ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 29 เล่ม 2-2565

ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 2: การใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน

BIOMETRIC TECHNOLOGY – PART 2: FACIAL RECOGNITION TECHNOLOGY USAGE FOR PERSONAL VERIFICATION

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.240.15

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 2: การใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน

ขมธอ. 29 เล่ม 2-2565

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 21 เมษายน พ.ศ. 2565

คณะทำงานจัดทำมาตรฐานเกี่ยวกับการพิสูจน์และยืนยันตัวตนด้วยเทคโนโลยีชีวมิติ

ที่ปรึกษาคณะทำงาน

ศาสตราจารย์ ดร.วุฒิพงศ์ อารีกุล	มหาวิทยาลัยเกษตรศาสตร์

ประธานคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะทำงาน

นางสมศรี หอกันยา	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	สำนักงานปลัดกระทรวงมหาดไทย
นายสัญชัย เตชนิมิตวัช	กรมการปกครอง
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวอาจารีย์ ศุภพิโรจน์	ธนาคารแห่งประเทศไทย
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริม การประกอบธุรกิจประกันภัย
นายวิบูลย์ ภัทรพิบูล	สำนักงานคณะกรรมการกำกับหลักทรัพย์ และตลาดหลักทรัพย์
นายศุภกาญจน์ บุญจันทร์	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ศาสตราจารย์ ดร.วิเชียร เปรมชัยสวัสดิ์	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายสืบศักดิ์ สืบภักดี	สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์
นายยศ กิมสวัสดิ์	สมาคมธนาคารไทย
นายณัฐพล โลหชิตพิทักษ์	สมาคมบริษัทหลักทรัพย์ไทย
นายทำนุ อมาตยกุล	สมาคมประกันชีวิตไทย
นางสาวปิยกานต์ ญาณอุดม	สมาคมประกันวินาศภัยไทย

เลขานุการ

นายสมบัติ ชั้นอินทร์งาม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายธวัชชัย พริ้งพร้อม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

วิเคราะห์และจัดทำข้อเสนอแนะมาตรฐานฯ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 2: การใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน

ดร. อรุชา รุ่งโชคอนันต์	มหาวิทยาลัยเกษตรศาสตร์
ดร. กิตติพล โหราพงศ์	มหาวิทยาลัยเกษตรศาสตร์
นางสาวพลอยนภัส เกิดจิรโรจน์	มหาวิทยาลัยเกษตรศาสตร์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 2: การใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน ฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดและข้อเสนอแนะสำหรับการบริหารจัดการอัตลักษณ์บุคคลที่มาจากการพิสูจน์และยืนยันตัวตนด้วยเทคโนโลยีการรู้จำใบหน้า โดยมีเป้าหมายเพื่อให้มีการนำเทคโนโลยีการรู้จำใบหน้าไปประยุกต์ใช้กับการพิสูจน์และยืนยันตัวตนในภาคบริการประชาชนได้อย่างมีประสิทธิภาพสูงสุด มีความน่าเชื่อถือในระดับสากล มีความถูกต้อง โปร่งใส มีความปลอดภัย และมีธรรมาภิบาล

ข้อเสนอแนะมาตรฐานนี้เหมาะกับหน่วยงานภาครัฐหรือภาคเอกชนที่ต้องการนำเทคโนโลยีการรู้จำใบหน้าไปประยุกต์ใช้กับการพิสูจน์และยืนยันตัวตน ซึ่งเป็นส่วนหนึ่งของระบบบริหารจัดการอัตลักษณ์บุคคล (Identity Management System (IdMS)) โดยข้อเสนอแนะมาตรฐานนี้ สามารถนำไปประยุกต์ใช้ในหน่วยงานที่เกี่ยวข้องกับการรักษาความปลอดภัยในหน่วยงานของรัฐหรือเอกชน รวมถึงหน่วยงานของรัฐที่ให้บริการประชาชนที่ต้องพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีการรู้จำใบหน้าร่วมกับหลักฐานแสดงตน อาทิ บัตรประชาชน หนังสือเดินทาง บัตรสวัสดิการแห่งรัฐ ใบอนุญาตทำงานต่างด้าว บัตรประกันสุขภาพถ้วนหน้า บัตรประกันสังคม บัตรประกันสังคมต่างด้าว ฯลฯ

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตนฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th
Website: www.etda.or.th

คำนำ

การให้บริการประชาชนของภาครัฐหรือภาคเอกชน อาจประกอบด้วยขั้นตอนการพิสูจน์และยืนยันตัวตนซึ่งมีความสำคัญเป็นอย่างยิ่ง รัฐบาลจึงได้ดำเนินงานพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่สอดคล้องกับนโยบายอำนวยความสะดวกในการประกอบธุรกิจ และการให้บริการกับประชาชน เพื่อให้เป็นโครงสร้างพื้นฐานทางดิจิทัลที่สำคัญของประเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ได้ร่วมกันกำหนดแนวทางการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของประเทศ และจัดทำข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล ขึ้นประกอบด้วยมาตรฐานทั้งหมดสามฉบับ คือ ขมธอ. 18-2564 [1] ขมธอ. 19-2564 [2] และ ขมธอ. 20-2564 [3] โดยมาตรฐานทั้งสามฉบับดังกล่าวได้ครอบคลุมการใช้ชีวมิติสำหรับสำหรับการพิสูจน์และยืนยันตัวตน

สำหรับข้อเสนอแนะมาตรฐานฉบับนี้ มีจุดมุ่งหมายในการกำหนดข้อเสนอแนะที่เน้นเกี่ยวกับการใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน ซึ่งเป็นส่วนจำเป็นที่ต่อขยายจากมาตรฐานทั้งสามฉบับข้างต้น เพื่อให้สามารถนำเทคโนโลยีการรู้จำใบหน้าไปปฏิบัติใช้งานได้จริงโดยมีประสิทธิภาพสูงสุด มีความถูกต้องน่าเชื่อถือในระดับสากล มีความโปร่งใส มีความมั่นคงปลอดภัย และรักษาสิทธิส่วนบุคคลของประชาชน รวมทั้งสามารถทำให้แต่ละหน่วยงานทั้งภาครัฐและเอกชนทำงานบูรณาการร่วมกัน โดยสามารถแลกเปลี่ยนข้อมูลภาพใบหน้าระหว่างกันได้อย่างมีประสิทธิภาพภายใต้ข้อจำกัดของกฎหมาย

ข้อเสนอแนะมาตรฐานนี้เหมาะกับหน่วยงานภาครัฐหรือภาคเอกชนที่ต้องการนำเทคโนโลยีการรู้จำใบหน้าไปประยุกต์ใช้งานในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งเป็นส่วนหนึ่งของระบบบริหารจัดการอัตลักษณ์บุคคล (Identity Management System: IdMS) โดยข้อเสนอแนะมาตรฐานนี้ สามารถนำไปประยุกต์ใช้ในหน่วยงานที่เกี่ยวข้องกับการรักษาความปลอดภัยในหน่วยงานของรัฐหรือเอกชน รวมถึงหน่วยงานของรัฐที่ให้บริการประชาชนที่ต้องพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีชีวมิติร่วมกับหลักฐานแสดงตน เช่น บัตรประชาชน หนังสือเดินทาง บัตรสวัสดิการแห่งรัฐ ใบอนุญาตทำงานต่างด้าว บัตรประกันสุขภาพถ้วนหน้า บัตรประกันสังคม บัตรประกันสังคมต่างด้าว ฯลฯ ทั้งนี้ การประยุกต์ใช้ข้อเสนอแนะมาตรฐานนี้ จะเป็นไปในภาพรวมเพื่อประยุกต์ใช้งานเทคโนโลยีชีวมิติให้มีประสิทธิภาพสูงสุดและทำงานได้อย่างเต็มประสิทธิภาพ โดยในกรณีที่มีหน่วยงานกำกับดูแลเฉพาะของแต่ละภาคส่วนกำหนดมาตรฐานการใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตนเป็นการเฉพาะแล้ว ให้ปฏิบัติตามมาตรฐานของหน่วยงานที่กำกับดูแลเหล่านั้น

สารบัญ

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม ๒: การใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน

โดยที่เป็นการสมควรกำหนดแนวทางการบริหารจัดการอัตลักษณ์บุคคลเพื่อการพิสูจน์และยืนยันตัวตนด้วยเทคโนโลยีการรู้จำใบหน้า เพื่อให้มีการนำเทคโนโลยีการรู้จำใบหน้าไปประยุกต์ใช้กับการพิสูจน์และยืนยันตัวตนในภาคบริการประชาชนได้อย่างมีประสิทธิภาพสูงสุด มีความน่าเชื่อถือในระดับสากล มีความถูกต้องโปร่งใส มีความปลอดภัย และมีธรรมาภิบาล

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม ๒: การใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน เลขที่ ขมธอ. ๒๙ เล่ม ๒-๒๕๖๕ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๒๑ เมษายน พ.ศ. ๒๕๖๕

ชัยชนะ มิตรพันธ์

(นายชัยชนะ มิตรพันธ์)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยเทคโนโลยีชีวมิติ - เล่ม 2: การใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานการใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตนฉบับนี้ เป็นส่วนต่อขยายของ “มาตรฐานการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน” [4] โดยเป็นข้อเสนอแนะมาตรฐานที่ลงรายละเอียดสำหรับหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน ในประเทศไทย ที่จะต้องประยุกต์ใช้เทคโนโลยีการรู้จำใบหน้าในการพิสูจน์และยืนยันตัวตนสำหรับงานบริการประชาชนในรูปแบบต่าง ๆ ตามหน้าที่และความรับผิดชอบ เพื่อให้มีแนวทางการทำงานร่วมกันในการใช้เทคโนโลยีการรู้จำใบหน้าให้เกิดประสิทธิภาพสูงสุด มีความถูกน่าเชื่อถือในระดับสากล มีความโปร่งใส มีความมั่นคงปลอดภัย และรักษาสิทธิส่วนบุคคลของประชาชน

ข้อเสนอแนะมาตรฐานฉบับนี้ ไม่ได้ครอบคลุมการใช้งานการรู้จำใบหน้าทางด้านนิติวิทยาศาสตร์ (forensic science) งานด้านการตรวจการณ์ด้วยกล้องวงจรปิด (video surveillance) และการรู้จำใบหน้าสามมิติ (3D face recognition) ซึ่งการใช้งานดังกล่าวต้องใช้ระบบการจัดการและการรู้จำใบหน้าในรูปแบบที่เฉพาะเจาะจง ซึ่งไม่ใช่เป้าหมายของข้อเสนอแนะมาตรฐานฉบับนี้

ทั้งนี้การประยุกต์ใช้ข้อเสนอแนะมาตรฐานนี้ จะเป็นไปในภาพรวมเพื่อประยุกต์ใช้งานเทคโนโลยีชีวมิติให้มีประสิทธิภาพสูงสุดและทำงานได้อย่างเต็มประสิทธิภาพ โดยในกรณีที่มีหน่วยงานกำกับดูแลเฉพาะของแต่ละภาคส่วนกำหนดมาตรฐานการใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตนเป็นการเฉพาะแล้ว ให้ปฏิบัติตามมาตรฐานของหน่วยงานที่กำกับดูแลเหล่านั้น

ในข้อเสนอแนะมาตรฐานฉบับนี้ จะใช้รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐานและเนื้อหาเชิงให้ข้อมูล ดังต่อไปนี้

- “ต้อง” ใช้ระบุสิ่งที่เป็นข้อกำหนด ซึ่งต้องปฏิบัติตาม
- “ควร” ใช้ระบุสิ่งที่เป็นข้อแนะนำ
- “อาจ” ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้

2. นิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 ลักษณะเฉพาะชีวมิติ (biometric characteristic) หมายถึง ลักษณะเฉพาะทางสรีรวิทยาหรือทางพฤติกรรมของแต่ละบุคคล ซึ่งสามารถใช้บอกความแตกต่าง และสามารถสกัดลักษณะเด่นที่สามารถทำซ้ำได้เพื่อใช้ในการรู้จำชีวมิติ

2.2 อัตลักษณ์ (identity) หมายถึง คุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล ซึ่งเป็นลักษณะเฉพาะและสามารถบ่งบอกหรือจำแนกบุคคลได้ภายในบริบทที่กำหนด [ขมธอ. 18-2564] [1]

2.3 ระบบบริหารอัตลักษณ์บุคคล (identity management system: IdMS) หมายถึง ระบบที่ทำหน้าที่บริหารจัดการเกี่ยวกับอัตลักษณ์บุคคล

2.4 ระบบรู้จำใบหน้าอัตโนมัติ (automated face recognition system) หมายถึง ระบบที่ใช้ทำหน้าที่ในการรู้จำใบหน้าโดยอัตโนมัติ โดยใช้ในการพิสูจน์ยืนยันตัวตน (personal verification) หรือการระบุตัวตน (personal identification) ด้วยลักษณะเฉพาะชีวมิติประเภทใบหน้า

2.5 การพิสูจน์ยืนยันชีวมิติ (biometric verification) หมายถึง กระบวนการในการพิสูจน์ยืนยันชีวมิติของผู้กล่าวอ้างผ่านการเปรียบเทียบชีวมิติอ้างอิง

2.6 การระบุชีวมิติ (biometric identification) หมายถึง กระบวนการค้นหาชีวมิติในฐานข้อมูลที่ลงทะเบียนไว้ก่อนโดยตอบกลับเป็นตัวระบุอัตลักษณ์อ้างอิงชีวมิติซึ่งบ่งชี้ไปถึงแต่ละบุคคล

2.7 ข้อมูลตัวอย่างชีวมิติ (biometric sample) หมายถึง ลักษณะเฉพาะชีวมิติที่แทนด้วยข้อมูลแอนะล็อกหรือดิจิทัลก่อนการสกัดลักษณะสำคัญชีวมิติ [4] เช่น ภาพใบหน้า ภาพลายนิ้วมือ ภาพม่านตา สัญญาณเสียงพูด

2.8 ข้อมูลอ้างอิงชีวมิติ (biometric reference) หมายถึง ข้อมูลตัวอย่างชีวมิติอย่างน้อยหนึ่งข้อมูล ซึ่งอาจมีมากกว่าหนึ่งก็ได้ โดยเป็นลักษณะประจำของบุคคลเจ้าของข้อมูลชีวมิติและถูกใช้เป็นตัวเปรียบเทียบชีวมิติ

2.9 อัตราการเข้าคู่ผิดพลาด (false match rate: FMR) หมายถึง อัตราความผิดพลาดที่ระบบเข้าคู่ระหว่างข้อมูลตัวอย่างชีวมิติตั้งต้นกับข้อมูลอ้างอิงชีวมิติอ้างอิงในฐานข้อมูล โดยระบบเข้าคู่บุคคลคนละคนกันและให้คะแนนความเหมือนที่มีความคล้ายกัน

2.10 อัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) หมายถึง อัตราความผิดพลาดที่ระบบไม่เข้าคู่ให้ถูกต้องระหว่างข้อมูลตัวอย่างชีวมิติตั้งต้นกับข้อมูลอ้างอิงชีวมิติอ้างอิงในฐานข้อมูล โดยระบบไม่เข้าคู่บุคคลคนเดียวกันและให้คะแนนความเหมือนที่แตกต่างกัน

2.11 การโจมตีหลอกระบบ (presentation attack) หมายถึง บุคคลนำเสนอลักษณะเฉพาะชีวมิติปลอมเพื่อหลอกระบบรู้จำชีวมิติอัตโนมัติ

2.12 การโจมตีแบบรวมภาพ (morph attack) หมายถึง บุคคลนำเสนอลักษณะเฉพาะชีวมิติที่เกิดจากการรวมภาพใบหน้าจากสองบุคคลเข้าหากันเป็นภาพเดียว เพื่อหลอกระบบรู้จำชีวมิติอัตโนมัติ

2.13 การตรวจจับการโจมตีหลอกระบบ (presentation attack detection: PAD) หมายถึง กระบวนการที่ใช้ตรวจสอบการปลอมแปลงลักษณะเฉพาะชีวมิติของบุคคลที่เข้ามาใช้งานระบบ

3. อักษรย่อ

อักษรย่อที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

อักษรย่อ	คำเต็ม	คำภาษาไทย
IdMS	Identity Management System	ระบบบริหารอัตลักษณ์บุคคล
FMR	False Match Rate	อัตราการเข้าคู่ผิดพลาด
FNMR	False Non-Match Rate	อัตราการไม่เข้าคู่ผิดพลาด

4. ข้อเสนอแนะเกี่ยวกับการใช้งานเทคโนโลยีการรู้จำใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน

รายละเอียดข้อกำหนดและข้อเสนอแนะในภาพรวมสำหรับการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตนได้ถูกกำหนดไว้ใน มาตรฐาน ขมธอ. 29 เล่ม 1-2565 [4] อย่างละเอียดแล้ว สำหรับข้อเสนอแนะมาตรฐานนี้จะเป็นการขยายรายละเอียดข้อเสนอแนะที่เกี่ยวข้องกับการรู้จำใบหน้า (face recognition) โดยตรง โดยจะใช้โครงสร้างตาม มาตรฐาน ขมธอ. 29 เล่ม 1-2565 [4] เพื่อให้สามารถใช้งานทั้งสองมาตรฐานควบคู่กันได้ โดยมีหัวข้อดังต่อไปนี้

(1) ข้อควรพิจารณาก่อนการนำเทคโนโลยีการรู้จำใบหน้าไปประยุกต์ใช้งาน

(2) ข้อควรระวังเกี่ยวกับการเก็บและการบันทึกข้อมูลภาพใบหน้า

(3) ข้อเสนอแนะการเก็บข้อมูลภาพใบหน้าสำหรับระบบรู้จำใบหน้าอัตโนมัติ

(4) มาตรฐานอุปกรณ์การเก็บภาพใบหน้า

(5) ข้อเสนอแนะการวัดคุณภาพภาพใบหน้า

(6) มาตรฐานการบันทึกข้อมูลภาพใบหน้า

(7) มาตรฐานความแม่นยำขั้นต่ำสำหรับระบบรู้จำใบหน้าอัตโนมัติ

(8) มาตรฐานการแลกเปลี่ยนข้อมูลภาพใบหน้าระหว่างหน่วยงาน

(9) ข้อเสนอแนะเกี่ยวกับการรักษาความปลอดภัยข้อมูลภาพใบหน้า

(10)ข้อเสนอแนะเกี่ยวกับสิทธิส่วนบุคคลกับข้อมูลภาพใบหน้า

โดยมีรายละเอียดของแต่ละหัวข้อดังต่อไปนี้

4.1 ข้อควรพิจารณาก่อนการนำเทคโนโลยีการรู้จำใบหน้าไปประยุกต์ใช้งาน

เทคโนโลยีการรู้จำใบหน้า เป็นเทคโนโลยีปัจจุบันซึ่งยังอยู่ในช่วงการพัฒนา และขยายสู่การประยุกต์ใช้งานในวงกว้าง โดยมีจุดเด่นดังต่อไปนี้

(1) มีความแม่นยำสูงในสภาพแวดล้อมที่ถูกควบคุม ได้ถูกพัฒนาโดยเทคโนโลยีปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง ทำให้ความแม่นยำเพิ่มขึ้นเทียบเคียงกับระบบรู้จำชีวมิติอัตโนมัติอื่นที่ใช้งานอยู่ก่อนหน้า เช่น ลายนิ้วมือ และม่านตา จนสามารถนำไปประยุกต์ใช้งานได้อย่างกว้างขวางในปัจจุบัน

(2) การเก็บข้อมูลภาพใบหน้ามีความสะดวก ใช้กล้องที่มีใช้งานกันอย่างแพร่หลายทำให้สามารถเก็บข้อมูลภาพใบหน้าได้ง่าย สามารถใช้งานร่วมกับระบบกล้องวงจรปิดเพื่อรักษาความปลอดภัยได้เป็นอย่างดี ระบบสามารถขยายขนาดได้และสามารถรองรับผู้ใช้จำนวนมากได้

(3) บุคคลทั่วไปให้การยอมรับ เมื่อเปรียบเทียบกับชีวมิติอื่น ๆ ใบหน้าจะเป็นชีวมิติที่ประชาชนทั่วไปให้การยอมรับมากที่สุด ไม่ต่อต้านและมีความสะดวกใจในการใช้งาน

(4) สามารถรู้จำใบหน้าได้ในระยะห่าง โดยมีระยะห่างระหว่างบุคคลกับอุปกรณ์กล้องหลายเมตร ปลอดภัยต่อการแพร่เชื้อเมื่อเทียบกับระบบที่ต้องมีการสัมผัสกับตัวเซนเซอร์ อย่างเช่น ลายนิ้วมือ

เมื่อพิจารณาปัญหาของเทคโนโลยีการรู้จำใบหน้า มีปัจจัยที่ทำให้ระบบรู้จำใบหน้าอัตโนมัติเกิดความผิดพลาดหรือมีความแม่นยำลดลง โดยมีข้อจำกัดดังต่อไปนี้

(1) กรรมพันธุ์ (genetic) ฝาแฝดไข่ใบเดียวกันที่มี DNA เหมือนกัน มักจะมีหน้าตาที่เหมือนกัน พี่น้องจะมีหน้าตาที่คล้ายกันเกิดจากกรรมพันธุ์ รวมทั้ง พ่อ แม่ ลูก ที่อาจมีหน้าตาที่คล้ายกันตามธรรมชาติของมนุษย์ ซึ่งจะทำให้ระบบรู้จำใบหน้าอัตโนมัติ ให้คะแนนความเหมือนที่ใกล้เคียงกัน ไม่สามารถแยกความแตกต่างของบุคคลเหล่านี้อย่างชัดเจนได้

(2) ช่วงอายุ (age) โดยใบหน้าจะมีการเปลี่ยนแปลงไปตามอายุ ตั้งแต่แรกเกิด ทารก เด็ก วัยรุ่น ผู้ใหญ่ และคนชรา ซึ่งระบบรู้จำใบหน้าอัตโนมัติโดยทั่วไปไม่สามารถรองรับการเปลี่ยนแปลงเหล่านี้ ระยะห่างระหว่างเวลาการเก็บภาพใบหน้าที่ลงทะเบียนในระบบและภาพใบหน้าในเวลาปัจจุบันเป็นปัจจัยสำคัญมาก ระบบรู้จำใบหน้าอัตโนมัติจะให้ผลคะแนนความเหมือนที่ต่ำลง เมื่อระยะเวลาห่างกันมากขึ้น งานวิจัย [5] แนะนำว่าควรลงทะเบียนใบหน้าซ้ำไม่ควรมีระยะเวลาห่างกันเกิน 6 ปี

(3) การแสดงอารมณ์บนใบหน้า (facial expression) ตามธรรมชาติของมนุษย์ ใบหน้าจะเปลี่ยนแปลงไปตามอารมณ์และมีผลต่อความแม่นยำของระบบรู้จำใบหน้าอัตโนมัติ ทั้งนี้ ขึ้นอยู่กับอัลกอริทึมในการวิเคราะห์รูปใบหน้าของระบบรู้จำใบหน้าอัตโนมัติที่เลือกใช้

(4) สุขภาพ (health) สุขภาพของแต่ละบุคคล ความเจ็บป่วยด้วยโรคต่าง ๆ อาจทำให้ใบหน้ามีการเปลี่ยนแปลงไป ทำให้ระบบรู้จำใบหน้าอัตโนมัติมีประสิทธิภาพที่ต่ำลง

(5) รูปพรรณสัณฐาน (appearance) เช่น การไว้หนวดเครา การแต่งหน้า เขียนคิ้ว ตัดผม ดัดผม หรือทรงผมที่แตกต่าง จะทำให้ระบบรู้จำใบหน้าอัตโนมัติมีปัญหาทำงานผิดพลาดได้

(6) การมีสิ่งปกปิดใบหน้า (occlusion) เช่น การใส่แว่น การใส่หน้ากากอนามัยในยุคการแพร่ระบาดของ COVID-19 การปกปิดใบหน้าในทางศาสนา ทำให้ประสิทธิภาพของระบบรู้จำใบหน้าอัตโนมัติต่ำลง

(7) การทำศัลยกรรม (surgery) ที่เปลี่ยนแปลงโครงสร้างใบหน้า เป็นปัญหาใหญ่ของระบบรู้จำใบหน้าอัตโนมัติ ซึ่งระบบอาจจะไม่สามารถรู้จำใบหน้าหลังการทำศัลยกรรมได้

(8) ทิศทางการวางหน้า (facial pose) ระบบรู้จำใบหน้าอัตโนมัติโดยปกติต้องการภาพถ่ายใบหน้าตรง ถ้ามีหน้าเฉียงเข้ามาระบบรู้จำใบหน้าอัตโนมัติอาจมีปัญหาได้ ซึ่งการลงทะเบียนโดยการให้วางหน้าในหลายมุมเพื่อให้ระบบวิเคราะห์เพิ่มเติม ตัวอย่างเช่น มุมเฉียง มุมก้ม และมุมเงย หรือการเก็บภาพในรูปแบบวีดิทัศน์ที่ถ่ายใบหน้าในทิศทางที่แตกต่างกันไปจะช่วยแก้ปัญหานี้ได้

(9) แสงที่ใช้ (illumination) โดยปกติใบหน้าจะมีการเปลี่ยนแปลงไปตามทิศทางที่แสงเข้ามากระทบและเงาที่เกิดขึ้น ซึ่งมีผลต่อระบบรู้จำใบหน้าอัตโนมัติ ทั้งนี้การถ่ายภาพใบหน้าโดยใช้แสงอินฟราเรดย่านใกล้ (near infrared) จะช่วยลดผลกระทบของแสงธรรมชาติที่เข้ามาในทิศทางต่าง ๆ ให้หายไปรวมทั้งเงาที่เกิดขึ้นด้วย ซึ่งการใช้แสงอินฟราเรดย่านใกล้สามารถทำให้แสงทั่วถึงเสมอกันบนใบหน้า จึงเป็นสาเหตุที่ทำให้หลายหน่วยงานต้องมีอุปกรณ์ถ่ายภาพเสริมสำหรับใช้แสงอินฟราเรดย่านใกล้เข้ามาช่วยระบบรู้จำใบหน้าอัตโนมัติ

(10)การถ่ายภาพ (photography) ปัญหาจากการถ่ายภาพที่อาจทำให้ระบบรู้จำใบหน้าผิดพลาด อาทิ การใช้เลนส์ที่มีระยะโฟกัสสั้น เช่น เลนส์มุมกว้าง จะทำให้ภาพมีความผิดเพี้ยนที่เกิดจากเลนส์ (lens

distortion) นอกจากนี้ขึ้นอยู่กับปัจจัยอื่น ๆ ที่มีผลต่อคุณภาพของภาพใบหน้า อาทิ ความละเอียดของภาพ (resolution) ความคมชัดของภาพ (contrast) การถ่ายภาพใบหน้าในที่มืดเกินไปหรือสว่างเกินไป (over/under Exposure) การบีบอัดภาพ (compression) การถ่ายภาพที่ไม่โฟกัสหรือภาพเบลอ (mis-focus or blur) หรือระยะห่างจากกล้องถึงใบหน้าไกลเกินไปทำให้มีรายละเอียดน้อย เป็นต้น

4.2 ข้อควรระวังเกี่ยวกับการเก็บและการบันทึกข้อมูลภาพใบหน้า

ข้อมูลภาพใบหน้า ถือเป็นข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล [15] ผู้ให้บริการต้องขอความยินยอมจากผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูลอย่างชัดเจน โดยต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมและการใช้งานข้อมูลภาพใบหน้าให้เข้าใจได้โดยง่าย หากได้รับความยินยอมแล้วผู้ให้บริการต้องจัดเก็บภาพใบหน้าต้นฉบับภายใต้มาตรการรักษาความปลอดภัยในการเก็บข้อมูลชีวมิติอย่างเคร่งครัด ห้ามมิให้เกิดการรั่วไหลของข้อมูลและละเมิดการใช้งานซึ่งอยู่นอกเหนือจากความยินยอมตามที่ได้แจ้งต่อผู้ใช้บริการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล [15]

การเก็บข้อมูลภาพใบหน้า ผู้ให้บริการอาจนำไปใช้ในกรณีต่าง ๆ ตามวัตถุประสงค์ 7 ข้อ ดังต่อไปนี้ หรืออาจมีการนำไปใช้ตามความจำเป็นอื่นที่ไม่ได้กำหนดไว้ในข้อเสนอแนะมาตรฐานนี้ โดยต้องระบุวัตถุประสงค์อื่น ๆ ไว้ให้เจ้าของข้อมูลรับทราบและให้ความยินยอม

(1) **การพิสูจน์ยืนยันชีวมิติด้วยใบหน้า** ในกรณีที่ผู้ให้บริการต้องพิสูจน์ยืนยันชีวมิติด้วยใบหน้าของผู้ใช้บริการหรือผู้กล่าวอ้างเป็นเจ้าของอัตลักษณ์ โดยเปรียบเทียบข้อมูลภาพใบหน้าของผู้ใช้บริการหรือผู้กล่าวอ้าง กับข้อมูลอ้างอิงภาพใบหน้าเชื่อมโยงกับข้อมูลในหลักฐานแสดงตน (เช่น เลขประจำตัวประชาชน) ซึ่งได้ลงทะเบียนเก็บไว้ก่อนล่วงหน้าในฐานข้อมูลของ IdMS

(2) **การระบุชีวมิติด้วยใบหน้า** ในกรณีที่ผู้ให้บริการต้องการค้นหาระบุตัวบุคคลด้วยใบหน้าของผู้ใช้บริการที่มีข้อมูลภาพใบหน้าอยู่ในฐานข้อมูล IdMS

(3) **การแก้ปัญหาในกรณีที่ระบบรู้จำใบหน้าอัตโนมัติทำงานผิดพลาด** ในกรณีที่ผู้ใช้บริการร้องเรียนว่าถูกปฏิเสธการยืนยันตัวตนโดยระบบรู้จำใบหน้าอัตโนมัติ แต่ผู้ใช้บริการยืนยันว่าเป็นเจ้าของใบหน้าตัวจริง ผู้ให้บริการจึงต้องมีการพิสูจน์และยืนยันตัวตนด้วยเจ้าหน้าที่ โดยเจ้าหน้าที่ผู้ซึ่งมีความเชี่ยวชาญจะเปรียบเทียบข้อมูลอ้างอิงภาพใบหน้ากับข้อมูลภาพใบหน้าที่ได้จากผู้ใช้บริการในขณะนั้น เพื่อตัดสินใจว่าใช่คน ๆ เดียวกันหรือไม่ใช่

(4) **การป้องกันปัญหาข้อมูลภาพใบหน้ามีการเปลี่ยนแปลง** ข้อมูลภาพใบหน้ามีการเปลี่ยนแปลงได้ตลอดตามช่วงอายุ รวมไปถึงการเกิดอุบัติเหตุหรือการจงใจทำศัลยกรรมที่เปลี่ยนแปลงโครงสร้างใบหน้า ผู้ให้บริการจึงมีความจำเป็นต้องเก็บและบันทึกข้อมูลภาพใบหน้าไว้เป็นหลักฐานตามความจำเป็นที่ผู้ใช้บริการเข้าใช้งานระบบรู้จำใบหน้าอัตโนมัติ โดยเก็บและบันทึกข้อมูลภาพใบหน้าในแต่ละช่วงเวลาในรูปแบบระเบียนที่สามารถทำการตรวจสอบย้อนหลังได้ นอกจากนี้ การเก็บและบันทึกข้อมูลภาพใบหน้าในลักษณะนี้สามารถป้องกันการถูกสวมตัวกันในอนาคต ในกรณีที่เจ้าหน้าที่ร่วมมือกับอาชญากรในการสวมตัวผู้ใช้บริการโดยการลงทะเบียนทับข้อมูลภาพใบหน้าเดิม

(5) **การแลกเปลี่ยนข้อมูลภาพใบหน้าระหว่างหน่วยงาน** ในกรณีที่ผู้ให้บริการมีความจำเป็นต้องแลกเปลี่ยนข้อมูลภาพใบหน้าระหว่างหน่วยงานที่ทำงานเกี่ยวข้องประสานความร่วมมือกัน เนื่องจากแต่ละหน่วยงานอาจใช้งานผลิตภัณฑ์ระบบรู้จำใบหน้าอัตโนมัติที่ต่างกัน การแลกเปลี่ยนข้ามระบบที่แตกต่างกัน

จำเป็นต้องแลกเปลี่ยนด้วยข้อมูลภาพใบหน้า โดยเฉพาะในงานทางด้านนิติวิทยาศาสตร์ซึ่งมีความจำเป็นต้องพิจารณาข้อมูลภาพใบหน้าเป็นหลักในการทำงาน

(6) **การปรับปรุงพัฒนาและทดสอบสมรรถนะของระบบ** ในกรณีที่ผู้ให้บริการต้องการปรับปรุงบริการของระบบรู้จำใบหน้าอัตโนมัติให้สามารถทำงานได้เต็มประสิทธิภาพสอดคล้องตามข้อกำหนดการใช้งานของแต่ละภาคอุตสาหกรรมได้อย่างสม่ำเสมอ ผู้ให้บริการจำเป็นต้องเก็บและบันทึกข้อมูลภาพใบหน้าสำหรับทดสอบสมรรถนะของระบบ เพื่อพัฒนาปรับปรุงงานบริการที่ใช้ระบบรู้จำใบหน้าอัตโนมัติให้มีประสิทธิภาพสูงสุด

(7) **การแก้ปัญหาในกรณีที่ต้องเริ่มระบบรู้จำใบหน้าอัตโนมัติใหม่ทั้งหมด** ในกรณีที่ผู้ให้บริการต้องเปลี่ยนซอฟต์แวร์ของระบบรู้จำใบหน้าอัตโนมัติจากบริษัทผู้ผลิตเดิมที่มีการใช้งานอยู่ หรือการเปลี่ยนผู้รับจ้างดูแลระบบในกรณีที่ผู้รับจ้างเดิมหมดสัญญาหรือไม่สามารถทำงานต่อไปได้ การเก็บข้อมูลภาพใบหน้าต้นฉบับที่เป็นไปตามมาตรฐานจะทำให้สามารถกู้ฐานข้อมูลภาพใบหน้าตั้งต้นและสร้างระบบรู้จำใบหน้าอัตโนมัติขึ้นมาใหม่ทั้งหมดได้ และสามารถใช้งานต่อไปได้อย่างต่อเนื่องโดยไม่ต้องสูญเสียข้อมูลภาพใบหน้าเดิม

ข้อแนะนำเพิ่มเติม ในกรณีการใช้งานตามข้อที่ (1) เพียงอย่างเดียว อาจไม่จำเป็นต้องบันทึกข้อมูลภาพใบหน้าเก็บไว้ในฐานข้อมูลและไม่จำเป็นที่จะต้องแสดงข้อมูลภาพใบหน้าในจอภาพ ในกรณีการใช้งานข้อ (2) อาจมีความจำเป็นที่จะต้องใช้ข้อมูลภาพใบหน้ามาแสดงในจอภาพเพื่อเปรียบเทียบกับข้อมูลอ้างอิงภาพใบหน้าประกอบกับการพิจารณาของเจ้าหน้าที่ เพื่อให้สามารถทำงานระบุตัวตน ให้สำเร็จลุล่วงไปได้ด้วยดี สำหรับในกรณีการใช้งานตั้งแต่ข้อ (2), (3), (4), (5), (6), (7) อาจมีความจำเป็นต้องบันทึกข้อมูลอ้างอิงภาพใบหน้าสำหรับการใช้ในงานต่าง ๆ ดังกล่าว และในกรณี (3), (4), (5), (6), (7) อาจต้องบันทึกข้อมูลภาพใบหน้าที่ได้จากผู้ใช้บริการในขณะนั้นด้วย ดังนั้นผู้ให้บริการต้องขอความยินยอมจากเจ้าของข้อมูลชีวมิติโดยให้แจ้งวัตถุประสงค์ของการเก็บรวบรวมและการใช้งานข้อมูลภาพใบหน้าอย่างชัดเจน

หมายเหตุ: เมื่อผู้ใช้บริการยกเลิกการใช้บริการ หรือขอถอนความยินยอมในการเก็บรวบรวม ใช้ข้อมูลชีวมิติ ผู้ให้บริการจะต้องดำเนินการลบหรือทำลายข้อมูลอัตลักษณ์บุคคลทั้งหมด หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล [15]

4.3 ข้อเสนอแนะการเก็บข้อมูลภาพใบหน้าสำหรับระบบรู้จำใบหน้าอัตโนมัติ

กระบวนการเก็บข้อมูลภาพใบหน้า ควรพิจารณาข้อเสนอแนะสำหรับกระบวนการเก็บข้อมูลชีวมิติตามมาตรฐาน ขมธอ. 29 เล่ม 1-2565 [4] โดยข้อเสนอแนะที่จำเป็นสำหรับการเก็บข้อมูลภาพใบหน้า ได้มีการกำหนดเพิ่มเติมดังต่อไปนี้

(1) การเก็บข้อมูลภาพใบหน้าในการลงทะเบียน ผู้ให้บริการควรเก็บภาพถ่ายใบหน้าสด (live captured image) เพื่อเป็นการคัดกรองคุณภาพโดยเจ้าหน้าที่เก็บข้อมูล

(2) การเก็บข้อมูลภาพใบหน้าในสภาพแวดล้อมที่ถูกควบคุม เพื่อให้การถ่ายภาพใบหน้ามีคุณภาพดีที่สุด ผู้ให้บริการควรให้การอำนวยความสะดวกแก่ผู้ใช้บริการ ตลอดจนควบคุมและจัดสภาพแวดล้อมให้มีความปลอดภัย มีแสงสว่างเหมาะสมและเพียงพอ และมีการควบคุมแสงรบกวนรอบพื้นที่การรับภาพ รวมทั้งควรจัดเตรียมจำนวนอุปกรณ์ถ่ายภาพที่พร้อมใช้งานให้มีความเหมาะสมกับจำนวนผู้รับบริการ

(3) การเก็บข้อมูลภาพใบหน้าในสภาพแวดล้อมที่ไม่ถูกควบคุม ในกรณีที่ไม่สามารถควบคุมสภาพแวดล้อมได้หรือการเก็บภาพใบหน้าโดยผู้ใช้เอง อาทิ การถ่ายภาพใบหน้าผ่านอุปกรณ์สมาร์ทโฟนหรือคอมพิวเตอร์และส่งภาพใบหน้าผ่านทางอินเตอร์เน็ต ผู้ให้บริการควรให้คำแนะนำหรือมีโปรแกรมแอพพลิเคชันช่วยแนะนำในการถ่ายให้ได้ภาพใบหน้าที่มีคุณภาพดีที่สุด ควรมีการตอบสนองและให้คำแนะนำผู้ใช้ทันทีเพื่อให้ผู้ใช้สามารถปรับปรุงภาพใบหน้าของตนให้มีคุณภาพเพียงพอที่จะใช้งานระบบรู้จำใบหน้าอัตโนมัติได้อย่างถูกต้องแม่นยำ

(4) การแสดงอารมณ์ทางใบหน้าของผู้ใช้ ผู้ให้บริการควรเก็บข้อมูลภาพใบหน้าในสภาพที่ไม่แสดงอารมณ์ ควรควบคุมปัจจัยที่สามารถส่งผลกระทบต่ออารมณ์ของมนุษย์ที่ทำให้ใบหน้าเปลี่ยนแปลงไป เช่น เกิดอารมณ์ที่แสดงออกทางสีหน้า เกิดความอ่อนล้าที่ไม่อยากให้ความร่วมมือในการถ่ายภาพใบหน้า โดยสภาพใบหน้าที่เปลี่ยนไปจากท่าทางปกติ (neutral) เหล่านี้สามารถส่งผลถึงประสิทธิภาพและความแม่นยำของระบบรู้จำใบหน้าอัตโนมัติได้

(5) การระบุตัวตนก่อนเก็บข้อมูลภาพใบหน้า ผู้ให้บริการต้องป้องกันการปลอมแปลงตัวบุคคลและความซ้ำซ้อนที่อาจเกิดขึ้นของอัตลักษณ์อ้างอิงในหลักฐานแสดงตน ตัวอย่างเช่น หากหน่วยงานใช้การตรวจสอบระหว่างภาพถ่ายใบหน้าสดกับภาพพิมพ์ใบหน้า (printed image) ที่ปรากฏในเอกสารสำคัญหรือบัตรประจำตัว หน่วยงานต้องตรวจสอบภาพถ่ายใบหน้าสดกับแหล่งข้อมูลที่น่าเชื่อถืออื่นร่วมด้วย เนื่องจากเทคนิคการโจมตีแบบรวมภาพ (morph attack) โดยนำภาพใบหน้าของบุคคลสองคนรวมเข้าด้วยกัน สามารถหลอกระบบรู้จำใบหน้าอัตโนมัติให้เกิดความผิดพลาดในการยืนยันตัวตนโดยสามารถใช้ผ่านระบบได้ทั้งสองบุคคล

(6) การฝึกอบรมเจ้าหน้าที่เก็บข้อมูลภาพใบหน้า ผู้ให้บริการต้องมีการจัดอบรมเจ้าหน้าที่ก่อนทุกครั้งหากเจ้าหน้าที่มีการปฏิบัติงานในกระบวนการที่เกี่ยวข้องกับระบบรู้จำใบหน้าอัตโนมัติ เช่น เจ้าหน้าที่ถ่ายภาพใบหน้าในกระบวนการลงทะเบียนข้อมูลชีวมิติด้วยใบหน้า และตรวจสอบคุณภาพของภาพใบหน้าก่อนนำเข้าระบบ เจ้าหน้าที่ตรวจสอบใบหน้าในกระบวนการพิสูจน์และยืนยันตัวตนด้วยใบหน้า ทั้งนี้ เพื่อให้การใช้งานระบบรู้จำใบหน้าอัตโนมัติเกิดประสิทธิภาพสูงสุด และป้องกันการนำภาพถ่ายใบหน้าคุณภาพต่ำเข้าสู่ระบบรู้จำใบหน้าอัตโนมัติอย่างรู้เท่าไม่ถึงการณ์ได้

หมายเหตุ : การฝึกอบรมควรมีการกล่าวถึง วิธีถ่ายภาพใบหน้าในการลงทะเบียนตามมาตรฐานที่กำหนด การสังเกตการปลอมแปลงใบหน้าก่อนเข้าสู่ระบบรู้จำใบหน้าอัตโนมัติ รวมไปถึงการปฏิสัมพันธ์กับผู้รับบริการนกรณีต่าง ๆ อาทิ หากเกิดความล้มเหลวในการเก็บข้อมูลระหว่างการลงทะเบียน จะมีกระบวนการแก้ไขปัญหาอย่างไร

(7) ความถี่ในการเก็บข้อมูลภาพใบหน้า ผู้ให้บริการควรมีการพิจารณาระยะเวลาในการเก็บข้อมูลซ้ำโดยเฉพาะชีวมิติประเภทใบหน้าที่มีการเปลี่ยนแปลงเร็วกว่าชีวมิติประเภทอื่น หน่วยงานไม่ควรประวิงระยะเวลาเพื่อติดต่อผู้รับบริการให้เข้ามาลงทะเบียนภาพใบหน้าซ้ำ หรือใช้โอกาสที่ผู้รับบริการเข้ามาติดต่อทำธุรกรรมและให้ทำการลงทะเบียนซ้ำเพื่อให้ภาพใบหน้าอ้างอิงของผู้รับบริการในฐานข้อมูลทันสมัยอยู่เสมอ โดยภาพใบหน้าต้องมีการใช้วงรอบการลงทะเบียนซ้ำสูงสุดไม่เกิน 6 ปี [5] โดยระยะเวลาที่เหมาะสมควรลงทะเบียนซ้ำทุก 2 ปี เพื่อลดอัตราผิดพลาดที่เพิ่มขึ้นตามระยะเวลาให้น้อยที่สุด เนื่องจากใบหน้ามีการเปลี่ยนแปลงตามกาลเวลามากกว่าชีวมิติประเภทอื่น

(8) ข้อจำกัดเกี่ยวกับอายุในการเก็บข้อมูลภาพใบหน้า ผู้ให้บริการไม่ควรใช้ระบบรู้จำใบหน้ากับเด็กตั้งแต่แรกเกิดจนถึง 5 ขวบเนื่องจากมีใบหน้าที่ไม่เสถียร ใบหน้าจะเสถียรเมื่อเด็กมีอายุมากกว่า 13 ปี [6] ผู้ให้บริการควรออกนโยบายเพิ่มเติมสำหรับจำกัดการใช้งานกับเด็กที่มีอายุตั้งแต่ 5 ปี ถึง 13 ปี ในการพิสูจน์และยืนยันตัวตนด้วยใบหน้า เช่น การลงทะเบียนภาพใบหน้าซ้ำที่มีระยะเวลากระชั้นขึ้น โดยกำหนดวงรอบการลงทะเบียนซ้ำไม่เกิน 6 เดือน เนื่องจากอายุในช่วงนี้เป็นช่วงของการเจริญเติบโตของร่างกาย ซึ่งใบหน้าอาจจะมีการเปลี่ยนแปลงได้เร็ว

4.4 มาตรฐานอุปกรณ์การเก็บภาพใบหน้า

ข้อเสนอแนะสำหรับมาตรฐานอุปกรณ์การเก็บภาพใบหน้า หรือ กล้องถ่ายภาพใบหน้า สำหรับระบบรู้จำใบหน้าอัตโนมัติ มีไว้เพื่อเป็นแนวทางเพื่อให้หน่วยงานผู้ให้บริการได้ใช้อ้างอิง โดยไม่ได้กำหนดคุณสมบัติของอุปกรณ์โดยเฉพาะเจาะจง แต่เป็นคุณสมบัติพื้นฐานที่อุปกรณ์การเก็บภาพใบหน้าพึงมี เพื่อให้ได้มาตรฐานของภาพใบหน้าที่มีคุณภาพดี โดยมีรายละเอียดดังต่อไปนี้

(1) ชนิดของภาพ อุปกรณ์การเก็บภาพใบหน้าต้องสามารถรับภาพสีได้

หมายเหตุ : หน่วยงานต้องเลือกใช้ภาพสีสำหรับการลงทะเบียนและการใช้งานในระบบรู้จำใบหน้าอัตโนมัติ อย่างไรก็ตาม หน่วยงานอาจใช้ภาพระดับเทา (grey-scale image) หรือการรับภาพด้วยแสงอินฟราเรดย่านใกล้ (near infrared) เพื่อใช้งานในระบบรู้จำใบหน้าอัตโนมัติได้

(2) ขนาดภาพ อุปกรณ์การเก็บภาพใบหน้าควรมีขนาดภาพ ในโหมดแนวตั้ง (portrait) ขั้นต่ำ 600 x 800 pixels โดยอ้างอิงจากการใช้งานของ EU [7] แต่อย่างไรก็ตาม หากมีข้อกำหนดเฉพาะของภาคอุตสาหกรรมให้ยึดตามแนวทางการใช้ชีวมิติของภาคอุตสาหกรรมนั้น อาทิ ผู้ให้บริการทางการเงินที่อยู่ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย ให้ยึดแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (biometric technology) ในการให้บริการทางการเงิน ซึ่งขนาดภาพจะถูกกำหนดอยู่ในมาตรฐานขั้นต่ำสำหรับการรวบรวมข้อมูลภาพใบหน้าเพื่อใช้กับเทคโนโลยีชีวมิติโดยต้องมีความละเอียดของภาพไม่น้อยกว่า 1280 x 720 pixels หรือ 1080 x 1080 pixels [8]

(3) ขนาดใบหน้าที่ปรากฏบนภาพ อุปกรณ์การเก็บภาพใบหน้าควรสามารถรับภาพใบหน้าตรง (frontal face image) โดยให้มีขนาดของระยะห่างระหว่างจุดศูนย์กลางของดวงตาทั้งสองข้าง ไม่น้อยกว่า 120 pixels และยังคงมีความชัดเจนของใบหน้าภายในภาพ รวมทั้งมีโฟกัสอยู่บนใบหน้า

(4) การบีบอัดข้อมูลภาพ อุปกรณ์การเก็บภาพใบหน้าอาจใช้การบีบอัดข้อมูลภาพเพื่อประโยชน์ในการจัดเก็บข้อมูล โดยหากมีการบีบอัดข้อมูลควรกำหนดอัตราการบีบอัด (compression ratio) ให้มีค่าต่ำสุด หรือกล่าวอีกนัยหนึ่งคือควรกำหนดค่าคุณภาพการบีบอัด (quality) ให้มีค่าสูงสุด ซึ่งผู้ให้บริการต้องตรวจสอบภาพใบหน้าหลังจากมีการบีบอัดข้อมูลให้มั่นใจว่ามีคุณภาพเพียงพอต่อการใช้งานในระบบรู้จำใบหน้าอัตโนมัติ

4.5 ข้อเสนอแนะการวัดคุณภาพภาพใบหน้า

เนื่องจากคุณภาพของภาพใบหน้าเป็นตัวกำหนดความแม่นยำของระบบรู้จำใบหน้าอัตโนมัติ การวัดคุณภาพของภาพถ่ายใบหน้าเป็นสิ่งที่จำเป็นต้องทำเพื่อคัดภาพใบหน้าที่มีคุณภาพที่ไม่ดีให้ถ่ายใหม่ และเก็บแต่ภาพใบหน้าที่มีคุณภาพดี การวัดคุณภาพข้อมูลภาพใบหน้าให้ใช้แนวทางตาม ISO/IEC TR 29794-5:2010

[9] โดยมาตรฐานนี้กำลังอยู่ในช่วงปรับปรุงและกำลังจะเปลี่ยนเป็นมาตรฐาน ISO/IEC 29794-5 ฉบับปรับปรุงใหม่ที่มีรายละเอียดมากกว่าเดิม

วัตถุประสงค์ที่สำคัญของการทำตามมาตรฐานการวัดคุณภาพของภาพใบหน้า คือ การรักษาประสิทธิภาพของระบบรู้จำใบหน้าให้มีความแม่นยำและน่าเชื่อถือได้ ซึ่งการวัดคุณภาพภาพใบหน้า ควรทำในทุกกระบวนการ ได้แก่ การลงทะเบียน การยืนยันตัวตน การระบุตัวตน โดยรายละเอียดข้อเสนอแนะที่เพิ่มเติมมีดังต่อไปนี้

(1) ความจำเป็นในการวัดคุณภาพ ผู้ให้บริการควรมีการวัดคุณภาพข้อมูลภาพใบหน้า ในระบบรู้จำใบหน้าอัตโนมัติอย่างสม่ำเสมอหากต้องการรักษาประสิทธิภาพของระบบรู้จำใบหน้าอัตโนมัติให้มีความแม่นยำสูงสุด ในกรณีที่ข้อมูลภาพใบหน้าไม่ผ่านการวัดคุณภาพ ไม่ควรนำภาพใบหน้าที่มีคุณภาพต่ำเข้ามาลงทะเบียนในระบบรู้จำใบหน้าอัตโนมัติ

หมายเหตุ: ปัจจุบัน อัลกอริทึมการวัดคุณภาพภาพใบหน้ายังไม่มีมาตรฐานที่ชัดเจน โดยแต่ละอัลกอริทึมมีข้อดีข้อเสียที่แตกต่างกัน ซึ่งยังไม่มีอัลกอริทึมใดให้ประสิทธิภาพที่ดีเพียงพอในการวัดคุณภาพของภาพใบหน้าครบทุกรูปแบบ

(2) ผลการวัดคุณภาพ อัลกอริทึมการวัดคุณภาพที่เลือกใช้ควรให้ผลลัพธ์เป็นค่าคะแนนซึ่งมีค่าอยู่ระหว่าง 0 ถึง 100 และบันทึกค่าคะแนนตามรูปแบบของโครงสร้างระเบียนข้อมูลคุณภาพ (quality data record structure) ซึ่งอธิบายในมาตรฐาน ISO/IEC 29794-1:2016 [10] เพื่อใช้บันทึกข้อมูลชีวมิติตามมาตรฐาน ISO/IEC 39794-1:2019 [11]

(3) การกำหนดค่าเทรชโฮลด์ (threshold) ซึ่งเป็นค่าคะแนนความเชื่อมั่นที่ยอมรับได้ เพื่อใช้เป็นเกณฑ์ยอมรับภาพใบหน้าเข้าสู่ระบบรู้จำใบหน้าอัตโนมัติ ผู้ให้บริการต้องเลือกค่าเทรชโฮลด์ที่เหมาะสมในการกำหนดเกณฑ์คุณภาพของภาพใบหน้าว่าผ่านหรือไม่ผ่าน โดยที่ยังคงรักษาค่าประสิทธิภาพ FMR และ FNMR ให้เป็นไปตามแนวทางการใช้งานชีวมิติของแต่ละภาคอุตสาหกรรม อาทิ แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงินของธนาคารแห่งประเทศไทย

(4) ข้อควรระวังเกี่ยวกับการประยุกต์ใช้การวัดคุณภาพ ผู้ให้บริการควรกำหนดขั้นตอนเพิ่มเติมหากคะแนนคุณภาพของผู้ใช้บริการ ไม่เป็นไปตามเกณฑ์ค่าเทรชโฮลด์ที่กำหนด ซึ่งหน่วยงานควรดำเนินการพิสูจน์และยืนยันตัวตนด้วยวิธีอื่น เช่น คุณภาพภาพใบหน้ามีค่าต่ำในกรณีที่เกิดจากใบหน้าเสียโฉม หรือ กรณีที่ผู้พิการไม่สามารถแสดงตนหน้ากล้องเพื่อถ่ายภาพใบหน้าได้สมบูรณ์

4.6 มาตรฐานการบันทึกข้อมูลภาพใบหน้า

การบันทึกข้อมูลภาพใบหน้าต้องบันทึกข้อมูลชีวมิติในรูปแบบตามมาตรฐาน ISO/IEC 39794-1:2019 [11] และมีมาตรฐานเฉพาะสำหรับการบันทึกข้อมูลภาพใบหน้าอ้างอิงตามมาตรฐาน ISO/IEC 39794-5:2019 [12] โดยรายละเอียดข้อเสนอแนะที่เพิ่มเติมจากมาตรฐานทั้งสอง มีดังต่อไปนี้

(1) **ก่อนการบันทึกข้อมูลภาพใบหน้า** ผู้ให้บริการต้องมีการวัดคุณภาพภาพใบหน้าก่อนเพื่อให้มั่นใจว่าข้อมูลที่บันทึกมีคุณภาพดี ภาพใบหน้าที่รับเข้ามาต้องได้รับการประเมินคุณภาพชีวมิติตามมาตรฐาน ISO/IEC 29794-1:2016 [10] และมีมาตรฐานเฉพาะสำหรับการประเมินคุณภาพชีวมิติประเภทใบหน้าอ้างอิงตามมาตรฐาน ISO/IEC TR 29794-5:2010 [9] หรือมาตรฐาน ISO/IEC 29794-5 ฉบับปรับปรุงที่กำลังจะออกมาใหม่

(2) **การบันทึกแยกประเภทภาพใบหน้าในฐานข้อมูลที่แตกต่างกัน** หากหน่วยงานมีการบันทึกภาพใบหน้าประเภทไม่มีข้อจำกัด (unconstrainted face image) นอกเหนือจากภาพใบหน้าตรง (frontal face image) ผู้ให้บริการต้องแยกฐานข้อมูลออกจากกัน โดยแยกเป็นฐานข้อมูลภาพใบหน้าตรง และฐานข้อมูลภาพใบหน้าประเภทไม่มีข้อจำกัด เช่น ภาพใบหน้าจากการถ่ายภาพตนเองผ่านสมาร์ทโฟน ภาพใบหน้าจากกล้องถ่ายภาพโดยใช้แสงอินฟราเรดย่านใกล้ ภาพใบหน้าสามมิติ ทั้งนี้ เนื่องจากอัลกอริทึมการเปรียบเทียบภาพใบหน้าในระบบรู้จำใบหน้าอัตโนมัติจะให้ผลความแม่นยำที่ลดลงในกรณีที่รูปแบบข้อมูลภาพนำเข้าไม่ตรงกับรูปแบบที่ใช้อยู่ในระบบ

4.7 มาตรฐานความแม่นยำขั้นต่ำสำหรับระบบรู้จำใบหน้าอัตโนมัติ

ในการเลือกใช้ระบบรู้จำใบหน้าอัตโนมัติ สมรรถนะของระบบเป็นหนึ่งในเรื่องที่ต้องให้ความสำคัญ เพราะมีผลกระทบต่อผู้ใช้งานอย่างมีนัยสำคัญ เนื่องจากเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว การกำหนดมาตรฐานความแม่นยำขั้นต่ำของระบบรู้จำใบหน้าอัตโนมัติ ควรอ้างอิงกับการทดสอบสมรรถนะของเทคโนโลยีการรู้จำใบหน้าอัตโนมัติในขณะนั้นเป็นสำคัญ ข้อเสนอแนะมาตรฐานนี้จะกำหนดความแม่นยำขั้นต่ำอ้างอิงกับหน่วยงานที่ทดสอบระบบรู้จำใบหน้าอัตโนมัติที่มีความน่าเชื่อถือ โดยแบ่งแยกออกเป็นสองประเด็น คือในกรณีที่ไม่มีฐานข้อมูลการทดสอบภาพใบหน้าโดยเฉพาะของผู้ใช้หลัก และในกรณีที่มีฐานข้อมูลการทดสอบภาพใบหน้าของผู้ใช้หลัก โดยข้อเสนอแนะมีดังต่อไปนี้

(1) **ในกรณีที่ยังไม่มีฐานข้อมูลการทดสอบภาพใบหน้าโดยเฉพาะของผู้ใช้หลัก** การกำหนดค่าความแม่นยำในการเปรียบเทียบภาพใบหน้าของระบบรู้จำใบหน้าอัตโนมัติ ต้องอ้างอิงกับผลการทดสอบสมรรถนะระบบซึ่งผ่านการทดสอบโดยสถาบันที่น่าเชื่อถืออย่างเช่น NIST โดยเลือกผลการวัดสมรรถนะระบบที่ใช้ฐานข้อมูลภาพใบหน้าที่ใกล้เคียงกับการนำไปใช้งานจริงตามที่ผู้ให้บริการต้องการใช้งาน เช่น ภาพใบหน้าสำหรับการตรวจลงตรา (visa) ภาพใบหน้าสำหรับทำประวัติ (mugshot) ภาพใบหน้าขณะเข้าด่านตรวจคนเข้าเมือง (visa border) ภาพใบหน้าไม่ควบคุมสภาพแวดล้อม (wild) และภาพใบหน้าหน้าตู้อัตโนมัติ (kiosk) โดยการใช้งานแบบพิสูจน์ยืนยันชีวมิติ (biometric verification 1:1) ให้อ้างอิงจาก https://pages.nist.gov/frvt/html/frvt11.html และการใช้งานแบบระบุชีวมิติ (biometric identification 1:many) ให้อ้างอิงจาก https://pages.nist.gov/frvt/html/frvt1N.html สำหรับการกำหนดมาตรฐานความแม่นยำขั้นต่ำของระบบรู้จำใบหน้าอัตโนมัติ แบ่งแยกเป็นสองกรณีดังต่อไปนี้

(1.1) กรณีที่ผู้ให้บริการที่มีจำนวนผู้ใช้งานเกิน 10,000,000 คน (สิบล้านคน) และมีระดับความเสี่ยงที่อาจก่อให้เกิดผลกระทบต่อผู้ใช้งานในระดับสูงโดยใช้หลักการประเมินระดับผลกระทบตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ [16] ควรเลือกใช้ระบบรู้จำใบหน้าอัตโนมัติที่มีความแม่นยำสูงเพื่อลดผลกระทบและความเสี่ยงของคนหมู่มากกับความผิดพลาดที่จะเกิดขึ้นจากระบบอัตโนมัติ โดยกำหนดให้นำผลการทดสอบสมรรถนะจาก NIST ที่ได้จากการทดสอบกับฐานข้อมูลใบหน้าที่ต้องการนำไปใช้งาน นำผลการทดสอบมาเรียงลำดับความแม่นยำจากสูงสุดไปต่ำสุด โดยผลการทดสอบของแต่ละบริษัทให้เลือกเฉพาะระบบที่ดีที่สุดของบริษัท โดยต้องเลือกใช้ระบบรู้จำใบหน้าอัตโนมัติจากบริษัทที่มีผลิตภัณฑ์ที่มีสมรรถนะหรือความถูกต้องแม่นยำเหนือกว่าหรือเท่ากับ 85 percentile ของจำนวนบริษัทที่เข้าทดสอบทั้งหมด

(1.2) ผู้ให้บริการที่มีจำนวนผู้ใช้งานไม่เกิน 10,000,000 คน (สิบล้านคน) หรือมีระดับความเสี่ยงที่อาจก่อให้เกิดผลกระทบในระดับกลางหรือระดับต่ำ โดยใช้หลักการประเมินระดับผลกระทบตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ [16] ควรเลือกใช้ระบบรู้จำใบหน้าอัตโนมัติที่มีสมรรถนะและประสิทธิภาพสูงสุดเท่าที่งบประมาณจะอำนวยโดยอ้างอิงจากผลการทดสอบสมรรถนะจาก NIST ซึ่งในกรณีนี้ไม่ได้กำหนดความแม่นยำขั้นต่ำ แต่จะเน้นประโยชน์ของการนำเทคโนโลยีรู้จำใบหน้าไปใช้งานให้เกิดประโยชน์กับผู้ใช้บริการสูงสุด สะดวก และปลอดภัย

(2) **ในกรณีที่มีฐานข้อมูลการทดสอบภาพใบหน้าโดยเฉพาะของผู้ใช้หลัก** การกำหนดค่าความแม่นยำในการเปรียบเทียบภาพใบหน้าของระบบรู้จำใบหน้าอัตโนมัติ ต้องอ้างอิงกับผลการทดสอบสมรรถนะระบบซึ่งผ่านการทดสอบโดยหน่วยงานหรือสถาบันที่มีความน่าเชื่อถือซึ่งได้รับการยอมรับจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ สำหรับการกำหนดมาตรฐานความแม่นยำขั้นต่ำให้เป็นไปตามแนวทางการใช้งานชีวมิติของภาคอุตสาหกรรมนั้น อาทิ ผู้ให้บริการทางการเงินที่อยู่ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย ให้ยึดแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน

ข้อเสนอแนะการกำหนดมาตรฐานความแม่นยำขั้นต่ำนี้ ใช้สำหรับเวลาเริ่มต้นในการเลือกระบบรู้จำใบหน้าอัตโนมัติเท่านั้น เมื่อเลือกระบบไปแล้วและใช้งานระบบไปตามระยะเวลาที่เหมาะสม ควรมีการปรับปรุงระบบให้ลดความผิดพลาด เพิ่มประสิทธิภาพ ป้องกันการโจมตีหลอกใหม่ ๆ โดยปรับปรุงระบบให้ทันสมัยตามเทคโนโลยีที่เปลี่ยนแปลงไป เพื่อให้สามารถใช้งานระบบได้อย่างมีประสิทธิภาพสูงสุด สะดวก และปลอดภัย

4.8 มาตรฐานการแลกเปลี่ยนข้อมูลภาพใบหน้าระหว่างหน่วยงาน

การแลกเปลี่ยนข้อมูลภาพใบหน้าระหว่างหน่วยงาน ควรพิจารณาตามแนวทางข้อเสนอแนะในมาตรฐาน ขมธอ. 29 เล่ม 1-2565 [4] โดยในกรณีที่จะมีการแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน ควรเป็นไปตามมาตรฐานสากล อาทิ มาตรฐานการแลกเปลี่ยนชีวมิติร่วมกัน (common biometric exchange formats: CBEF) ซึ่งกำหนดอยู่ในมาตรฐาน ISO/IEC 19785-1:2020 [13]

การแลกเปลี่ยนข้อมูลใบหน้าต้องผ่านช่องทางที่มีความปลอดภัย เมื่อมีการแลกเปลี่ยนข้อมูลใบหน้าระหว่างหน่วยงาน ข้อมูลใบหน้าต้องถูกเข้ารหัส โดยข้อมูลที่เข้ารหัสแล้วต้องแยกส่วนกับข้อมูลส่วนบุคคลอื่น ๆ และส่งข้อมูลเหล่านี้แยกกันไม่รวมกัน เพื่อป้องกันข้อมูลใบหน้าในกรณีที่ข้อมูลอยู่ในระหว่างนำส่งโดยเจ้าหน้าที่ผู้ประสานงานหรือในกรณีที่มีการดักจับข้อมูลระหว่างหน่วยงาน เจ้าหน้าที่ผู้รับผิดชอบจะเข้าถึงข้อมูลส่วนนี้ได้จะต้องได้รับกุญแจในการถอดรหัสในช่องทางที่มีการรักษาความปลอดภัยของข้อมูลสูงสุด

4.9 ข้อเสนอแนะเกี่ยวกับการรักษาความปลอดภัยข้อมูลภาพใบหน้า

การรักษาความปลอดภัยของข้อมูลสำหรับการรู้จำใบหน้าควรมีการพิจารณาด้านการโจมตีหลอกระบบ (presentation attack) และการโจมตีแบบรวมภาพ (morph attack) โดยรายละเอียดข้อเสนอแนะที่เพิ่มเติมจากแนวทางซึ่งอ้างอิงอยู่ในมาตรฐาน ขมธอ. 29 เล่ม 1-2565 [4] เฉพาะที่เกี่ยวข้องกับข้อมูลภาพใบหน้า มีดังต่อไปนี้

(1) การป้องกันการสับเปลี่ยนภาพใบหน้า ผู้ให้บริการควรกำหนดการลงทะเบียนข้อมูลภาพใบหน้าทั้งการลงทะเบียนครั้งแรกและการเก็บข้อมูลภาพใบหน้าซ้ำให้เป็นแบบพบเจอตัวจริง (face-to-face) หรือกรณีที่หน่วยงานมีระบบการลงทะเบียนอัตโนมัติ (auto-enrolment) ควรจัดเจ้าหน้าที่สอดส่องดูแลที่

เครื่องลงทะเบียน หรือมีระบบอัตโนมัติตรวจสอบการทุจริต และมีการบันทึกวีดิทัศน์ตลอดการลงทะเบียนอัตโนมัติเพื่อป้องปรามหรือสืบสวนเมื่อมีปัญหาเกิดขึ้น

หากผู้ให้บริการไม่สามารถปฏิบัติตามข้อเสนอแนะในการลงทะเบียนแบบพบเจอตัวจริงได้ ในกรณีของการลงทะเบียนแบบไม่พบเจอตัวจริง (non face-to-face) นั้น ผู้ให้บริการจำเป็นต้องมั่นใจว่าผู้ใช้บริการเป็นตัวจริงก่อนการเก็บภาพใบหน้า ผู้ให้บริการต้องสามารถป้องกันการสวมตัวหรือการลงทะเบียนแทนกันโดยใช้อัตลักษณ์ของคนหนึ่งและใช้ใบหน้าของอีกคนหนึ่งในการลงทะเบียนในกรณีที่มีการสมรู้ร่วมคิดกัน และผู้ให้บริการต้องมีกระบวนการตรวจสอบคุณภาพและความน่าเชื่อถือของภาพใบหน้า โดยการตรวจสอบความน่าเชื่อถือของภาพใบหน้าต้องมีการทดสอบการตรวจจับการโจมตีหลอกผ่านการเก็บข้อมูล (through data capture) และ การตรวจจับการมีชีวิต (liveness detection) เป็นอย่างน้อย ซึ่งอ้างอิงอยู่ในมาตรฐาน ขมธอ. 29 เล่ม 1-2565 (หัวข้อที่ 7) [4]

หมายเหตุ: ข้อเสนอแนะมาตรฐานฉบับนี้ แนะนำให้การลงทะเบียนข้อมูลภาพใบหน้าควรเป็นแบบพบเจอตัวจริง เพื่อป้องกันการถูกสวมตัวและเพื่อให้ได้ข้อมูลภาพใบหน้าที่มีความน่าเชื่อถือ ซึ่งอาจก่อให้เกิดผลเสียแก่ผู้ใช้บริการและการจัดการระบบรู้จำใบหน้าอัตโนมัติของผู้ให้บริการได้ต่อไป

(2) การป้องกันการปลอมแปลงภาพใบหน้า ผู้ให้บริการต้องใช้ใบหน้าจริงในการรับภาพเท่านั้น โดยเก็บภาพถ่ายใบหน้าสด (live captured image) เพื่อนำเข้าระบบรู้จำใบหน้าอัตโนมัติ นอกจากนี้ภาพใบหน้าควรมีข้อกำหนดทางกายภาพดังต่อไปนี้

- ควรเห็นใบหน้าเต็มวง
- ไม่ควรหลับตา ให้มองตาตรงตามปกติ
- ไม่ควรแสดงอารมณ์ทางสีหน้า เช่น การยิ้ม
- ไม่ควรสวมแว่นหรือมีผมปิดบังใบหน้า
- หากผู้ใช้บริการจำเป็นต้องสวมแว่น ต้องให้เห็นดวงตาชัดเจนโดยปราศจากแสงสะท้อนที่เลนส์แว่นตา
- การคลุมผ้าโพกศีรษะตามประเพณี ศาสนา หรือข้อจำกัดด้านการแพทย์ ต้องมองเห็นใบหน้าได้ตั้งแต่ไรผมถึงคางและไปถึงด้านหน้าของใบหู
- การถ่ายภาพผ่านพลาสติกใส ต้องไม่มีแสงสะท้อนหรือเงาทาบบนใบหน้า

(3) การป้องกันการสับสนของการใช้งาน ผู้ให้บริการต้องใช้ภาพใบหน้าที่ไม่มีใบหน้าบุคคลอื่นอยู่ในภาพเป็นภาพใบหน้าที่จะนำเข้าระบบรู้จำใบหน้าอัตโนมัติ

(4) การดูแล บริหารจัดการ และการรักษาความมั่นคงปลอดภัยของอุปกรณ์ ผู้ให้บริการต้องจำกัดการเชื่อมต่ออุปกรณ์กับเครือข่ายสาธารณะ จำกัดการติดตั้งซอฟต์แวร์ และปิดพอร์ตเชื่อมต่ออุปกรณ์ เช่น พอร์ตยูเอสบี (USB) นอกจากนี้ ผู้ให้บริการต้องมีระบบการเฝ้าระวังภัยคุกคามทางไซเบอร์สำหรับระบบเครือข่ายของระบบรู้จำใบหน้าอัตโนมัติ

4.10 ข้อเสนอแนะเกี่ยวกับสิทธิส่วนบุคคลกับข้อมูลภาพใบหน้า

ข้อมูลภาพใบหน้า ถือเป็นข้อมูลส่วนบุคคลซึ่งมีกฎหมายให้การคุ้มครอง อยู่ 2 ฉบับคือ

(1) กฎหมายข้อมูลข่าวสารทางราชการ [14]

(2) กฎหมายคุ้มครองข้อมูลส่วนบุคคล [15]

หน่วยงานต่าง ๆ ที่จะใช้ข้อมูลภาพใบหน้าสำหรับการพิสูจน์และยืนยันตัวตน จะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และสำหรับการแลกเปลี่ยนข้อมูลข่าวสารระหว่างหน่วยงานของรัฐ จะต้องปฏิบัติตามกฎหมายข้อมูลข่าวสารทางราชการ อย่างเคร่งครัด

บรรณานุกรม

[1] ขมธอ. 18-2564 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน (เวอร์ชัน 2.0)

[2] ขมธอ. 19-2564 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (เวอร์ชัน 2.0)

[3] ขมธอ. 20-2564 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (เวอร์ชัน 2.0)

[4] ขมธอ. 29 เล่ม 1-2565 ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยเทคโนโลยีชีวมิติ – เล่ม 1: การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน

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

[6] [8]International Organization for Standardization, “ISO/IEC TR 30110:2015 Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and children”, November 2015.

[7] Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down for the quality, resolution and use of fingerprint and facial image for biometric verification and identification in the Entry/Exit System (EES)
Access: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0329

[8] แนวปฏิบัติการใช้เทคโนโลยีชีวมิติในการให้บริการทางการเงิน ธนาคารแห่งประเทศไทย

[9] International Organization for Standardization, “ISO/IEC 29794-5:2010 Information technology — Biometric sample quality — Part 5: Face image data”, April 2010.

[10] International Organization for Standardization, “ISO/IEC 29794-1:2016 Information technology — Biometric sample quality — Part 1: Framework”, January 2016.

[11] International Organization for Standardization, “ISO/IEC 39794-1:2019 Information technology — Extensible biometric data interchange formats — Part 1: Framework”, December 2019.

[12] International Organization for Standardization, “ISO/IEC 39794-5:2019 Information technology — Extensible biometric data interchange formats — Part 5: Face image data”, December 2019.

[13] International Organization for Standardization, “ISO/IEC 19785-1:2020 Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification”, September 2020.

[14] พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540

[15] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[16] ประกาศคณะกรรมการธุรกรรมทางอิเล็กกทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555