. 5-22, 2011.

[Belhumeur1997] P. N. Belhumeur, J. P. Hespanha and D. J. Kriegman, “Eigenfaces vs. fisherfaces: Recognition using class specific linear projection,” IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 19, pp. 711-720, 1997.

[Benesty2008] J. Benesty, M.M. Sondhi, and Y. Huang, Handbook of Speech Processing, Vol. 1, Springer, 2008.

[Best-Rowden2017] L. Best-Rowden and A. K. Jain, “Longitudinal study of automatic face recognition,” IEEE transactions on pattern analysis and machine intelligence, 40(1), 148-162, 2017.

[Cai2020] Y. Cai, L. Li, D. Wang and A. Abel, "Deep Normalization for Speaker Vectors," IEEE/ACM Transactions on Audio, Speech, and Language Processing, Dec. 2020. DOI: 10.1109/TASLP.2020.3039573

[Cao2010] Z. Cao, Q. Yin, X. Tang and J. Sun, “Face recognition with learning-based descriptor,” in Proc. CVPR 2010, 2707-2714.

[Cao2019] K. Cao, D. L. Nguyen, C. Tymoszek and A. K. Jain. End-to-end latent fingerprint search. IEEE Transactions on Information Forensics and Security, 15, pp.880-894. 2019.

[Cappelli2010] R. Cappelli, M. Ferrara and D. Maltoni. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. IEEE transactions on pattern analysis and machine intelligence, 32(12), pp.2128-2141. 2010.

[Casula2021] R. Casula, M. Micheletto, G. Orrù, R. Delussu, S. Concas, A. Panzino and G. L. Marcialis. LivDet 2021 Fingerprint Liveness Detection Competition-Into the unknown. In 2021 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-6). IEEE. 2021.

[Chen2005] W. Chen, K. Chih, S. Shih, and C. Hsieh, “Personal identification technique based on human iris recognition with wavelet transform,” in Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '05), 2005, pp.949–952.

[Chen2013] D. Chen, X. Cao, F. Wen and J. Sun, “Blessing of dimensionality: High-dimensional feature and its efficient compression for face verification,” in Proc. CVPR, 2013.

[Chen2015] T.-H. Chan, K. Jia, S. Gao, J. Lu, Z. Zeng and Y. Ma, “PCAnet: A simple deep learning baseline for image classification?,” IEEE Trans. on Image Processing, vol. 24, pp. 5017-5032, 2015.

[Chen2021] K. Chen, T. Yi and Q. Lv, "LightQNet: Lightweight Deep Face Quality Assessment for Risk-Controlled Face Recognition," in IEEE Signal Processing Letters, vol. 28, pp. 1878-1882, 2021, doi:10.1109/LSP.2021.3109781

[Chettri2021] B. Chettri, E. Benetos and B. L. T. Sturm, "Dataset Artefacts in Anti-Spoofing Systems: A Case Study on the ASVspoof 2017 Benchmark," IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 28, pp. 3018-3028, 2020. DOI: 10.1109/TASLP.2020.3036777

[Chugh2019] T. Chugh and A. K. Jain. OCT fingerprints: Resilience to presentation attacks. arXiv preprint arXiv:1908.00102. 2019.

[Chugh2020a] T. Chugh and A. K. Jain. Fingerprint spoof detector generalization. IEEE Transactions on Information Forensics and Security, 16, pp.42-55. 2020.

[Chugh2020b] T. Chugh and A. K. Jain. Fingerprint spoof detection: Temporal analysis of image sequence. In 2020 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-10). IEEE. 2020.

[Darlow2015] L. N. Darlow, S. S. Akhoury and J. Connan. Internal fingerprint acquisition from optical coherence tomography fingertip scans. In 2015 Third International Conference on Digital Information, Networking, and Wireless Communications (DINWC) (pp. 188-191). IEEE. 2015.

[Das2020] P. Das, J. Mcfiratht, Z. Fang, A. Boyd, G. Jang, A. Mohammadi, S. Purnapatra, D. Yambay, S. Marcel, M. Trokielewicz and P. Maciejewicz. Iris liveness detection competition (livdet-iris)-the 2020 edition. In 2020 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-9), IEEE. 2020.

[Daugman1993] J. G. Daugman, “High confidence visual recognition of persons by a test of statistical independence”, IEEE Trans. Pattern Anal. Mach. Intell., vol. 15, no. 11, pp. 1148–1161, Nov. 1993.

[Daugman1994] J. G. Daugman, “Biometric Personal Identification System Based on Iris Analysis”, U.S.Patent 5,291,560, Mar 1994.

[Daugman2004] J. G. Daugman, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, 2004.

[Daugman2006] J. G. Daugman, “Probing the Uniqueness and Randomness of IrisCodes: Results From 200Billion Iris Pair Comparisons”, Proceedings of the IEEE; 2006, vol. 94, p. 1927-1935.

[Daugman2007] J. G. Daugman, “New Methods in Iris Recognition,” IEEE Trans. Systems, Man, and Cybernetics, Part B, vol. 37, no. 5, pp. 1167-1175, 2007.

[Deng2012] W. Deng, J. Hu and J. Guo, “Extended SRC: Undersampled face recognition via intraclass variant dictionary,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 34, pp. 1864-1870, 2012.

[Deng2018] W. Deng, J. Hu and J. Guo, “Face recognition via collaborative representation: Its discriminant nature and superposed representation,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 99, pp. 1-1, 2018.

[Deng2019a] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, “Arcface: Additive angular margin loss for deep face recognition,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4690-4699, 2019.

[Deng2019b] J. Deng, J. Guo, E. Ververas, I. Kotsia, and S. Zafeiriou, “Retinaface: Single-shot multi-level face localisation in the wild. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 5203-5212, 2020.

[Engelsma2019] J. J. Engelsma, K. Cao and A. K. Jain. Learning a fixed-length fingerprint representation. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2019.

[Engelsma2021] J. J. Engelsma, D. Deb, K. Cao, A. Bhatnagar, P. S. Sudhish and A. K. Jain. Infant-ID: Fingerprints for Global Good. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2021.

[Fang2021] M. Fang, N. Damer, F. Boutros, F. Kirchbuchner, and A. Kuijper, “Iris Presentation Attack Detection by Attention-based and Deep Pixel-wise Binary Supervision Network,” In 2021 IEEE International Joint Conference on Biometrics (IJCB), pp. 1-8, Aug 2021

[Feng2010] J. Feng, A. K. Jain and A. Ross. Detecting altered fingerprints. In 2010 20th International Conference on Pattern Recognition (pp. 1622-1625). IEEE. 2010.

[Flom1987] L. Flom and A. Safir, “Iris Recognition System”, U.S.Patent 4,641,349, Feb 1987.

[Galbally2019] J. Galbally, P. Ferrara, R. Haraksim, A. Psyllos, and L. Beslay, “Study on face identification technology for its implementation in the Schengen information system,” Joint Res. Centre, Ispra, Italy, Rep. JRC-34751, 2019.

[Gangwar2016] A. Gangwar and A. Joshi, “DeepIrisNet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition,” in IEEE ICIP, Sept 2016, pp. 2301–2305.

[Garcia2021] Evan Garcia, “Illinois’ Law Protecting Biometric Privacy Could Be Changed” WTTW NEWS, March 30, 2021 สืบค้นเมื่อ 10 ต.ค. 2564 จาก https://news.wttw.com/2021/03/30/illinois-law-protecting-biometric-privacy-could-be-changed

[Garris2001] M. D. Garris. Latent Fingerprint Training with NIST Special Database 27 and Universal Latent Workstation. Rep. NISTIR 6799. 2001.

[Gomez-Alanis2021] A. Gomez-Alanis, J. A. Gonzalez-Lopez, S. P. Dubagunta, A. M. Peinado and M. Magimai.-Doss, "On Joint Optimization of Automatic Speaker Verification and Anti-Spoofing in the Embedding Space," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1579-1593, 2021. DOI: 10.1109/TIFS.2020.3039045

[Grosz2021] S. A. Grosz, J. J. Engelsma and A. K. Jain. C2CL: Contact to Contactless Fingerprint Matching. arXiv preprint arXiv:2104.02811. 2021.

[Grother2020] P. Grother, A. Hom, M. Ngan and K. Hanaoka. Ongoing face recognition vendor test (frvt) part 5: Face Image Quality Assessment (Draft). National Institute of Standards and Technology, 2020.

[Grother2021a] P. Grother, M. Ngan and K. Hanaoka. Ongoing face recognition vendor test (frvt) part 1: Verification. National Institute of Standards and Technology. 2021.

[Grother2021b] P. Grother, M. L. Ngan and K. Hanaoka. Ongoing face recognition vendor test (frvt) part 2: Identification. 2021.

[Guillaumin2009] M. Guillaumin, J. Verbeek and C. Schmid, “Is that you? Metric learning approaches for face identification,” in Proc. ICCV, 2009.

[Hafner2021] A. Hafner, P. Peer, Z. Emersic, M. Vitek, “Deep Iris Feature Extraction,” in 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), April 2021, pp. 258–262.

[Hayes2019] Ned Hayes, “Ethics and biometric identity,” Security Info Watch, March 19, 2019. สืบค้นเมื่อ 10 ต.ค. 2564 จาก https://www.securityinfowatch.com/access-identity/biometrics/article/21072152/ethics-and-biometric-identity

[He2005] X. He, S. Yan, Y. Hu, P. Niyogi and H.-J. Zhang, “Face recognition using laplacianfaces,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 27, pp. 328-340, 2005.

[Henniger2009] O. Henniger, D. Muramatsu, T. Matsumoto, I. Yoshimura, M. Yoshimura (2009) Signature Recognition. In: Li S.Z., Jain A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-73003-5_137

[Henry1900] E. R. Henry. Classification and Uses of Finger Prints.[Sl]: George Routledge and Sons, 1900.

[Horapong2021] K. Horapong, K. Srisutheenon and V. Areekul. Progressive and Corrective Feedback for Latent Fingerprint Enhancement Using Boosted Spectral Filtering and Spectral Autoencoder. IEEE Access, 9, pp.96288-96308. 2021.

[Hou2021a] B. Hou and R. Yan, “ArcVein-Arccosine Center Loss for Finger-Vein Verification,” IEEE Transactions on Instrumentation and Measurement, Feb. 2021. DOI: 10.1109/TIM.2021.3062164

[Hou2020b] B. Hou and R. Yan, “Convolutional Autoencoder Model for Finger-Vein Verification,” IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 5, pp. 2067-2074, May 2020. DOI: 10.1109/TIM.2019.29211355

[Hu2021a] W. Hu, W. Yan and H. Hua, "Dual Face Alignment Learning Network for NIR-VIS Face Recognition," in IEEE Transactions on Circuits and Systems for Video Technology, doi: 10.1109/TCSVT.2021.3081514.

[Hu2021b] W. Hu and H. Hu, "Orthogonal Modality Disentanglement and Representation Alignment Network for NIR-VIS Face Recognition," in IEEE Transactions on Circuits and Systems for Video Technology, doi: 10.1109/TCSVT.2021.3105411.

[Huang2021] T. -R. Huang, S. -M. Hsu and L. -C. Fu, "Data Augmentation via Face Morphing for Recognizing Intensities of Facial Emotions," in IEEE Transactions on Affective Computing, doi: 10.1109/TAFFC.2021.3096922.

[ISO/IEC_19795-1] ISO/IEC 19795-1:2021(en) Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

[Jain2007] A.K. Jain, P. Flynn, A.A. Ross, Handbook of Biometrics, Springer, 2007.

[Jain2011] A. K. Jain, A. Ross and K. Nandakumar. Introduction to biometrics. Springer Science & Business Media. 2011.

[Jia2021] G. Jia et al., "Inconsistency-Aware Wavelet Dual-Branch Network for Face Forgery Detection," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 3, pp. 308-319, July 2021, doi: 10.1109/TBIOM.2021.3086109.

[Kauba2021] C. Kauba, S. Kirchgasser, V. Mirjalili, A. Uhl and A. Ross, “Inverse Biometrics: Generating Vascular Images from Binary Templates," IEEE Transactions on Biometrics, Behavior, and Identity Science, April 2021. DOI: 10.1109/TBIOM.2021.3073666

[Kelly2021] F. Kelly and J. H. L. Hansen, “Analysis and calibration of Lombard effect and whisper for speaker recognition,” IEEE/ACM Transactions on Audio, Speech, and Language Processing, Jan. 2021. DOI: 10.1109/TASLP.2021.3053388

[Keykhaie2021] S. Keykhaie and S. Pierre, "Lightweight and Secure Face-based Active Authentication for Mobile Users," in IEEE Transactions on Mobile Computing, doi: 10.1109/TMC.2021.3106256.

[Krichen2005] E. Krichen, L.Allano, S. Garcia-Salicetti, B. Dorizzi, “Specific Texture Analysis for Iris Recognition,” Audio- and Video-Based Biometric Person Authentication. AVBPA 2005. Lecture Notes in Computer Science, vol 3546. Springer, Berlin, Heidelberg.

[Lai2021] S. Lai, L. Jin, Y. Zhu, Z. Li and L. Lin, “SynSig2Vec: Forgery-free Learning of Dynamic Signature Representations by Sigma Lognormal-based Synthesis,” IEEE Transactions on Pattern Analysis and Machine Intelligence, June 2021. DOI: 10.1109/TPAMI.2021.3087619

[Lei2014] Z. Lei, M. Pietikainen and S. Z. Li, “Learning discriminant face descriptor,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 36, pp. 289-302, 2014.

[Li2020] L. Li, M. -W. Mak and J. -T. Chien, "Contrastive Adversarial Domain Adaptation Networks for Speaker Recognition," IEEE Transactions on Neural Networks and Learning Systems, Dec. 2020. DOI: 10.1109/TNNLS.2020.3044215

[Li2021] H. Li, P. Wei and P. Hu, “AVN: An Adversarial Variation Network Model for Handwritten Signature Verification,” IEEE Transactions on Multimedia, Feb. 2021. DOI: 10.1109/TMM.2021.3056217

[Lin2021] J. -D. Lin et al., "Lightweight Face Anti-Spoofing Network for Telehealth Applications," in IEEE Journal of Biomedical and Health Informatics, doi: 10.1109/JBHI.2021.3107735.

[Maio2002a] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain. FVC2000: Fingerprint verification competition. IEEE transactions on pattern analysis and machine intelligence, 24(3), pp.402-412. 2002.

[Maio2002b] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain. FVC2002: Second fingerprint verification competition. In Object recognition supported by user interaction for service robots (Vol. 3, pp. 811-814). IEEE. 2002.

[Maio2004] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain. FVC2004: Third fingerprint verification competition. In International conference on biometric authentication (pp. 1-7). Springer, Berlin, Heidelberg. 2004.

[Maltoni2009] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition. Springer Science & Business Media, 2009.

[Matey2006] J.R. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D.J. Lolacono, S. Mangru, M. Tinker, T.M. Zappia, and W.Y. Zhao, “Iris on the move: Acquisition of images for iris recognition in less constrained environments”. Proceedings of the IEEE, 94(11), 2006, pp.1936-1947.

[Medina-Pérez2014] M. A. Medina-Pérez, O. Loyola-González, A. E. Gutierrez-Rodríguez, M. García-Borroto and L. Altamirano-Robles. Introducing an experimental framework in c# for fingerprint recognition. In Mexican Conference on Pattern Recognition (pp. 132-141). Springer, Cham. 2014.

[Moghaddam2000] B. Moghaddam, T. Jebara and A. Pentland, “Bayesian face recognition,” Pattern Recognition, vol. 33, pp. 1771-1782, 2000.

[Nautsch2021] A. Nautsch et al., “ASVspoof 2019: spoofing countermeasures for the detection of synthesized, converted and replayed speech,” IEEE Transactions on Biometrics, Behavior, and Identity Science, Feb. 2021.

[Ng-Kruelle2006] G. Ng-Kruelle, P.A. Swatman, J.F. Hampe, D.S. Rebne, “Biometrics and e-Identity (e-Passport) in the European Union: End-User Perspectives on the Adoption of a Controversial Innovation,” in Journal Theor. Appl. Electron. Commer. Res. 2006, vol. 1, pp. 12-35.

[Ngan2020] M. Ngan, M. Ngan, P. Grother, K. Hanaoka and J. Kuo. Face recognition vendor test (frvt) part 4: Morph-performance of automated face morph detection. US Department of Commerce, National Institute of Standards and Technology. 2020.

[Nguyen2011] K. Nguyen, C. Fookes, S. Sridharan, and S. Denman, "Quality-driven super-resolution for less constrained iris recognition at a distance and on the move," IEEE Trans. on Information Forensics and Security 6(4), pp. 1248–1258, Dec 2011.

[Nguyen2017] K. Nguyen, C. Fookes, R. Jillela, S. Sridharan, and A. Ross, “Long range iris recognition: A survey,” Pattern Recognition, vol. 72, pp. 123-143. 2017.

[Nguyen2018] D. L. Nguyen, K. Cao and A. K. Jain. Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge. In 2018 International Conference on Biometrics (ICB) (pp. 9-16). IEEE. 2018.

[NIST-ITL2011] ANSI/NIST-ITL 1-2011 “Data format for the interchange of fingerprint, facial & other biometric information,” NIST Special Publication 500-290 Edition 3, 2015.

[Oktiana2019] M. Oktiana, K. Saddami, F. Arnia, Y. Away, K. Hirai, T. Horiuchi, and K. Munadi, “Advances in Cross-Spectral Iris Recognition Using Integrated Gradientface-Based Normalization,” IEEE Access, vol.7, pp. 130484-130494, Aug 2019.

[Othman2016] N. Othman, B. Dorizzi, S. Garcia-Salicetti, “OSIRIS: An open source iris recognition software,” Pattern Recognition Letters, vol.82, part2, pp.124-131, 2016.

[Ouda2021] O. Ouda, “On the Practicality of Local Ranking-Based Cancelable Iris Recognition,” IEEE Access, vol.9, pp. 86392-86403, Jun 2021.

[Pakrasi2021] Susmita Pakrasi, “Aadhaar card: No fingerprint, eye scan for children below 5 years,” Hindustan Times, Jul 27, 2021. สืบค้นเมื่อ 10 ต.ค. 2564 จาก https://www.hindustantimes.com/india-news/aadhaar-card-no-fingerprint-eye-scan-for-children-below-5-years-101627353199035.html

[Parkhi2015] O. M. Parkhi, A. Vedaldi and A. Zisserman, “Deep Face Recognition,” 2015.

[Peng2021] C. Peng, M. Chen and X. Jiang, “Under-Display Ultrasonic Fingerprint Recognition With Finger Vessel Imaging,” IEEE Sensors Journal, vol. 21, no. 6, pp. 7412-7419, March 2021. DOI: 10.1109/JSEN.2021.3051975

[Priesnitz2021] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch and M. Margraf. An overview of touchless 2D fingerprint recognition. EURASIP Journal on Image and Video Processing, 2021(1), pp.1-28. 2021.

[Purnapatra2021] S. Purnapatra, N. Smalt, K. Bahmani, P. Das, D. Yambay, A. Mohammadi, A. George, T. Bourlai, S. Marcel, S. Schuckers and M. Fang. Face Liveness Detection Competition (LivDet-Face)-2021. In 2021 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-10). IEEE. 2021.

[Qian2021] Y. Qian, Z. Chen and S. Wang, “Audio-Visual Deep Neural Network for Robust Person Verification,” IEEE/ACM Transactions on Audio, Speech, and Language Processing, Feb. 2021.

[Qin2021a] Y. Qin, Z. Yu, L. Yan, Z. Wang, C. Zhao and Z. Lei, "Meta-teacher for Face Anti-Spoofing," in IEEE Transactions on Pattern Analysis and Machine Intelligence, doi: 10.1109/TPAMI.2021.3091167.

[Qin2021b] H. Qin, M. A. El-Yacoubi, Y. Li and C. Liu, “Multi-scale and Multi-direction GAN for CNN-based Single Palm-vein Identification,” IEEE Transactions on Information Forensics and Security, Feb. 2021. DOI: 10.1109/TIFS.2021.3059340

[Qiu2021] H. Qiu, D. Gong, Z. Li, W. Liu and D. Tao, "End2End Occluded Face Recognition by Masking Corrupted Features," in IEEE Transactions on Pattern Analysis and Machine Intelligence, doi: 10.1109/TPAMI.2021.3098962.

[Raja2014] K. B. Raja; R. Raghavendra, C. Busch, “Binarized statistical features for improved iris and periocular recognition in visible spectrum,” In Proc. IWBF, pp. 1–6, 2014.

[Rathgeb2016] C. Rathgeb, A. Uhl, P. Wild, and H. Hofbauer, “Design decisions for an Iris recognition SDK,” in Handbook of Iris Recognition (Advances in Computer Vision and Pattern Recognition), 2nd ed., K. Bowyer and M. J. Burge, Eds. London, U.K.: Springer, 2016.

[Rebera2012] A. P. Rebera and B. Guihen “Biometrics for an Ageing Society Societal and Ethical Factors in Biometrics and Ageing” in 2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), pp. 409-416, Sept 2012.

[Robinson&Cole2019] Robinson & Cole LLP, “Google Sued Under Illinois Biometric Information Privacy Act,” Lexology, October 3 2019 สืบค้นเมื่อ 10 ต.ค. 2564 จาก https://www.lexology.com/library/detail.aspx?g=51dd0122-9399-48e9-b6ef-fc357760d387

[Ross2010] A. Ross, "Iris Recognition: The Path Forward" in Computer, vol. 43, no. 02, pp. 30-35, 2010.

[Schroff2015] F. Schroff, D. Kalenichenko and J. Philbin, “Facenet: A unified embedding for face recognition and clustering,” in Proc. CVPR, 2015.

[Shahreza2021] H. O. Shahreza and S. Marcel, “Towards Protecting and Enhancing Vascular Biometric Recognition methods via Biohashing and Deep Neural Networks,” IEEE Transactions on Biometrics, Behavior, and Identity Science, April 2021. DOI: 10.1109/TBIOM.2021.3076444

[Sharma2020] R. Sharma and A. Ross, “Viability of Optical Coherence Tomography for Iris Presentation Attack Detection,” In 2020 25th International Conference on Pattern Recognition (ICPR), pp. 6165-6172.

[Sharma2021] R. Sharma and A. Ross, “Image-Level Iris Morph Attack,” In 2021 IEEE International Conference on Image Processing (ICIP), pp. 3013-3017, Sep 2021.

[Shen2021] M. Shen, H. Yu, L. Zhu, K. Xu, Q. Li and J. Hu, "Effective and Robust Physical-World Attacks on Deep Learning Face Recognition Systems," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4063-4077, 2021, doi: 10.1109/TIFS.2021.3102492.

[Simonyan2013] K. Simonyan, O. M. Parkhi, A. Vedaldi and A. Zisserman, “Fisher Vector Faces in the Wild,” 2013.

[Song2004] Y. Song, C. Lee and J. Kim. A new scheme for touchless fingerprint recognition system. In Proceedings of 2004 International Symposium on Intelligent Signal Processing and Communication Systems, 2004. ISPACS 2004. (pp. 524-527). IEEE. 2004.

[Sun2014] Y. Sun, Y. Chen, X. Wang and X. Tang, “Deep learning face representation by joint identification-verification,” in Proc. NIPS, 2014.

[Sundararajan2018] K. Sundararajan and D.L. Woodard, “Deep learning for biometrics: A survey,” ACM Computing Surveys (CSUR), 51(3),pp. 1-34, 2018.

[Tabassi2021] E. Tabassi, M. Olsen, O. Bausinger, C. Busch, A. Figlarz, G. Fiumara, O. Henniger, J. Merkle, T. Ruhland, C. Schiel and M. Schwaiger. NFIQ 2 NIST Fingerprint Image Quality. 2021.

[Taigman2014] Y. Taigman, M. Yang, M. Ranzato and L. Wolf, “Deepface: Closing the gap to human-level performance in face verification,” in Proc. CVPR, 2014.

[Tang2017] Y. Tang, F. Gao, J. Feng and Y. Liu. FingerNet: An unified deep network for fingerprint minutiae extraction. In 2017 IEEE International Joint Conference on Biometrics (IJCB) (pp. 108-116). IEEE. 2017.

[TechCrunch2021] TechCrunch, “Facebook will pay $650 million to settle class action suit centered on illinois privacy law” สืบค้นเมื่อ 10 ต.ค. 2564 จาก https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/

[Tolosana2021] R. Tolosana, R. Vera-Rodriguez, J. Fierrez and J. Ortega-Garcia, “DeepSign: Deep On-Line Signature Verification,” IEEE Transactions on Biometrics, Behavior, and Identity Science, Jan. 2021. DOI: 10.1109/TBIOM.2021.3054533

[Tu2021] X. Tu et al., "Joint Face Image Restoration and Frontalization for Recognition," in IEEE Transactions on Circuits and Systems for Video Technology, doi: 10.1109/TCSVT.2021.3078517.

[Turk1991] M. Turk and A. Pentland, “Eigenfaces for recognition,” Journal of cognitive neuroscience, vol. 3, pp. 71-86, 1991.

[Venugopalan2011] S. Venugopalan and M. Savvides, “How to Generate Spoofed Irises From an Iris Code Template,” IEEE Transactions on Information Forensics and Security, vol. 6, pp. 385–395, Jun 2011.

[Vestman2018] V. Vestman, D. Gowda, M. Sahidullah, P. Alku, and T. Kinnunen, “Speaker recognition from whispered speech: A tutorial survey and an application of time-varying linear prediction,” Speech Communication, 99, pp. 62-79, 2018.

[Wang2021a] Q. Wang and G. Guo, "DSA-Face: Diverse and Sparse Attentions for Face Recognition Robust to Pose Variation and Occlusion," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4534-4543, 2021, doi: 10.1109/TIFS.2021.3109463.

[Wang2021b] Y. Wang, X. Song, T. Xu, Z. Feng and X. -J. Wu, "From RGB to Depth: Domain Transfer Network for Face Anti-Spoofing," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4280-4290, 2021, doi: 10.1109/TIFS.2021.3102448.

[Wang2021c] K. Wang, G. Chen and H. Chu, “Finger Vein Recognition Based On Multi-receptive Field Bilinear Convolutional Neural Network,” IEEE Signal Processing Letters, July 2021. DOI:10.1109/LSP.2021.3094998

[Watson1992] C.I. Watson and C.L. Wilson. NIST special database 4. Fingerprint Database, National Institute of Standards and Technology, 17(77), p.5. 1992.

[Wildes1994] R. P. Wildes, J. C. Asmuth, G. L. Green, S. C. Hsu, R. J. Kolczynski, J. R. Matey, and S. E. McBride, “A system for automated iris recognition,” in Proc. IEEE Workshop on Applications of Computer Vision, Sarasota, FL, 1994, pp. 121–128.

[Wiskott1997] L. Wiskott, J.-M. Fellous, N. Kruger and C. von der Malsburg, “Face recognition by elastic bunch graph matching,” in Proc. ICIP, 1997.

[Xia2021] Y. Xia, H. Yu, X. Wang, M. Jian and F. -Y. Wang, "Relation-Aware Facial Expression Recognition," in IEEE Transactions on Cognitive and Developmental Systems, doi: 10.1109/TCDS.2021.3100131.

[Xu2006] A. Xu, X. Jin, Y. Jiang and P. Guo, “Complete Two-Dimensional PCA for Face Recognition,” in Proc. ICPR, 2006.

[Yadav2021] S. Yadav and A. Ross, “CIT-GAN: Cyclic Image Translation Generative Adversarial Network With Application in Iris Presentation Attack Detection,” In 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), pp. 2411-2420, Jan 2021.

[Yang2020] C. -Z. Yang, J. Ma, S. -L. Wang and A. W. -C. Liew, "Preventing DeepFake Attacks on Speaker Authentication by Dynamic Lip Movement Analysis," IEEE Transactions on Information Forensics and Security, Dec. 2020. DOI: 10.1109/TIFS.2020.3045937

[Yoon2012a] S. Yoon, J. Feng and A. K. Jain. Altered fingerprints: Analysis and detection. IEEE transactions on pattern analysis and machine intelligence, 34(3), pp.451-464. 2012.

[Yoon2012b] S. Yoon, Q. Zhao and A. K. Jain. On matching altered fingerprints. In 2012 5th IAPR International Conference on Biometrics (ICB) (pp. 222-229). IEEE. 2012.

[Yoon2015] S. Yoon and A. K. Jain. Longitudinal study of fingerprint recognition. Proceedings of the National Academy of Sciences, 112(28), pp.8555-8560. 2015.

[Yu2021] Z. Yu, X. Li, P. Wang and G. Zhao, "TransRPPG: Remote Photoplethysmography Transformer for 3D Mask Face Presentation Attack Detection," in IEEE Signal Processing Letters, vol. 28, pp. 1290-1294, 2021, doi: 10.1109/LSP.2021.3089908.

[Yuan2005] X. Yuan, P. Shi, "Iris Feature Extraction Using 2D Phase Congruency," in the 3rd International Conference on Information Technology and Applications (ICITA), 2005, pp. 437-441.

[Zhang2005] W. Zhang, S. Shan, W. Gao, X. Chen and H. Zhang, “Local gabor binary pattern histogram sequence (LGBPHS): A novel non-statistical model for face representation and recognition,” in Proc. ICCV, 2005.

[Zhang2020] K. Zhang, Z. Shen, Y. Wang, Z. Sun, “All-in-Focus Iris Camera With a Great Capture Volume,” In 2020 International Joint Conference on Biometrics (IJCB 2020), pp. 1-9, Sep 2020.

[Zhang2021] Z. Zhang, F. Zhong and W. Kang, “Study on Reflection-Based Imaging Finger Vein Recognition,” IEEE Transactions on Information Forensics and Security, July 2021. DOI: 10.1109/TIFS.2021.3093791