

การใช้ระบบรู้จำใบหน้า (Facial Recognition)

ตอบโจทย์การพิสูจน์และยืนยันตัวตน
ได้จริงไหม?



การใช้ระบบรู้จำใบหน้า (Facial Recognition) ตอบโจทย์การพิสูจน์และยืนยันตัวตนได้จริงไหม

1. บทนำ

ในปัจจุบัน ระบบรู้จำใบหน้า (Facial Recognition) เป็นส่วนสำคัญของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ทั้งในแง่ของการเพิ่มความรวดเร็ว สะดวก และมีความน่าเชื่อถือที่ค่อนข้างสูง อย่างไรก็ตาม เทคโนโลยีนี้อาจไม่สามารถแก้ปัญหาที่เกิดขึ้นในการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ทั้งหมด รวมถึงยังมีข้อจำกัดและความท้าทายที่ต้องพิจารณาในการนำระบบรู้จำใบหน้ามาใช้งาน เช่น การจัดการความเสี่ยงด้านความเป็นส่วนตัวของผู้ใช้บริการ การรั่วไหลของข้อมูลภาพใบหน้า รวมถึงการที่ประชากรบางกลุ่มไม่สามารถเข้าถึงเทคโนโลยีนี้ได้ เช่น กลุ่มผู้ที่ไม่มีความรู้เรื่องเทคโนโลยี สิ่งเหล่านี้ล้วนเป็นช่องว่างที่ควรพิจารณาแนวทางการแก้ปัญหา และกำหนดให้มีการนำวิธีการทางเลือกอื่น ๆ มาใช้ร่วมด้วยเพื่อเสริมสร้างความน่าเชื่อถือและความมั่นคงปลอดภัยของการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ข้อดีของระบบรู้จำใบหน้า	ข้อจำกัดและความท้าทายของระบบรู้จำใบหน้า
● ประสิทธิภาพ ยืนยันตัวตนรวดเร็ว ลดเวลารอ ● ความสะดวก ใช้ใบหน้ายืนยันตัวตนผ่านสมาร์ทโฟน ไม่ต้องใช้บัตรหรือจ่ารหัสผ่าน ● ความสามารถในการขยายขอบเขตการใช้งาน มือถือส่วนใหญ่มีกล้องหน้า รองรับผู้ใช้งานจำนวนมาก ● ความแม่นยำสูง อัลกอริทึมก้าวหน้า แม่นยำกว่า 99% ● ศักยภาพด้านความปลอดภัย ยากต่อการปลอมแปลง มีการตรวจจับการปลอมแปลงแบบกันทั่วทั้ง	● ความเสี่ยงด้านความปลอดภัย ข้อมูลรั่วไหล, Deepfake ● การยินยอมการใช้ข้อมูล ต้องแจ้งผู้ใช้งานชัดเจน ● การพึ่งพาเทคโนโลยีภายนอก อาจมีความเสี่ยงระบบหยุดชะงัก ● การเข้าถึงสมาร์ทโฟน ข้อจำกัดสำหรับผู้ที่ไม่ใช้สมาร์ทโฟนหรืออินเทอร์เน็ต ● การขาดทางเลือก ควรมียุติวิธีผู้ไม่สะดวกทางเลือกอื่น ● ความท้าทายกับความคล่องตัวในครอบครัว ยากในการแยกแยะฝ่าแฝด

2. ข้อดีของระบบรู้จำใบหน้า

ระบบรู้จำใบหน้ามีข้อดีหลายด้านที่ช่วยส่งเสริมการพิสูจน์และยืนยันตัวตนทางดิจิทัล ทั้งนี้ประสิทธิภาพที่ได้รับขึ้นอยู่กับแนวทางการใช้งานและพัฒนาระบบรู้จำใบหน้าของหน่วยงาน

- **ประสิทธิภาพ (Efficiency):** ระบบรู้จำใบหน้าช่วยลดเวลาที่ต้องใช้ในการยืนยันตัวตนผู้ใช้บริการ เพิ่มความสะดวกสบาย โดยยังคงความน่าเชื่อถือในการยืนยันตัวตนอยู่
- **ความสะดวก (Convenience):** ผู้ใช้บริการสามารถยืนยันตัวตนด้วยใบหน้าผ่านกล้องสมาร์ทโฟน ลดการจดจำรหัสผ่าน และลดความเสี่ยงจากการสัมผัสอุปกรณ์ร่วมกับผู้อื่น เช่น การใช้อุปกรณ์สแกนลายนิ้วมือเพื่อเข้าอาคาร
- **ความสามารถในการขยายขอบเขตการใช้งาน:** ปัจจุบันผู้ใช้อินเทอร์เน็ตในไทยมีสัดส่วนร้อยละ 89.5 ของประชากรอายุ 6 ปีขึ้นไป และผู้ใช้โทรศัพท์มือถือมีสัดส่วนร้อยละ 95.5 [1] โดยโทรศัพท์มือถือส่วนใหญ่จะมีกล้องหน้าสำหรับใช้ยืนยันตัวตนด้วยใบหน้า ในขณะที่โทรศัพท์มือถือที่รองรับการสแกนลายนิ้วมือมีจำนวนน้อยกว่า นอกจากนี้ การใช้ลายนิ้วมือยังมีข้อจำกัด เช่น ผู้พิการบางรายไม่สามารถใช้ระบบสแกนลายนิ้วมือได้ หรือแรงงานบางกลุ่มที่ลายนิ้วมือไม่ชัดเจนเนื่องจากการทำงานหนักเป็นประจำ
- **ความแม่นยำ (Accuracy):** เทคโนโลยีรู้จำใบหน้ามีความก้าวหน้าอย่างมากจากการพัฒนาอัลกอริทึมปัญญาประดิษฐ์ (AI) และการเรียนรู้เชิงลึก (Deep Learning) โดยพบว่าอัลกอริทึมที่ได้รับการพัฒนามีความแม่นยำสูงกว่า 99% และมีอัตราความผิดพลาดต่ำกว่าการใช้ลายนิ้วมืออย่างมีนัยสำคัญ [2] อย่างไรก็ตาม การพัฒนาระบบรู้จำใบหน้าให้มีความแม่นยำสูง ต้องอาศัยข้อมูลปริมาณมากและเครื่องมือการเรียนรู้เชิงลึกที่มีประสิทธิภาพ [3]

- **ศักยภาพด้านความปลอดภัย (Security Potential):** เทคโนโลยีรู้จำใบหน้าที่มีประสิทธิภาพสามารถเพิ่มความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะเมื่อผสานกับเทคนิคตรวจจับการปลอมแปลงข้อมูลภาพใบหน้า เพื่อให้สามารถป้องกันการโจมตีแบบสวมรอยได้อย่างทันทั่วทั้งที่

3. ข้อจำกัดและความท้าทายของระบบรู้จำใบหน้า

แม้ระบบรู้จำใบหน้าจะมีข้อดีที่หลากหลาย แต่ก็มีข้อจำกัดและความท้าทายที่สำคัญที่ต้องพิจารณาอย่างรอบคอบในการนำระบบรู้จำใบหน้ามาใช้ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- **ความเสี่ยงด้านความปลอดภัย (Security Risks) และการโจมตีแบบปลอมแปลง (Spoofing Attacks):** หากไม่มีมาตรการป้องกันที่เพียงพอ ข้อมูลชีวมิติ เช่น ภาพใบหน้า อาจรั่วไหลและถูกนำไปใช้ในทางที่ผิด ระบบรู้จำใบหน้าที่ยังมีความเสี่ยงต่อการโจมตีด้วยเทคนิคต่าง ๆ เช่น การใช้ภาพถ่ายที่พิมพ์ออกมา หน้ากากสามมิติ (3D Mask) และเทคโนโลยี Deepfake ดังนั้น การใช้เทคนิคต่าง ๆ เพื่อตรวจจับการโจมตี เช่น การตรวจจับการมีชีวิตหรือการปลอมใบหน้า (Liveness Detection) จึงเป็นมาตรการสำคัญเพื่อยืนยันว่าข้อมูลภายในที่ระบบได้รับนั้น มาจากบุคคลจริง ไม่ใช่วัตถุหรือสื่อปลอม
- **ปัญหาจากการยินยอมการใช้ข้อมูล (Consent Issues):** ผู้ให้บริการต้องแจ้งวัตถุประสงค์การใช้ข้อมูลภาพใบหน้าที่ชัดเจน และต้องได้รับความยินยอมจากผู้ใช้บริการ เพื่อให้เป็นไปตามกฎหมาย และเพื่อสร้างความโปร่งใสและรักษาความเชื่อมั่นของผู้ใช้บริการ [4]
- **การพึ่งพาเทคโนโลยีจากภายนอก (Reliance on External Technology):** ผู้ให้บริการบางรายใช้เทคโนโลยีรู้จำใบหน้าจากหน่วยงานที่เป็นบุคคลที่สาม ซึ่งอาจทำให้ผู้ให้บริการต้องปฏิบัติตามข้อกำหนด และเผชิญความเสี่ยงจากการหยุดชะงักของระบบหากเกิดปัญหากับหน่วยงานที่เป็นบุคคลที่สาม
- **การเข้าถึงสมาร์ทโฟน (Smartphone Accessibility):** ประชากรบางกลุ่มอาจไม่มีสมาร์ทโฟน ทำให้ไม่สามารถเข้าถึงบริการที่ต้องใช้การยืนยันตัวตนด้วยใบหน้าได้
- **การขาดทางเลือก (Lack of Alternatives):** หากระบบของผู้ให้บริการบังคับให้ใช้การยืนยันตัวตนด้วยใบหน้าเพียงวิธีเดียว อาจสร้างความไม่สะดวกหรือความกังวลแก่ผู้ใช้บางกลุ่ม ซึ่งผู้ให้บริการควรกำหนดแนวทางแก้ไขหรือการเพิ่มตัวเลือกในการยืนยันตัวตน เช่น การใช้รหัส OTP หรือใช้ข้อมูลชีวมิติอื่น เช่น ลายนิ้วมือ
- **อคติและความไม่แม่นยำ (Bias and Inaccuracy):** เทคโนโลยีรู้จำใบหน้าถูกวิจารณ์ว่ามีอคติ โดยเฉพาะเมื่อใช้งานกับกลุ่มประชากรที่หลากหลาย เช่น เชื้อชาติ เพศ อายุ และสีผิว จากการศึกษาพบว่าระบบรู้จำใบหน้ามีความแม่นยำที่น้อยลง เมื่อนำมาใช้กับในกลุ่มคนผิวสี ผู้หญิง และบุคคลกลุ่มพิเศษ (เช่น ดาวน์ซินโดรม) ซึ่งอาจนำไปสู่การยืนยันตัวตนผิดพลาดได้ [2] [5]
- **ความท้าทายกับความคล้ายคลึงกันในครอบครัว (Challenges with Familial Similarity):** ระบบรู้จำใบหน้าอาจมีข้อจำกัดในการแยกแยะฝาแฝด หรือเกิดความผิดพลาดในการแยกภาพใบหน้า

ของสมาชิกในครอบครัวที่มีความคล้ายคลึงกัน ซึ่งปัญหานี้พบได้ค่อนข้างน้อยในระบบชีวมิติที่ใช้การเปรียบเทียบข้อมูลลายนิ้วมือหรือม่านตา

4. สรุป

ระบบรู้จำใบหน้าเป็นเทคโนโลยีสำคัญที่ช่วยเพิ่มความสะดวกและประสิทธิภาพในการพิสูจน์และยืนยันตัวตนทางดิจิทัล ด้วยความสามารถในการทำงานที่รวดเร็วและแม่นยำสูงเมื่อใช้อัลกอริทึมที่น่าเชื่อถือ อย่างไรก็ตาม เทคโนโลยีนี้ยังมีข้อจำกัดและความท้าทายหลายด้าน เช่น ความเสี่ยงจากการรั่วไหลของข้อมูลชีวมิติ การโจมตีแบบปลอมแปลง และปัญหาอคติ (bias) ของอัลกอริทึมที่ส่งผลต่อความแม่นยำของระบบเมื่อนำมาใช้กับกลุ่มประชากรจากหลากหลายเชื้อชาติ นอกจากนี้ยังมีประเด็นด้านความเป็นส่วนตัว การยินยอมใช้ข้อมูล และการเข้าถึงเทคโนโลยีสำหรับประชากรบางกลุ่ม การพึ่งพาเทคโนโลยีจากบุคคลที่สามก็เป็นอีกปัจจัยที่เพิ่มความเสี่ยงต่อความต่อเนื่องของบริการ เพื่อแก้ไขข้อจำกัดเหล่านี้ ผู้ให้บริการควรพิจารณาแนวทางการเสริมความมั่นคงปลอดภัยของระบบรู้จำใบหน้า การยืนยันตัวตนด้วยวิธีอื่น (เช่น การใช้รหัส OTP หรือเทคโนโลยีชีวมิติอื่น ๆ) พร้อมทั้งกำหนดมาตรการด้านความปลอดภัยและความเป็นส่วนตัวอย่างเข้มงวด เพื่อให้การพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความมั่นคงปลอดภัย โปร่งใส และครอบคลุมผู้ใช้ทุกกลุ่ม

อ้างอิง

- [1] “High percentage of Thais ICT savvy, survey shows”, Accessed: Jun. 17, 2025. [Online]. Available: <https://www.nationthailand.com/thailand/general/40036030>
- [2] M. Daud, “How Does Facial Recognition Work in Identity Verification?”, Keesing. Accessed: Jun. 22, 2025. [Online]. Available: <https://www.keesingtechnologies.com/blog/keesing-blog/how-does-facial-recognition-work-in-identity-verification/>
- [3] B. Klare, “The Pros and Cons of Face & Facial Recognition - advantages and disadvantages, how accurate Face id technology”, ROC. Accessed: Jun. 22, 2025. [Online]. Available: <https://roc.ai/2023/03/29/the-pros-and-cons-of-face-recognition/>
- [4] R. Healey, “Dangers of Using AI Facial Recognition Technology”, Formiti. Accessed: Jun. 22, 2025. [Online]. Available: <https://formiti.com/dangers-of-using-ai-facial-recognition-under-the-thailand-pdpa/>
- [5] “What is Facial Recognition & How does it work?”, /. Accessed: Jun. 22, 2025. [Online]. Available: <https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition>