การเรียนรู้ของเครื่องในการพิสูจน์ตัวตนด้วยชีวมาตร
Machine learning in biometric authentication

สุวิมล วงศ์สิงห์ทอง[1*], จุฑามาส ไพบูลย์ศักดิ์[2] และ ทรงพล นคเรศเรืองศักดิ์[3]
Suwimon Vongsingthong[1*], Juthamas Paiboonsak[2] and Songpon Nakaresruengsak[3]

Received: 29 August 2022 ; **Revised**: 24 October 2022 ; **Accepted**: 28 December 2022

บทคัดย่อ
ไบโอเมตริกซ์ เป็นนวัตกรรมที่มีการพัฒนาอย่างรวดเร็วในยุคที่ปัญญาประดิษฐ์แพร่หลาย โดยอัตลักษณ์ดิจิทัลของมนุษย์ที่นิยมใช้ในการพิสูจน์ตัวตนในอุปกรณ์ทั่วไปและอุปกรณ์เคลื่อนที่ ได้แก่ ลายนิ้วมือ ม่านตา และใบหน้า ด้วยความเป็นเอกลักษณ์และความสะดวกในการใช้งานที่ให้ทั้งความปลอดภัยและความรวดเร็วในการทำรายการ ทั้งยังเป็นการเพิ่มความมั่นใจให้กับผู้ทำธุรกรรมออนไลน์และผู้ใช้อุปกรณ์เคลื่อนที่ในยุคปกติใหม่ จนรหัสผ่านเพื่อพิสูจน์ตัวตนแบบดั้งเดิมได้รับความนิยมน้อยลง การทำงานของระบบการพิสูจน์ตัวตนแบบไบโอเมตริกซ์ใช้เทคนิคการประมวลผลภาพและการจดจำรูปแบบ คุณภาพของภาพนำเข้าจึงมีผลต่อประสิทธิภาพของระบบอย่างมาก ความท้าทายที่สำคัญ ในการประมวลผลของระบบเกิดจากการนำเข้าภาพที่มีสัญญาณรบกวน ตัวอย่างทางพยาธิสภาพที่ไม่ดี และสภาพแวดล้อมที่ยากต่อการควบคุม ดังนั้น การบูรณาการการเรียนรู้ของเครื่องเข้ากับระบบพิสูจน์ตัวตนแบบไบโอเมตริกซ์จึงเป็นนวัตกรรมทางเลือกที่ได้รับความสนใจในการเพิ่มความชาญฉลาดและประสิทธิภาพของกระบวนการตรวจสอบความถูกต้อง ขณะเดียวกันยังช่วยลดเวลาในการประมวลผล และลดกระบวนการที่ซับซ้อนโดยไม่ต้องปรับแก้โปรแกรม บทความวิชาการนี้จึงจัดทำขึ้นเพื่อประเมินจุดแข็ง และจุดอ่อนของไบโอเมตริกซ์ข้างต้น โดยนำเสนอหลักฐานเชิงประจักษ์เกี่ยวกับความก้าวหน้าในการบูรณาการการเรียนรู้ของเครื่องเข้ากับระบบพิสูจน์ตัวตนแบบไบโอเมตริกซ์ ประโยชน์ที่ได้ คือ การให้ข้อมูลทางเลือกที่เหมาะสม คุ้มค่า และมีประสิทธิภาพสำหรับผู้ที่กำลังมองหาเทคโนโลยีรักษาความปลอดภัยในการทำธุรกรรมต่างๆ เช่น การจองที่พัก การทำรายการบัญชีธนาคาร การขอรับสวัสดิการจากรัฐ การรับคำขอเป็นเพื่อนบนโซเชียลมีเดีย หรือการมีปฏิสัมพันธ์อื่นๆทางออนไลน์

คำสำคัญ: การเรียนรู้ของเครื่อง ไบโอเมตริกซ์ ระบบพิสูจน์ตัวตน อัตลักษณ์ดิจิทัล

Abstract
Within the artificial intelligence rebellion, barely any innovation has been meliorated as quickly as biometrics. Fingerprint, iris, and face are popular digital identities, routinely integrated into common devices and portable gadgets to empower a quick and secure authentication. The uniqueness and ease of use of biometrics have subrogated traditional authentication, such as password and powered up the confidence of users conducting online transactions and using mobile devices in the new normal era. The authentication systems are actuated by image processing and pattern recognition techniques. The performance of these systems are highly affected by the quality of the acquired input where noisy images, poor pathological samples, and less controlled surroundings are major challenges to overcome. An innovative and attractive alternative is the machine learning based authentication. The intelligence and efficiency of authentication process can be increased while processing time and complication processes are lessen without program

[1] สาขาวิชาธุรกิจวิศวกรรม คณะวิทยาการจัดการ สถาบันวิทยาการจัดการแห่งแปซิฟิค วิทยาเขตนิมิตใหม่ ปทุมธานี 12150
[2] สาขาวิชาเทคโนโลยีสารสนเทศและการจัดการ คณะบริหารธุรกิจ มหาวิทยาลัยเกริก กรุงเทพ 10220
[3] สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี วิทยาลัยเซาธ์อีสท์บางกอก กรุงเทพ 10260
[1] Department of Engineering Business, Faculty of Management Science, Pacific Institute of Management Science, Nimitmai Campus, Pathum Thani 10220, Thailand
[2] Department of Information Technology and Management, Faculty of Business Administration, Krirk University, Bangkok 10220, Thailand
[3] Department of Information technology, Faculty of Science and Technology, Southeast College Bangkok, Bangkok, 10260, Thailand
[*] Corresponding Author, e-mail: suwimonv@yahoo.com

adjustment. Therefore, this academic article was composed to evaluate the strengths and weaknesses of the top three aforementioned biometrics. Empirical evidences on the breakthrough of machine learning based authentication systems were presented. The benefits lie in providing solutions for those who are looking for the appropriate, cost-effective and efficient security technology for booking accommodation with a host, accessing bank account, applying for government benefits, accepting a new friend request on social media or any online interactions.

Keywords: Authentication, Biometrics, Digital Identity, Machine Learning

บทนำ

การระบาดของ COVID-19 ที่เริ่มขึ้นตั้งแต่ต้นปี พ.ศ.2563 ส่งผลให้ผู้คนปรับเปลี่ยนพฤติกรรมการใช้ชีวิตประจำวัน ลดการทำกิจกรรมนอกบ้าน เช่น เดินทาง ทำงาน เดินเที่ยวซื้อสินค้า รับประทานอาหารในร้าน เป็นการใช้เวลาในบ้านและท่องไซเบอร์เสปสมากขึ้น อัตลักษณ์ดิจิทัลจึงมีความจำเป็นต่อการทำกิจกรรมดังกล่าวเพื่อยืนยันว่าตนเองเป็นผู้ใช้ที่ถูกต้องและได้รับอนุญาตให้ทำธุรกรรมนั้น โดยอัตลักษณ์ดิจิทัลเป็นได้ทั้ง รหัสผู้ใช้ รหัสผ่าน ภาพถ่าย หรืออุปกรณ์ฮาร์ดแวร์ เช่น บัตร ATM สมาร์ทการ์ด และโทรศัพท์เคลื่อนที่ แม้สิ่งเหล่านี้มีความสำคัญต่อการรักษาความปลอดภัย แต่ก็เพิ่มความยุ่งยากในการจดจำหรือพกพา ทำให้เอกลักษณ์ทางชีวภาพของมนุษย์ หรือไบโอเมตริกซ์ (Biometrics) ที่ให้ทั้งความสะดวกสบาย และความแม่นยำในระดับสูง กลายเป็นทางเลือกต้นๆ ในการพิสูจน์และยืนยันตัวตน (Authentication) ที่ได้รับความนิยม เพราะช่วยแก้ปัญหาการลืมรหัสผ่าน และ token พิสูจน์ตัวตนสูญหาย (Ali, 2021; สุวิมล วงศ์สิงห์ทอง, 2565)

ไบโอเมตริกซ์ถูกนำมาใช้ในกระบวนการพิสูจน์ตัวตนที่ต้องการความถูกต้องและความปลอดภัยในระดับสูง ตัวอย่างเช่น สายการบิน Delta Air Lines ในรัฐแอตแลนตา สหรัฐอเมริกา และสายการบินเครือข่าย นำเทคโนโลยีจดจำใบหน้า (Face Recognition) มาให้ผู้โดยสารเช็คอินผ่านตู้บริการแบบเรียลไทม์ ทำให้ผู้โดยสารเดินทางผ่านสนามบินได้อย่างรวดเร็วแบบไร้รอยต่อ (Lardinois, 2021) ธนาคาร Seven ประเทศญี่ปุ่น (Seven Bank, 2019) ใช้เทคโนโลยีจดจำใบหน้ามาเพิ่มความปลอดภัยให้กับผู้ใช้บริการ ATM ที่ตู้กดเงิน รถไฟรางเบาแดลลัส (Dallas Area Rapid Transit: DART) ในนอร์ทเท็กซัส สหรัฐอเมริกา (Shepard, 2016) ใช้เทคโนโลยีจดจำใบหน้ามาพิสูจน์ตัวตนผู้ใช้บริการขนส่งสาธารณะเพื่อให้บริการได้อย่างครอบคลุมตั้งแต่การจองตั๋ว การจัดเก็บข้อมูลความต้องการพิเศษของผู้โดยสาร จนถึงเชื่อมต่อข้อมูลประวัติการรักษาพยาบาลของผู้โดยสารให้กับโรงพยาบาล หรือสถานีตำรวจเพื่อขอความช่วยเหลือกรณีฉุกเฉิน

แนวทางการเพิ่มระดับความปลอดภัยให้สูงขึ้นสามารถทำได้โดยการเพิ่มปัจจัยในการพิสูจน์ตัวตน ดังเช่น สำนักงานสอบสวนกลางสหรัฐ (Federal Bureau of Investigation: FBI) (Seffers, 2020) และองค์การตำรวจอาชญากรรมระหว่างประเทศ (International Criminal Police Organization: Interpol) ใช้ปัจจัยในการยืนยันตัวตนที่ประกอบด้วยลายนิ้วมือ ม่านตา ใบหน้า ท่าทางการเดิน และเสียง เพื่อสืบค้นและตรวจสอบประวัติอาชญากร (Macdonald, 2022) ผู้ผลิตอุปกรณ์ IoT (Internet of Things) เช่น Google Home, Alexa และ Siri ใช้เทคโนโลยีการจดจำเสียงมาผสมผสานกับเทคโนโลยีการจดจำใบหน้าเพื่อเปิดไฟ หรือปิด/เปิดประตูบ้าน (Noh, *et al.* 2020) นอกจากนี้ไบโอเมตริกซ์ยังถูกนำมาใช้ในโครงการระดับชาติขนาดใหญ่ เช่น โครงการ Aadhaar ที่ดำเนินการโดยกระทรวงอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศ ประเทศอินเดีย ตามพระราชบัญญัติ Aadhaar 2016 เพื่อนำไบโอเมตริกซ์มารักษาความปลอดภัยให้ฐานข้อมูลประชาชนอินเดียมากกว่าพันล้านคนแบบรวมศูนย์ ด้วยการให้ประชาชนที่เข้าร่วมโครงการใช้บัตร Adahaar ที่บูรณาการไบโอเมตริกซ์ของม่านตา และลายนิ้วมือ เข้ากับเลขบัตรประชาชน 12 หลัก แทนระบบสูติบัตรและบัตรปันส่วนแบบเดิมที่เสี่ยงต่อการสูญหายหรือเสียหาย ความสำเร็จในการนำไบโอเมตริกซ์มาใช้ครั้งนี้ทำให้คนชายขอบในชนบทสามารถเข้าถึงบริการของรัฐ และรัฐก็ลดเวลาและค่าใช้จ่ายในการบันทึกข้อมูลและตรวจสอบความถูกต้องของข้อมูลพลเมือง ประโยชน์เชิงประจักษ์ คือให้ความสะดวกและความปลอดภัยกับประชาชนเป็นอย่างมาก จนมีการขยายความร่วมมือต่อไปยังประเทศศรีลังกาและประเทศอื่นๆ ในภูมิภาค (Jayashree, 2019)

ไบโอเมตริกซ์ หรือการประยุกต์ใช้เอกลักษณ์ของมนุษย์จึงกลายเป็นแนวทางหลักในการรักษาความปลอดภัยในภาวะปกติใหม่ (New Normal) ด้วยจุดเด่นที่ไบโอเมตริกซ์ยากต่อการลอกเลียนหรือ ทำซ้ำ และให้ความปลอดภัยในระดับสูง จึงเป็นเรื่องสำคัญที่ผู้ใช้ชีวิตในยุคดิจิทัลควรเข้าใจจุดเด่น จุดด้อย และทิศทางการพัฒนาระบบพิสูจน์ตัวตนด้วยไบโอเมตริกซ์ เพื่อให้สามารถเลือกสรรแนวทางการพิสูจน์ตัวตนได้อย่างเหมาะสม สอดคล้องกับบริบทการใช้งาน และมีประสิทธิผลตามที่คาดหวัง บทความนี้จึงจัดทำขึ้น เพื่อวิเคราะห์ความก้าวหน้าในการนำไบโอเมตริกซ์มาใช้ในการพิสูจน์ตัวตน โดยศึกษาไบโอเมตริกซ์ที่มีความแพร่หลาย 3 คุณลักษณะ คือ ลายนิ้วมือ ม่านตา และใบหน้า เพื่อวิเคราะห์แนวทาง

การบูรณาการกระบวนการพิสูจน์ตัวตนด้วยไบโอเมตริกซ์กับการเรียนรู้ของปัญญาประดิษฐ์ หรือการเรียนรู้ของเครื่อง (Machine Learning) ที่ให้ทั้งความถูกต้อง ความมั่นคง และประสิทธิภาพในราคาที่คุ้มค่า

วรรณกรรมที่เกี่ยวข้อง

นับตั้งแต่ยุคเริ่มต้นของคอมพิวเตอร์ มนุษย์มีความพยายามที่จะปกป้องข้อมูลส่วนตัวหรือข้อมูลที่มีความสำคัญด้วยรหัสผ่าน ในขณะที่ผู้ไม่ประสงค์ดีก็คิดค้นวิธีขโมยหรือทำลายรหัสผ่านเพื่อเข้าถึงข้อมูล แม้ต่อมามนุษย์สามารถพัฒนารหัสผ่านที่ซับซ้อนขึ้น ผู้ไม่ประสงค์ดีก็ยังสามารถพัฒนาเครื่องมือทำลายรหัสผ่านที่ซับซ้อนได้เช่นกัน

ในยุคดิจิทัลที่ผู้คนนิยมทำธุรกรรมการเงิน ซื้อขายสินค้า และเข้าถึงข้อมูลส่วนบุคคลผ่านไซเบอร์สเปซ ผู้ใช้รายใดที่มีบัญชีดิจิทัลหลายบัญชีก็ต้องพยายามเพิ่มความปลอดภัยด้วยการสร้างรหัสผ่านที่ซับซ้อนและแตกต่างกันตามกระบวนการรักษาความปลอดภัยที่ถูกต้อง เช่น หากผู้ใช้มีบัญชีดิจิทัล 10 บัญชี หมายถึง มีรหัสผ่าน 10 รหัส การจดจำรหัสผ่านให้ได้ทั้งหมดจึงเป็นเรื่องยุ่งยากและอาจไม่ปลอดภัย เนื่องจากผู้ใช้อาจจะต้องจดรหัสไว้ที่ใดที่หนึ่ง แม้ต่อมามีการเพิ่มความปลอดภัยให้กับระบบพิสูจน์ตัวตนด้วยการเพิ่มปัจจัยเป็นแบบ 2 ปัจจัย(Two-Factor Authentication) หรือหลายปัจจัย(Multi-Factor Authentication) แต่ยังคงพบปัญหารหัสทางกายภาพ (Hardware Token) เช่น บัตรเครดิต หรือบัตร ATM สูญหายหรือถูกขโมย หรือการโจมตีรหัสที่ส่งมาทางโทรศัพท์ ข้อความ หรือ SMS ถูกส่งต่อไปยังโทรศัพท์เครื่องอื่น ทำให้ผู้พัฒนาสนใจแนวทางการตรวจสอบสิทธิ์ด้วยการวิเคราะห์ข้อมูล ที่เรียกว่า การพิสูจน์ตัวตนแบบปรับเปลี่ยนได้หรือการพิสูจน์ตัวตนตามความเสี่ยง (Adaptive/Risk Based Authentication) ที่แนวคิดพื้นฐานมาจากการรวบรวมข้อมูลที่ครอบคลุมพฤติกรรมที่เป็นไปได้ และสภาพแวดล้อมที่หลากหลายของผู้ใช้ในปริมาณมากที่สุด มาจัดทำฐานข้อมูลเพื่อนำมาใช้สร้างกฎเกณฑ์ที่น่าเชื่อถือในการระบุผู้ใช้ ตลอดจนตรวจสอบพฤติกรรมเสี่ยงที่มีแนวโน้มว่าจะเป็นอันตราย เพื่อเพิ่มความสามารถในการป้องกันการปลอมแปลงข้อมูลหรือลักลอบใช้บัญชีโดยปราศจากการแทรกแซงของผู้ใช้

ข้อมูลที่เหมาะสมจึงควรเป็นข้อมูลที่มีความหลากหลาย และมีจำนวนมากพอสำหรับสอนเครื่องให้เกิดการเรียนรู้ โดยข้อมูลนี้อาจเป็นไบโอเมติกซ์ของผู้ใช้ ได้แก่ ม่านตา ลายนิ้วมือ หรือคุณลักษณะอื่นๆ ที่สามารถบ่งบอกตัวตนของเจ้าของบัญชี

1. ไบโอเมตริกซ์ (Biometrics)

ไบโอเมตริกซ์ ประกอบด้วยส่วนสำคัญ 2 ส่วน คือ “Bio” หมายถึง “ชีววิทยา” ที่เป็นการศึกษาเกี่ยวกับวิทยาศาสตร์ของสิ่งมีชีวิต ส่วนใหญ่จัดอยู่ในกลุ่มการวัดเชิงคุณภาพ และ “Metric” หมายถึง ระบบการวัดข้อมูลทางสถิติเพื่อการเปรียบเทียบหรือการติดตาม ซึ่งเป็นตัวชี้วัดเชิงปริมาณ ทั้งสององค์ประกอบอาจดูไม่เข้าพวก แต่ถูกนำมาหลอมรวมกันเพื่อรับรองความถูกต้องและสร้างความปลอดภัยในโลกดิจิทัล ด้วยจุดเด่นที่ไบโอเมตริกซ์เป็นเอกลักษณ์เฉพาะสำหรับทุกคน การระบุตัวตนด้วยไบโอเมตริกซ์จึงให้ความปลอดภัยกว่ารหัสผ่านแบบเดิม

ไบโอเมตริกซ์ที่ใช้ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลมีหลากหลาย เช่น เสียงพูด จังหวะการพิมพ์คีย์บอร์ด ท่าทางการเคลื่อนไหว ลายนิ้วมือ ม่านตา และใบหน้า นอกจากความรวดเร็วและความสะดวกสบาย ยังมีความปลอดภัยสูง เนื่องไม่ปรากฏว่ามีบุคคลสองคนใด แม้กระทั่งเป็นฝาแฝดที่มีลายนิ้วมือ ม่านตา หรือใบหน้าเหมือนกันทุกประการ ดังนั้นไบโอเมตริกซ์จึงมีความพิเศษ ที่เป็นอัตลักษณ์เฉพาะของแต่ละบุคคลที่เหมาะสมจะใช้ตรวจสอบความแตกต่างระหว่างบุคคล

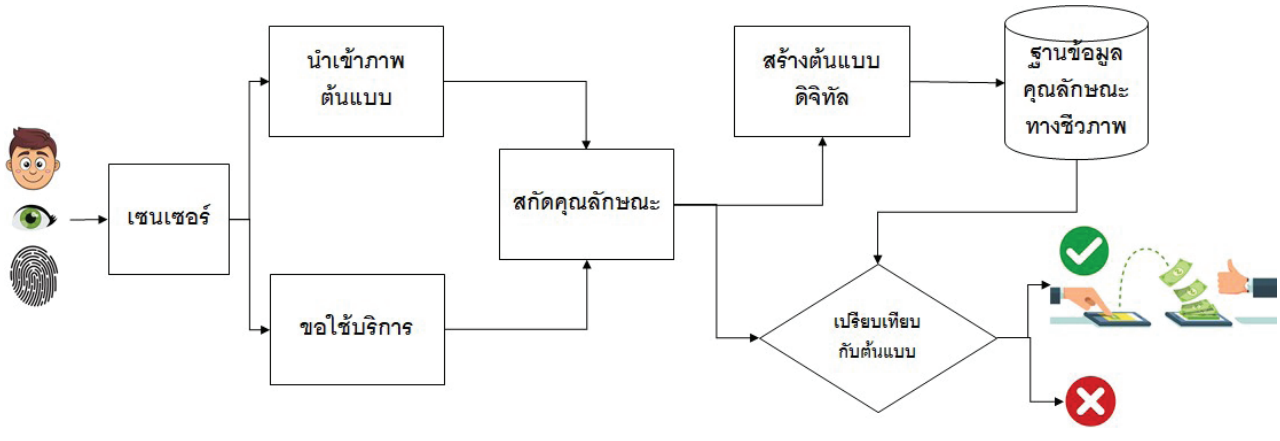

Figure 1 Biometric Authentication Process

Figure 1 แสดงตัวอย่างกระบวนการพิสูจน์ตัวตนด้วยไบโอเมตริกซ์แบบพื้นฐาน ที่ประกอบด้วย 3 ขั้นตอน: การลงทะเบียน การสกัดคุณลักษณะ และการยืนยันตัวตน ขั้นตอนแรกเป็นการนำเข้าไบโอเมตริกซ์ด้วยเซนเซอร์ เช่น ภาพดวงตา ลายนิ้วมือ หรือ ใบหน้าที่สมบูรณ์ของผู้ใช้ ข้อมูลนำเข้าจะถูกแปลงเป็นดิจิทัลเพื่อสกัดคุณลักษณะเฉพาะที่ไม่ซ้ำกันในผู้ใช้แต่ละราย เพื่อนำไปสร้างต้นแบบ (Template) จัดเก็บไว้ในฐานข้อมูล ในขั้นตอนที่ 2 ดังนั้นเมื่อผู้ใช้ต้องการเข้าถึงบริการ ผู้ใช้จะต้องยืนยันตัวตนด้วยไบโอเมตริกซ์ชนิดเดียวกันกับที่ลงทะเบียนไว้ ในขั้นตอนที่ 3 ข้อมูลนำเข้าจะถูกนำไปประมวลผลเพื่อสกัดคุณลักษณะเฉพาะมาเข้ากระบวนการพิสูจน์ตัวตนทำนองเดียวกับขั้นตอนการลงทะเบียน เพิ่มเติมคือข้อมูลที่รับเข้าจะถูกจับคู่เพื่อเปรียบเทียบกับต้นแบบที่จัดเก็บไว้ หากการจับคู่สำเร็จ หมายถึงผู้ใช้ผ่านการรับรองความถูกต้องและสามารถเข้าถึงบริการหรือทรัพยากรนั้นๆ (Zulfiqar, Syed, Khan, & Khurshid, 2019) โดยจะเน้นไบโอเมตริกซ์พื้นฐานในชีวิตประจำวัน ได้แก่ ลายนิ้วมือ ม่านตา และใบหน้า ซึ่งแต่ละคุณลักษณะล้วนมีคุณสมบัติเฉพาะที่แตกต่างและเหมาะสมกับการใช้งานในบริบทที่ต่างกัน (สุวิมล วงศ์สิงห์ทอง, 2565)

2. ลายนิ้วมือ (Fingerprint)

ลายนิ้วมือ เป็นคุณลักษณะที่นำมาใช้เพื่อพิสูจน์ตัวตนในหลายทศวรรษที่ผ่านมา แต่ยังคงได้รับความนิยมจากการใช้งานที่สะดวก อุปกรณ์รับภาพมีราคาถูก เป็นคุณลักษณะที่มีความเสถียร และให้ผลลัพธ์ที่มีความแม่นยำสูง โดยทั่วไปคุณลักษณะของลายนิ้วมือที่นำมาใช้ในการวิเคราะห์ ดังแสดงใน Figure 2 ประกอบด้วย สันลายนิ้วมือ (Ridge) ที่มีลักษณะเป็นเส้นนูนโค้ง สูงกว่าพื้นผิวของนิ้วมือ และร่องลายนิ้วมือ (Furrow) ที่มีลักษณะเป็นร่องสีขาวสลับอยู่ระหว่างสันลายนิ้วมือ ซึ่งการนำส่วนประกอบทั้งสองมาใช้ช่วยให้การบ่งชี้เจ้าของลายนิ้วมือเป็นไปอย่างถูกต้องแม่นยำ (Nguyen & Nguyen, 2019)

Figure 2 Fingerprint

3. ม่านตา (Iris)

ดวงตาของมนุษย์เปลี่ยนแปลงได้ตลอดเวลา ในขณะที่ม่านตาของบุคคลใดบุคคลหนึ่งจะไม่เปลี่ยนแปลง ภาพดวงตาที่สมบูรณ์ของมนุษย์ประกอบด้วยพื้นผิวของม่านตาที่เป็นวงกลมสีในดวงตา มีลักษณะคล้ายเครือข่ายที่ประกอบด้วยวงกลมและลวดลายรอบๆ มากมายมองเห็นได้ยาก ดังแสดงใน Figure 3 จึงนิยมใช้แสงอินฟราเรดที่มองไม่เห็นในเครื่องสแกนม่านตาเพื่อเพิ่มความสว่างให้ม่านตา ทำให้ภาพที่ได้มีความสมบูรณ์และเหมาะสมในการแปลงเป็นดิจิทัลยิ่งขึ้น สะดวกต่อการวัดรูปแบบเฉพาะของม่านตา และตรวจจับพื้นที่ของม่านตาเพื่อแยกขนตาและเปลือกตาออกจากดวงตา ผลลัพธ์สุดท้าย คือ ชุดของพิกเซลที่มีเพียงม่านตา ซึ่งข้อมูลนี้จะถูกนำเข้ากระบวนการจำแนกข้อมูล (Classification) เพื่อสร้างต้นแบบที่ประกอบด้วยคุณลักษณะเฉพาะของลวดลายเส้นและสี ของดวงตา (Marsico, Petrosino, & Ricciardi, 2016)

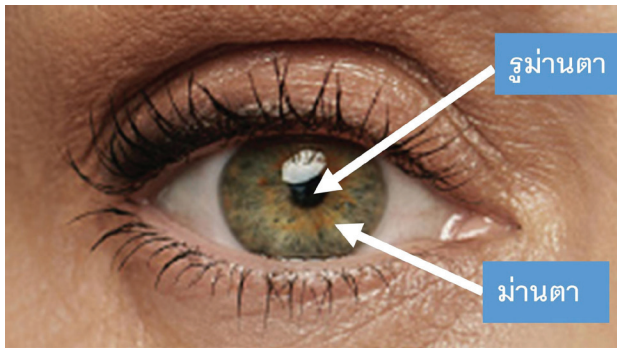

Figure 3 Iris

4. ใบหน้า (Face)

เทคโนโลยีการจดจำใบหน้าทำงานได้กับภาพทั้ง 2 มิติ และ 3 มิติ แต่การใช้ภาพ 2 มิติยังคงได้รับความนิยมมากกว่า ด้วยความรวดเร็วและความสะดวกในการจับคู่ระหว่างภาพถ่ายกับข้อมูล ซึ่งในขั้นตอนการพิสูจน์ตัวตนภาพใบหน้าทั้งกรณีเป็นภาพใบหน้าคนเดียวหรือเป็นกลุ่มจะถูกนำเข้าผ่านกล้อง เพื่อตรวจจับและระบุตำแหน่งที่ต้องการตรวจสอบ ดังแสดงใน Figure 4 จุดเน้น คือ ระยะห่างระหว่างดวงตา ความลึกของเบ้าตา ระยะห่างจากหน้าผากถึงคาง รูปร่างของโหนกแก้ม รูปร่างของริมฝีปาก หู และคาง หรือองค์ประกอบเพิ่มเติมอื่นๆ โดยกระบวนการพิสูจน์ตัวตนจะใช้วิธีอ่านรูปทรงใบหน้า เพื่อแยกแยะความแตกต่างระหว่างบุคคล หลังจากนั้นข้อมูลภาพจะถูกแปลงให้เป็นดิจิทัล แล้ววิเคราะห์ด้วยวิธีทางคณิตศาสตร์เพื่อเปรียบเทียบภาพที่ดิจิทัลที่ได้กับต้นแบบที่จัดเก็บในฐานข้อมูล (Marsico *et al.*, 2016)

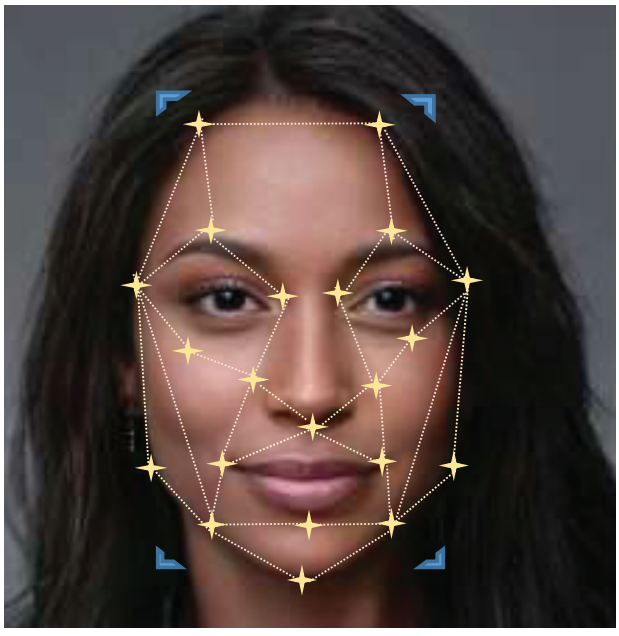

Figure 4 Face

ปัจจัยที่มีอิทธิพลต่อคุณภาพของไบโอเมตริกซ์

ตัวชี้วัดคุณภาพของต้นแบบไบโอเมตริกซ์มีความสำคัญต่อกระบวนการพิสูจน์ตัวตนอย่างมาก ทั้งในขั้นตอนการลงทะเบียนและการยืนยันตัวตน แม้ระบบพิสูจน์ตัวตนจะมีอัลกอริธึมที่มีประสิทธิภาพสูงเพียงไร แต่ยังคงมีความเสี่ยงจากปัจจัยภายนอกที่ยากต่อการควบคุม เป็นต้นว่า 1) ธรรมชาติของไบโอเมตริกซ์ เช่น ระหว่างจับภาพ ผู้ใช้มีพฤติกรรมหรือมีคุณลักษณะทางชีวภาพที่เปลี่ยนไป ทำให้คุณภาพของข้อมูลนำเข้าลดลง เช่น มีหนวด สวมหน้ากากอนามัย อยู่ในบริเวณที่มีแสงมาก หรือความเปลี่ยนแปลงที่เกิดจากปัจจัยที่ไม่อาจหลีกเลี่ยง เช่น อายุ ประเพณี เพศ และอาการบาดเจ็บ 2) ลักษณะการปฏิสัมพันธ์ระหว่างเซนเซอร์จับภาพกับผู้ใช้และข้อจำกัดในการปฏิบัติงาน เช่น ระยะในการสัมผัสไกลหรือใกล้เกินไป ทำให้ภาพที่รับเข้าแตกต่างไปจากต้นแบบ และ 3) สิ่งแวดล้อม เช่น อุณหภูมิ ความชื้น และพื้นหลัง

ปัจจัยเหล่านี้ล้วนมีอิทธิพลต่อคุณภาพของไบโอเมตริกซ์ และนำไปสู่ข้อจำกัดในการพยากรณ์ที่ใช้หลักการให้คะแนนความเสี่ยงที่สอดคล้องกับกฎ ซึ่งแนวทางการพัฒนาจำเป็นต้องใช้เทคนิคการเรียนรู้ของเครื่อง เพื่อให้คอมพิวเตอร์สามารถวิเคราะห์เชิงลึก หาความสัมพันธ์ ตีความ เรียนรู้และจดจำรูปแบบได้ด้วยประสบการณ์ที่เรียนรู้จากข้อมูลจำนวนมาก เพื่อนำไปปรับระบบให้รองรับประสบการณ์ใหม่อย่างอัตโนมัติ จึงเป็นความท้าทายในการบูรณาการการเรียนรู้ของเครื่องกับระบบพิสูจน์ตัวตนด้วยไบโอเมตริกซ์ เพราะกระบวนการนี้ช่วยลดอุปสรรคที่เกิดจากสภาพแวดล้อมที่มีปัญหา ไม่ว่าปัญหาของเซนเซอร์ หรือเสียงรบกวน ทั้งยังทำให้กระบวนการพิสูจน์ตัวตนด้วยไบโอเมตริกซ์มีความแม่นยำสูงขึ้น

การเรียนรู้ของเครื่อง (Machine Learning)

เป้าหมายหลักของการเรียนรู้ของเครื่อง คือ การทำให้คอมพิวเตอร์เรียนรู้ และปรับตนเองอย่างอัตโนมัติตามสถานการณ์โดยปราศจากการแทรกแซงหรือความช่วยเหลือจากมนุษย์เพื่อปรับแก้โปรแกรม (Fazala, *et al*, 2018) การเรียนรู้ของเครื่องจึงเป็นการประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence) ในการสร้างระบบเรียนรู้ของตัวเองจากข้อมูลจำนวนมากที่เป็นทั้งตัวอย่าง ประสบการณ์ หรือคำสั่งในการสอน เพื่อให้คอมพิวเตอร์สร้างแบบจำลอง (Model) ที่เข้าใจและรู้จำรูปแบบ (Pattern Recognition) ในข้อมูล เพื่อกำหนดรูปแบบ และความสัมพันธ์ของข้อมูลที่นำเข้า เพื่อให้คอมพิวเตอร์สามารถตัดสินใจหรือพยากรณ์ผลลัพธ์ตามหลักการทางสถิติหรือคณิตศาสตร์อย่างอัตโนมัติ ซึ่งแบบจำลองจะมีความสามารถในการปรับตนเองด้วยข้อมูลที่นำมาใช้สอนได้อย่างรวดเร็วในระดับเดียวกับการทำงานของสมองมนุษย์ และแนวทางการเรียนรู้ของเครื่องได้รับการพิสูจน์แล้วว่าช่วยลดอุปสรรคของระบบพิสูจน์ตัวตนแบบเดิมได้เป็นอย่างมาก (Matsumi, Nozaki, & Yoshikawa, 2018)

การสอน (Training) เครื่องให้เกิดการเรียนรู้มีหลายวิธี (Kantardzic, 2020) เป็นต้นว่า การเรียนรู้แบบมัลติทาสก์ (Multitask Learning) ที่เป็นพื้นฐานในการเรียนรู้แบบมีผู้สอน มักใช้วิธีปรับแบบจำลองให้เหมาะสมกับชุดข้อมูล เพื่อให้สามารถนำแบบจำลองไปใช้กับข้อมูลชุดอื่น และอีกวิธีที่ได้รับนิยมเช่นกัน คือ การถ่ายโอนการเรียนรู้ (Transfer Learning) เป็นการถ่ายโอนความรู้ที่เกิดจากการที่เครื่องเรียนรู้จากข้อมูลชุดหนึ่งแล้วนำผลที่ได้ไปตั้งต้นสำหรับการทำงานกับข้อมูลชุดอื่นที่มีลักษณะใกล้เคียงกัน วิธีนี้มีประโยชน์สำหรับการแก้ปัญหาที่สัมพันธ์กับข้อมูลจำนวนมากหรือข้อมูลขนาดใหญ่ (Big Data) เนื่องจากทำให้สามารถนำแบบจำลองที่มีอยู่ไปใช้ได้อย่างต่อเนื่อง ลดเวลาในการสอนเครื่องด้วยชุดข้อมูลใหม่ โดยสามารถกระบวนการเรียนรู้ของเครื่องเป็นประเภทหลัก (Mahdavinejad *et al.*, 2018) ได้ดังนี้

การเรียนรู้แบบไม่มีผู้สอน (Unsupervised learning) หมายถึง คอมพิวเตอร์มีอิสระในการค้นหารูปแบบที่ซ่อนอยู่ในข้อมูลเพื่อสร้างความเชื่อมโยงในการแยกแยะความเหมือนหรือความแตกต่างของข้อมูลด้วยตนเอง โดยไม่มีผลลัพธ์หรือตัวแปรเป้าหมาย วิธีการนี้นิยมใช้ในการจัดกลุ่มข้อมูลที่ยากต่อการตีความหรือยังไม่มีผู้ใดสามารถทำความเข้าใจข้อมูลได้ อัลกอริทึมในกลุ่ม ได้แก่ K-Nearest Neighbor (KNN), K-means, Hidden Markov Model (HMM), Density-based spatial clustering of applications with noise (DBSCAN) และ Principal Component Analysis (PCA)

การเรียนรู้แบบมีผู้สอน (Supervised learning) เป็นแนวทางในการสร้างปัญญาประดิษฐ์ การเรียนรู้วิธีนี้ต้องการ

การมีส่วนร่วมของมนุษย์อย่างต่อเนื่อง เนื่องจากคอมพิวเตอร์ต้องสอนและสร้างการเรียนรู้ให้แบบจำลอง เพื่อให้แบบจำลองสามารถตอบสนองและยืนยันผลได้อย่างถูกต้อง และเมื่อเวลาผ่านไปแบบจำลองจะสามารถปรับปรุงตัวเองให้จัดการกับชุดข้อมูลใหม่ตามรูปแบบที่ “เรียนรู้” ได้อย่างแม่นยำโดยอัตโนมัติ อัลกอริทึมของการเรียนรู้แบบมีผู้สอนนี้ เกิดจากการสอนให้คอมพิวเตอร์เรียนรู้จากข้อมูลที่มีการกำหนดค่า (Labeled) ซ้ำไปซ้ำมา จนสามารถตรวจจับรูปแบบและความสัมพันธ์ที่แฝงอยู่ระหว่างข้อมูลนำเข้าและกำหนดค่าให้ข้อมูลส่งออกได้อย่างแม่นยำเมื่อต้องทำงานกับข้อมูลใหม่ อัลกอริทึมในกลุ่มนี้ ได้แก่ Support Vector Machine (SVM), Decision Trees (DT), K-Nearest Neighbor (KNN) และ Random Forest (RF)

การทดสอบคุณภาพของผลลัพธ์ที่ผ่านการประมวลผลนิยมใช้มาตรวัดพื้นฐาน เป็นต้นว่า ความถูกต้อง (Accuracy) หมายถึง ร้อยละที่แบบจำลองการเรียนรู้ของเครื่องทำนายผลลัพธ์ได้ถูกต้อง, TP (True Positive) หมายถึง แบบจำลองทำนายว่าผลลัพธ์ถูกต้องและผลลัพธ์นั้นถูกต้อง, TN (True Negative) หมายถึง แบบจำลองทำนายผลลัพธ์ว่าไม่ถูกต้องและผลลัพธ์นั้นไม่ถูกต้อง, FP (False Positive) หมายถึง แบบจำลองทำนายว่าผลลัพธ์ถูกต้องแต่ผลลัพธ์นั้นไม่ถูกต้อง และ FN (False Negative) หมายถึง แบบจำลองทำนายว่าผลลัพธ์ไม่ถูกต้องแต่ผลลัพธ์นั้นถูกต้อง หรือในบางกรณีอาจใช้มาตรวัดอื่นเพิ่มเติม เช่น Average detection error rate ที่หมายถึงความผิดพลาดที่ตรวจสอบได้จากการทำงานของแบบจำลอง (Goodfellow, Bengio & Courville, 2022)

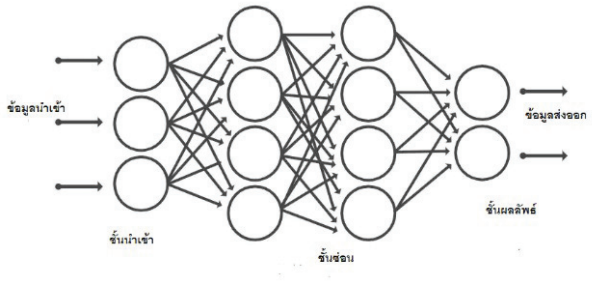

Figure 5 Deep Learning Model

แม้การเรียนรู้ของเครื่องแบบไม่มีผู้สอนและแบบมีผู้สอน เป็นเทคนิคการประมวลผลข้อมูลที่เพิ่มความแม่นยำให้กับการพิสูจน์ตัวตนด้วยไบโอเมตริกซ์ได้เป็นอย่างดี แต่การนำมาใช้กับอัตลักษณ์ดิจิทัลที่เป็นเสียง วิดีโอ หรือรูปภาพ การคัดเลือกลักษณะเฉพาะ (Feature) ที่เหมาะสมใช้เวลาและทรัพยากรค่อนข้างมาก ขณะที่แบบจำลองการเรียนรู้เชิงลึก (Deep Learning) ใช้เทคนิคการสร้างปัญญาประดิษฐ์ด้วยสถาปัตยกรรมโครงข่ายประสาทเทียมที่มีหลายชั้นเรียงซ้อนกันคล้ายตาข่ายของเซลล์ประสาทที่เชื่อมต่อกันในสมองมนุษย์ (Bock *et al.*, 2019) ประกอบด้วยชั้นสามระดับ ดังแสดงใน Figure 5 คือ ชั้นนำเข้า (Input Layer) ชั้นซ่อน (Hidden Layer) และชั้นผลลัพธ์ (Output Layer) แต่ละชั้นประกอบด้วยโหนดเซลล์ประสาทเทียมที่เชื่อมต่อถึงกัน ทำหน้าที่เป็นตาข่ายสามมิติ (Three Dimensional Network) ที่โหนดหนึ่งสามารถสื่อสารกับโหนดอื่นๆ ในบริเวณใกล้เคียง โดยชั้นนำเข้าข้อมูลจะรับข้อมูลเพื่อส่งไปประมวลผลที่ชั้นซ่อน และชั้นผลลัพธ์จะเป็นส่วนที่ตัดสินใจเกี่ยวกับข้อมูลผลลัพธ์ ทำให้แบบจำลองสร้างการเรียนรู้และปรับปรุงความแม่นยำของการพยากรณ์ได้ด้วยตัวเองด้วยการปรับน้ำหนักระหว่างโหนดในเครือข่าย ทำให้สามารถวิเคราะห์ได้แบบเรียลไทม์ โดยแบบจำลองจะคัดเลือกลักษณะเฉพาะที่ให้ผลลัพธ์ที่แม่นยำจากแต่ละภาพผ่านโครงข่ายประสาทเทียมที่เรียนรู้คุณลักษณะต่างๆ โดยตรงจากข้อมูลที่สอน ดังนั้นจึงลดภาระผู้เชี่ยวชาญในการแยกคุณลักษณะด้วยตนเอง (Yang, 2019)

การเรียนรู้เชิงลึก จึงเป็นแนวทางใหม่ที่ให้ความแม่นยำและประสิทธิภาพที่โดยเฉพาะอย่างยิ่งการทำงานกับข้อมูลที่ซับซ้อน เช่น เสียง รูปภาพ และวิดีโอ จึงเหมาะสมกับการพิสูจน์ตัวตนด้วยไบโอเมตริกซ์ (Charniak, 2018) ที่ทำให้คุณภาพของผลลัพธ์มีความแม่นยำกว่าการเรียนรู้ของเครื่องแบบพื้นฐาน (Bazrafkan, Thavalengal, & Corcoran, 2018) โดยแบบจำลองที่นิยมใช้ ได้แก่ Convolutional Neural Network (CNN), Fully Convolutional Deep Neural Network (FCDNN), Fully Convolutional Network (FCN) และ Multi-scale Convolutional Neural Network (MCNN) ในทางปฏิบัติการสอนแบบจำลองในกลุ่ม CNN ใช้เวลามาก เนื่องจากต้องใช้ข้อมูลขนาดใหญ่ในการสอน จึงนิยมใช้วิธีถ่ายโอนการเรียนรู้ ด้วยการนำแบบจำลองที่สอนไว้แล้วด้วยงานที่ใกล้เคียงกันมาใช้เป็นส่วนตั้งต้นของแบบจำลองใหม่ แล้วสอนเครื่องเพิ่มเติมด้วยข้อมูลในงานเฉพาะทาง (Manjunatha *et al.*, 2018)

การบูรณาการการเรียนรู้ของเครื่องเข้ากับ ระบบพิสูจน์ตัวตนด้วยไบโอเมตริกซ์

1. การจดจำลายนิ้วมือ (Fingerprint)

การจดจำลายนิ้วมือ เป็นแนวทางการรักษาความปลอดภัยที่มีการพัฒนาและแพร่หลายมากที่สุดในทางปฏิบัติ ลายนิ้วมือถูกนำไปใช้เป็นหลักฐานทางกฎหมายทั่วโลก ด้วยจุดเด่นที่มีการเปลี่ยนแปลงตามเวลาน้อย และง่ายต่อการใช้ จนลายนิ้วมือกลายเป็นมาตรฐานในการเข้าถึงอุปกรณ์ที่ใช้ในชีวิตประจำวันของผู้คนยุคดิจิทัลทั่วโลก ไม่ว่าเพื่อการใช้โทรศัพท์เคลื่อนที่ แท็บเล็ต และแม้แต่แล็ปท็อป ทั้งที่ทำงานหรือองค์กรล้วนนิยมนำเครื่องสแกนลายนิ้วมือไปใช้แทนรหัสผ่าน บัตรประจำตัว และรหัสเข้าประตู เพื่อประโยชน์ด้านความปลอดภัย ติดตามการเข้างาน และบริหารจัดการพนักงาน

แม้การจดจำลายนิ้วมือเป็นวิธีที่ให้ความปลอดภัยสูง และนิยมใช้ในหลายแพลตฟอร์ม แต่ยังเสี่ยงต่อการโจมตีเพราะปลอมแปลงได้ไม่ยากนัก จึงมีการนำเทคนิคต่างๆ มาใช้เพื่อเพิ่มประสิทธิภาพและความแม่นยำในการพิสูจน์ตัวตนด้วยลายนิ้วมือ ดังการศึกษาของ Tarare *et al.* (Tarare, Anjikar, & Turkar, 2015) ที่ใช้ภาพ 2 มิติของลายนิ้วมือไปประมวลผลด้วยกระบวนการแปลงเวฟเล็ตเต็มหน่วย (Discrete Wavelet Transform, DWT) เพื่อแปลงสัญญาณลายนิ้วมือจากฐานเวลา (Time Domain) เป็นฐานความถี่ (Frequency Domain) แล้วนำไปสกัดลักษณะเด่นของสัญญาณเพื่อจำแนกเพศผู้ใช้ โดยลักษณะเด่นที่ใช้ คือ ความหนาแน่นของลายนิ้วมือ และความถี่ของเส้นลายนิ้วมือ ที่เพศหญิงที่ค่าดังกล่าวสูงกว่าลายนิ้วมือของเพศชาย อัลกอริทึมการเรียนรู้ของเครื่องที่ใช้ คือ KNN และพบว่าแม้ลายนิ้วมือนำเข้าจะไม่ชัดเจน แต่ยังคงมี success rate ในการพยากรณ์ที่ 75% Nguyen, H.T., and Nguyen, L.T. (Nguyen & Nguyen, 2019) พัฒนาเทคนิคการจำแนกประเภท (Classification) ลายนิ้วมือด้วยเทคนิคการประมวลผลภาพ (Image Processing) ที่สามารถลดจำนวนครั้งในการเปรียบเทียบ ทำให้เวลาในการเปรียบเทียบลายนิ้วมือที่รับเข้าและลายนิ้วมือต้นแบบที่เก็บในฐานข้อมูลลดลง ทั้งยังเพิ่มคุณภาพของข้อมูลนำเข้า ทำให้กระบวนการสกัดคุณลักษณะ (Feature Extraction) ทำงานได้อย่างมีประสิทธิภาพ และพบว่าอัลกอริทึม RF ให้ค่าความถูกต้อง (accuracy) สูงกว่า 96.75% ขณะที่อัลกอริทึม SVM ให้ค่าความถูกต้อง (accuracy) สูงกว่า 95.5% Kim *et al.* (Kim, Cui, Kim, & Nguyen, 2019) แก้ปัญหาการจัดเก็บลายนิ้วมือเพื่อใช้ในการสอนเครื่องที่มีค่าใช้จ่ายสูง ใช้เวลามากในการจัดเตรียม และยังถูกควบคุมด้วยข้อจำกัดการคุ้มครองความเป็นส่วนตัว จึงใช้โครงข่ายประสาทแบบลึก (Deep Neural Network) สร้างฐานข้อมูลขนาดใหญ่ของลายนิ้วมือ เพื่อทดสอบการตรวจจับลายนิ้วมือปลอม และพบว่าข้อมูลที่สร้างขึ้นมีข้อผิดพลาดเฉลี่ยที่ตรวจพบ (average detection error rate) เพียง 1.57%

2. การจดจำใบหน้า (Face Recognition)

ในสามทศวรรษที่ผ่านมา เทคนิคการจดจำใบหน้าได้รับความนิยมเพิ่มขึ้นอย่างก้าวกระโดดในการใช้เพื่อเฝ้าระวัง ระบุอาชญากร ค้นหาบุคคลที่ สูญหาย โดยใช้วิธีเปรียบเทียบใบหน้าที่บันทึกในกล้องกับผู้ที่อยู่ในรายการเฝ้าระวัง ทำให้ระบบจดจำใบหน้าถูกใช้เป็นหนึ่งในมาตรการป้องกันการขโมยสินค้า การรักษาความปลอดภัยในสถานที่ที่ต้องการความปลอดภัยสูง เช่น ธนาคาร และสนามบิน เพราะหากมีอาชญากรปะปนมากับผู้โดยสารอาจก่อให้เกิดความเสี่ยงต่อทั้งสายการบินและผู้โดยสาร นอกจากนี้ยังนิยมนำมาใช้เพื่อควบคุมการเข้าอาคาร การเช็คอินในโรงแรม และการซื้อสินค้าออนไลน์ หรือนำไปเป็นคุณลักษณะเพิ่มเติมสำหรับการยืนยันตัวตน เพื่อเพิ่มความแม่นยำ โดยเทคนิคการจดจำใบหน้าที่น่าสนใจ ได้แก่ ผลการศึกษาของ Smith-Creasey *et al.* (Smith-Creasey, Albalooshib, & Rajarajana, 2018) ใช้เทคนิคการจดจำใบหน้าตามสัญญาณชีพ ด้วยการตรวจสอบใบหน้าแบบต่อเนื่องผ่านกล้องโทรศัพท์เคลื่อนที่ ใช้รูปถ่ายผู้ใช้ในหลายๆ กิจกรรม เช่น เดิน นั่ง และยืน เป็นข้อมูลตั้งต้นในการสอนโดยเครื่องจะตรวจสอบคุณลักษณะของผู้ใช้เป็นระยะ เพื่อตัดสิทธิการเข้าถึงอุปกรณ์ทันทีที่ตรวจสอบได้ว่ามีผู้แอบอ้าง ทั้งยังเป็นการลดปัญหาการปลอมแปลงใบหน้าด้วยภาพถ่าย (spoofing) การสกัดคุณลักษณะของใบหน้าใช้อัลกอริทึม SVM ให้ค่าความถูกต้อง (TRR) สูงสุดถึง 91.58% Bonazza *et al.* (Bonazza, Mitéran, Ginhac, & Dubois, 2018) เสนอแนวทางการลดปริมาณข้อมูลและเวลาที่ใช้ในการสอนเครื่อง โดยทดสอบความแตกต่างระหว่างการเรียนรู้ของเครื่องแบบดั้งเดิม (Classical Learning) และการเรียนรู้ของเครื่องแบบถ่ายโอน ด้วยแบบจำลอง RF พบว่าการเรียนรู้ของเครื่องแบบถ่ายโอน ช่วยลดเวลาในการสอนเครื่องและให้ค่าความถูกต้อง (accuracy) เพิ่มขึ้นเป็น 85% Phillips *et al.* (Phillips, Zou, Li, & Li, 2019) ใช้คุณลักษณะของม่านตามาบูรณาการกับการจดจำใบหน้า เพื่อการตรวจสอบสิทธิ์ผู้ใช้ พบว่าระบบพิสูจน์ตัวตนที่ออกแบบมีความถูกต้อง (accuracy) เพิ่มขึ้นเป็น 99.98% Zulfiqar *et al.* (Zulfiqar, Syed, Khan, & Khurshid, 2019) เพิ่มความแม่นยำการจดจำใบหน้า โดยทดสอบในบริเวณที่มีแสงสว่างแตกต่างกัน ผู้ใช้แสดงสีหน้าที่ต่างกัน ผู้ใช้มีรูปทรงใบหน้าที่เปลี่ยนไป ผู้ใช้สวมอุปกรณ์บดบังใบหน้า และผู้ใช้แสดงท่าทางที่แตกต่างกัน พบว่าการใช้แบบจำลองการเรียนรู้เชิงลึก (CNN) ช่วยให้ผลลัพธ์ที่ได้มีค่าความถูกต้อง (accuracy) สูงถึง 98.76%

3. การจดจำม่านตา (Iris Recognition)

เป็นที่ยอมรับกันว่าการพิสูจน์ตัวตนด้วย ม่านตา มีความเสถียรในระดับสูง แม้บุคคลที่มีพันธุกรรมเหมือนกัน พื้นผิวม่านตายังมีความแตกต่างกัน ทั้งยังเปลี่ยนแปลงตามอายุและสิ่งแวดล้อมน้อย ทว่าการตรวจสอบม่านตามีเงื่อนไขบางประการที่มีความจำเพาะเจาะจงมากกว่าคุณลักษณะทางชีวภาพอื่น และปัจจัยภายนอกที่มีผลกระทบต่อคุณภาพของม่านตาค่อนข้างมาก คือ ระยะห่างและมุมมองของการรับภาพ การยืนยันตัวตนด้วยม่านตาจึงต้องการความร่วมมือจากผู้ใช้อย่างมาก แต่แม้ผู้ใช้ให้ความร่วมมืออย่างครบถ้วนแล้ว ยังอาจต้องเผชิญปัญหาอื่น เช่น การบดบังของขนตา มุมในการอ่านภาพ การเคลื่อนไหวที่ทำให้ภาพไม่ชัดเจน แสงสะท้อนที่ผิดปกติจากดวงตา และสภาพแวดล้อมของแสงที่เปลี่ยนไป จึงควรหลีกเลี่ยงการใช้กล้อง near-infrared (NIR)

และไฟ near-infrared เพราะทำให้ยากต่อการแบ่งส่วนของตาและการกำหนดขอบเขตของม่านตา ซึ่งมีแนวทางการปรับปรุงคุณภาพและความถูกต้องของการจดจำม่านตาที่น่าสนใจ ดังนี้ Arsalan *et al.* (Arsalan *et al.*, 2017) เสนอวิธีการกำหนดขอบเขตของม่านตาให้แม่นยำในสถานการณ์ที่ยากต่อการควบคุม เช่น ผู้ใช้สวมแว่นสายตา มุมจับภาพไม่ถูกต้อง ผู้ใช้กรอกตาไปมา และเปิดตาบางส่วน โดยแบ่งออกเป็นสองขั้นตอน ขั้นตอนแรก คือ การกรองแบบ Bottom-hat เพื่อลบภาพส่วนที่ไม่ต้องการให้เหลือเฉพาะองค์ประกอบของโครงสร้างส่วนที่ต้องการ ขั้นตอนที่สอง ใช้แบบจำลอง CNN กำหนดขอบเขตม่านตาจากภาพดวงตาที่ได้จากขั้นตอนแรก โดยประมาณขอบเขตของรูม่านตาโดยใช้มาตรฐานของอัตราส่วนระหว่างการหดตัวและการขยายรูม่านตาเป็นเกณฑ์การพิจารณา เพื่อคำนวณพื้นที่จริงของม่านตา วิธีนี้ทำให้ average segmentation error ลดลงเหลือเพียง 0.0082 Bazrafkan *et al.* (Bazrafkan *et al.*, 2018) แก้ปัญหาข้อจำกัดของภาพม่านตาที่มีคุณภาพต่ำ โดยใช้แบบจำลอง FCDNN มาเพิ่มความแม่นยำในการคำนวณพื้นที่ม่านตา ทำให้ค่าความถูกต้อง (accuracy) เพิ่มขึ้นเป็น 96-99% สำหรับชุดข้อมูลทดสอบ Bath800, CASIA1000, UBIRIS, และ MobBio และเมื่อใช้แบบจำลองกับภาพที่มีคุณภาพระดับมาตรฐาน ค่าความถูกต้อง (accuracy) สูงสุดเพิ่มเป็น 99.30% Tobji *et al.* (Tobji, Di, & Ayoub, 2019) เตรียมข้อมูลม่านตาโดยวิธีถ่ายโอนการเรียนรู้จากระบบเดิม แล้วนำภาพที่มีความละเอียดสูงมาแยกออกเป็นส่วนย่อย เพื่อใช้แบบจำลอง FCN ตัดส่วนเฉพาะภาพม่านตาที่ต้องการ ส่งเข้าแบบจำลอง MCNN เพื่อสกัดคุณลักษณะเฉพาะของม่านตา จากนั้นนำข้อมูลมาจัดหมวดหมู่ โดยใช้แบบจำลอง FCN และ MCNN ผลที่ได้ให้ความถูกต้อง (accuracy) สูงถึง 99.41%

บทสรุป

ในกลุ่มของระบบพิสูจน์ตัวตนด้วยไบโอเมตริกซ์ พบว่าไบโอเมตริกซ์ที่ยอมรับมากที่สุด คือ ***ลายนิ้วมือ*** ด้วยจุดเด่นที่ลายนิ้วมือเป็นสรีระที่มนุษย์คุ้นเคย และมีความเป็นเอกลักษณ์เฉพาะจากลวดลายของเส้น สันและร่องบนพื้นผิวของนิ้วของบุคคลที่ต่างกัน แต่สิ่งที่น่ากังวล คือ เป็นไบโอเมตริกซ์ที่ง่ายต่อการทำซ้ำ แม้ข้อมูลที่จัดเก็บไว้จะผ่านการเข้ารหัส แต่ผู้ไม่ประสงค์ดียังสามารถสร้างภาพที่มีรูปแบบและลายเส้นคล้ายคลึงได้ เพราะมนุษย์อาจทิ้งรอยนิ้วมือไว้บนพื้นผิวที่สัมผัส แต่แม้ลายนิ้วมือจะมีจุดอ่อน การคาดเดาลายนิ้วมือก็ทำได้ยากกว่ารหัสผ่าน ทำให้ลายนิ้วมือเป็นหนึ่งในวิธีพิสูจน์ตัวตนที่พบบ่อยที่สุด ***การจดจำม่านตา*** เป็นเทคนิคที่มีความน่าเชื่อถือ มีความปลอดภัยในระดับสูงเนื่องจากเป็นวิธีการที่มีความละเอียด และมีโอกาสที่จะเกิดความผิดพลาดน้อยมากโดยเฉพาะหากใช้แสงอินฟราเรดในการแสกน ทั้งการทำซ้ำม่านตาก็ทำได้ยาก แต่ในทางปฏิบัติการพิสูจน์ตัวตนด้วยการแสกนม่านตา ยังได้รับการยอมรับในระดับปานกลาง ด้วยข้อกังวลด้านสุขอนามัยและการเข้าถึง เช่น หากผู้ใช้ต้องวางตาบนเบ้าตาของอุปกรณ์สแกนที่ใช้ร่วมกับผู้ใช้อื่น อาจเสี่ยงต่อสุขอนามัยโดยเฉพาะในสถานการณ์โรคระบาด ทั้งหากไม่สามารถปรับระดับเครื่องสแกนได้ย่อมเป็นเรื่องยากสำหรับคนที่มีส่วนสูงต่างกัน หรือหากผู้ใช้มีโรคประจำตัว เช่น โรคเบาหวาน อาจทำให้ลักษณะของดวงตาเปลี่ยนแปลงไปจนเกิดปัญหาในการจดจำม่านตา นอกจากนี้การกำหนดตำแหน่งของม่านตาผู้ใช้ให้ตรงกับกล้องยังมีความยุ่งยาก และอาจมีความผิดพลาดในการอ่านม่านตาจากระยะไกล ในขณะที่ ***การจดจำใบหน้า*** เป็นเทคโนโลยีใหม่ที่แก้ปัญหาการปลอมแปลงได้เป็นอย่างดี และได้รับการพิสูจน์ว่ามีประสิทธิภาพ เนื่องจากใช้การตรวจสอบใช้วิธีวิเคราะห์รูปร่าง และตำแหน่งของส่วนต่างๆ ของใบหน้ามาพิจารณาประกอบเพื่อสร้างเงื่อนไขการจับคู่ และเป็นเทคโนโลยีที่มีการพัฒนาอย่างรวดเร็วในช่วงไม่กี่ปีที่ผ่านมา จึงเป็นตัวเลือกที่ยอดเยี่ยมสำหรับการพิสูจน์ตัวตนระยะไกล จุดเด่นอีกประการคือ เทคโนโลยีนี้ง่ายต่อการสแกนฝูงชนเพื่อหาบุคคลต้องสงสัย ข้อเสียหลัก คือ เทคโนโลยีนี้เน้นที่ใบหน้าเป็นหลัก ทำให้ผู้ใช้ต้องมองตรงมาที่กล้องในมุมที่กำหนด เพื่อให้การทำงานเป็นไปอย่างถูกต้อง ทั้งรูปแบบการโจมตีในปัจจุบันมีการพัฒนาไปอย่างมาก ทำให้เห็นว่าระบบไบโอเมตริกซ์ยังต้องมีการพัฒนาให้มีความก้าวหน้าด้วยการบูรณาการกับเทคโนโลยีอื่น

การวิเคราะห์ข้อมูลไบโอเมตริกซ์ใช้หลักการประมวลผลรูปภาพที่นำเข้าผ่านกล้องมาแปลงเป็นข้อมูลดิจิทัล แล้วสกัดคุณลักษณะพิเศษเพื่อนำมาเปรียบเทียบกับคุณลักษณะพิเศษของข้อมูลต้นแบบที่สกัดในขั้นตอนการลงทะเบียน ความแม่นยำของระบบจึงขึ้นอยู่กับคุณภาพของข้อมูลนำเข้าและการควบคุมสภาวะแวดล้อมให้ปราศจากสัญญาณรบกวน อย่างไรก็ตามโดยธรรมชาติมักไม่สามารถหลีกเลี่ยงสัญญาณรบกวนชุดข้อมูลที่รวบรวมโดยเซนเซอร์รับภาพ ทำให้ความถูกต้องถูกลดทอนลงไป ดังนั้นการเพิ่มคุณภาพของสัญญาณนำเข้าเพื่อให้การประมวลผลเป็นไปอย่างแม่นยำในสถานการณ์ต่างๆ จึงเป็นสิ่งสำคัญ ดังมีการนำเทคโนโลยีการเรียนรู้ของเครื่องมาลดทอนข้อจำกัดเดิมๆ ของระบบพิสูจน์ตัวตน ด้วยจุดเด่นที่ผู้ใช้สามารถสร้างแบบจำลองในการประมวลผลภาพ (image processing) หาก แบบจำลองนั้นถูกสอนมาด้วยข้อมูลที่มีความหลากหลาย ครอบคลุมพฤติกรรมที่แตกต่างกันของผู้ใช้ และข้อมูลที่ใช้สอนมีปริมาณมากพอ แบบจำลองนั้นจะสามารถจำแนกรูปแบบ และหาแนวโน้มจากข้อมูลจำนวนมากเพื่อหาความสัมพันธ์ระหว่างตัวแปรได้เป็นอย่างดี ช่วยให้เครื่องเกิดการเรียนรู้และแยกแยะ

คุณลักษณะของผู้ใช้ได้อย่างถูกต้อง และวิเคราะห์ข้อมูลขนาดใหญ่ได้อย่างรวดเร็ว ปัญหาที่ตามมา คือ พื้นที่ในการจัดเก็บ เวลาและต้นทุนในการรวบรวมข้อมูล ตลอดจนทรัพยากรในการประมวลผลที่เพิ่มขึ้น ทำให้มีการทดลองเพื่อใช้ DNN สร้างฐานข้อมูลลายนิ้วมือเพื่อการสอนเครื่อง (Kim, Cui, Kim, & Nguyen, 2019) การกำหนดคุณลักษณะเพื่อลดเงื่อนไขในการทำงานของเครื่อง โดยใช้ความหนาแน่น และความถี่ของสันลายนิ้วมือมาเป็นคุณลักษณะพิเศษในการจำแนกเพศ (Tarare, Anjikar, & Turkar, 2015) และ การลดจำนวนครั้งในการเปรียบเทียบข้อมูลที่รับเข้าเพื่อลดเวลาในการประมวลผล (Nguyen & Nguyen, 2019) ทั้งยังมีความพยายามในการสอนเครื่องด้วยอริยบทที่หลากหลาย (Zulfiqar, Syed, Khan, & Khurshid, 2019) หรือการจับภาพใบหน้าอย่างต่อเนื่อง (Smith-Creasey, Albalooshib, & Rajarajana, 2018) เพื่อลดปัญหาการปลอมแปลงตัวตน การใช้เทคนิคการโอนย้ายข้อมูลเพื่อลดเวลาในการสอนเครื่อง (Bonazza, Mitéran, Ginhac, & Dubois, 2018; Tobji, Di, & Ayoub, 2019) หรือการใช้หลายคุณลักษณะมาบูรณาการเข้าด้วยกัน (Phillips, Zou, Li, & Li, 2019) หรือการใช้เทคนิคเพื่อปรับคุณภาพของข้อมูลนำเข้าในกรณีที่ข้อมูลมีคุณภาพต่ำ (Arsalan *et al.*, 2017; Bazrafkan *et al.*, 2018)

เทคนิคการเรียนรู้ของครื่องที่นำมาใช้ในการพิสูจน์ตัวตน ส่วนใหญ่เป็นการนำการเรียนรู้แบบไม่มีผู้สอนมาใช้ หากต้องการให้เครื่องพยากรณ์ผลลัพธ์ได้แม่นยำ ข้อมูลที่นำมาใช้สอนควรมีมีปริมาณมากพอ มีความถูกต้องสมบูรณ์ รองรับสถานการณ์ที่หลากหลาย และมีการกำหนดค่าผลลัพธ์ที่สอดคล้องกับข้อมูล เพื่อให้อุปสรรคอันเกิดจากพฤติกรรมของมนุษย์และสภาวะแวดล้อมมีผลต่อแบบจำลองน้อยที่สุด

เทคนิคการเรียนรู้แบบถ่ายโอนถูกนำมาใช้ในบางกรณีเพื่อลดเวลาในการเตรียมข้อมูล ขณะเดียวกันการศึกษาหลายชิ้นให้ความสำคัญกับการนำเทคนิคการเรียนรู้เชิงลึกมาใช้ระบบพิสูจน์ตัวตน ด้วยกระบวนการทำงานที่ใกล้เคียงกับกระบวนการคิดที่ปรับได้เองเช่นเดียวกับสมองมนุษย์ อย่างไรก็ตามเทคโนโลยีนี้ต้องการทรัพยากรสำหรับการวิเคราะห์และเปรียบเทียบข้อมูลที่มีประสิทธิภาพสูง ซึ่งอาจจำเป็นต้องใช้หน่วยประมวลผลกราฟิก (GPU) เพื่อออกแบบมาเพื่อเพิ่มความเร็วในการประมวลผลข้อมูลรูปภาพ มาช่วยในการคำนวณ หรืออาจใช้คอมพิวเตอร์ที่ประมวลผลแบบขนาน (Parallel Processing) มาเพิ่มความเร็วในการสืบค้นข้อมูลจากฐานข้อมูลที่มีขนาดใหญ่ ซึ่งผลการศึกษาล่าสุดแสดงให้เห็นว่าการใช้การเรียนรู้เชิงลึกช่วยลดความยุ่งยากให้กับผู้ใช้ในการคัดเลือกตัวแปรที่นำไปใช้ในการพยากรณ์ เพิ่มความถูกต้องของผลลัพธ์ มีศักยภาพในการรักษาความปลอดภัยแบบไบโอเมตริกซ์ได้สูง และเพิ่มความแข็งแกร่งในการโจมตีของผู้ไม่ประสงค์ดี ขณะเดียวกันในสถานการณ์ที่ต้องการความปลอดภัยที่สูงขึ้น ผู้ใช้ควรพิจารณาต่อว่า การใช้ปัจจัยในการพิสูจน์ตัวตนเพียงอย่างเดียวเช่น ลายนิ้วมือนั้นเพียงพอหรือไม่ หรือต้องใช้คุณลักษณะของสรีระมนุษย์หลายชนิดร่วมกัน เช่น เสียงและใบหน้า สัญญาณหัวใจและลายนิ้วมือหรืออื่นๆ ร่วมกัน เพิ่มเพื่อสร้างความแข็งแกร่งอย่างแท้จริง และคาดได้ว่าในอนาคตอันใกล้เทคโนโลยีการพิสูจน์ตัวตนด้วยไบโอเมตริกซ์จะยังคงมีความก้าวหน้าในการพัฒนาอย่างต่อเนื่อง และอาจถูกนำมาใช้เป็นมาตรฐานเบื้องต้นในการป้องกันโจร ผู้บุกรุก และบุคคลที่เป็นอันตราย

ข้อเสนอแนะ

แรงจูงใจหลักในการพิสูจน์ตัวตนด้วยไบโอเมตริกซ์ คือ ความถูกต้อง และความปลอดภัยจากการปลอมแปลงที่เพิ่มขึ้นในค่าใช้จ่ายที่ลดลง แม้ไบโอเมตริกซ์มีศักยภาพในการแก้ปัญหาการพิสูจน์ตัวตนได้ดี แต่การระบุตัวตนด้วยไบโอเมตริกซ์ยังมีความซับซ้อนจากปัจจัยต่างๆ ที่มีผลต่อความถูกต้องในทำงานของระบบ จากปัจจัยหลักด้านสภาพแวดล้อม ดังนั้นในบริบททั่วไปการจดจำลายนิ้วมืออาจเป็นตัวเลือกที่เหมาะในการใช้งานกับอุปกรณ์เคลื่อนที่ แต่อาจไม่ใช่ทางเลือกที่ดีที่สุดเมื่อต้องการระบุตัวตนจากระยะไกล ปัจจัยอื่นที่ต้องพิจารณาควบคู่เพื่อป้องกันการปลอมแปลงอัตลักษณ์ส่วนบุคคล คือ ในสภาวะแวดล้อมนั้นๆ คุณลักษณะใดของไบโอเมตริกซ์จะมีความเหมาะสมมากที่สุด ปัจจุบันยังคงไม่มีเทคโนโลยีการพิสูจน์ตัวตนด้วยไบโอเมตริกซ์ใดที่สมบูรณ์แบบ ทำให้มีการนำเทคนิคอื่นๆ มาปรับปรุงระบบเดิมเพื่อกำจัดจุดอ่อน เช่น การเรียนรู้ของเครื่อง การเรียนรู้เชิงลึก และคุณลักษณะทางชีวภาพมากกว่าหนึ่งคุณลักษณะมาบูรณาการ เพื่อลดจุดอ่อนของวิธีการเดิม และเพิ่มช่องทางการใช้ประโยชน์จากจุดแข็งของแต่ละวิธีการอย่างสร้างสรรค์ แต่แนวทางในการปรับปรุงประสิทธิภาพหรือการลดอัตราความผิดพลาดที่จะเกิดขึ้น ย่อมมีต้นทุน เช่น ทรัพยากรที่เพิ่มขึ้น และการทำงานที่ช้าลง ดังนั้นผู้ใช้จึงควรศึกษาข้อดีข้อเสียอย่างรอบคอบ ก่อนตัดสินใจใช้ระบบพิสูจน์ตัวตนด้วยไบโอเมตริกซ์ เพื่อให้มีความคุ้มค่าและสอดคล้องกับบริบทของตนมากที่สุด

เอกสารอ้างอิง

สุวิมล วงศ์สิงห์ทอง. (2565). *การบริหารความมั่นคงสารสนเทศ. มหาวิทยาลัยเกริก*. ศูนย์วิจัยและผลิตตำรา. มหาวิทยาลัยเกริก. 364 หน้า.

Ali, R. (2021). AI-enabled Decision Support System: Methodologies, Applications, and Advancements 2021. *Scientific Programming 2021*(Article ID 3225687). doi:https://doi.org/10.1155/2021/3225687

Arsalan, M., Hong, H. G., Naqvi, R. A., Lee, M. B., Kim, M. C., Kim, D. S., ... Park, K. R. (2017). Deep Learning-Based Iris Segmentation for Iris Recognition in Visible Light Environment. *Symmetry, 9*(263), 1-25. https://mdpi-res.com/d_attachment/symmetry/symmetry-09-00263/article_deploy/symmetry-09-00263.pdf?version=1509792574

Bazrafkan, S., Thavalengal, S., & Corcoran, P. (2018). An End to End Deep Neural Network for Iris Segmentation in Unconstraint Scenarios. *Neural Networks, 106*, 79-95. https://doi.org/10.1016/j.neunet.2018.06.011

Bock, F.E., Aydin, R.C., Cyron, C.J., Huber, N., Kalidindi, S.R., Klusemann, B. (2019). A Review of the Application of Machine Learning and Data Mining Approaches in Continuum Materials Mechanics. Sec. Computational Materials Science Front. Mater. 6:110. https://doi.org/10.3389/fmats.2019.00110

Bonazza, P., Mitéran, J., Ginhac, D., & Dubois, J. (2018). *PhD Forum : Machine Learning VS Transfer Learning Smart Camera Implementation for Face Authentication*. Paper presented at the ICDSC '18, September 3–4, 2018, Eindhoven, Netherlands. https://doi.org/10.1145/3243394.3243710

Charniak, E. (2018). *Introduction to Deep Learning,* The MIT Press Cambridge, Massachusetts London, England

Daugman J., 2004. How Iris Recognition Works.IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004

Fazala, M. I., Patela, M. E., Tyea, J., & Guptab, Y. (2018). The past, present and future role of artificial intelligence in imaging. *European Journal of Radiology, 105*, 246-250. https://doi.org/10.1016/j.ejrad.2018.06.020

Goodfellow, I., Bengio, Y., Courville, A. (2022). *Deep Learning (Adaptive Computation and Machine Learning series).* The MIT Press

Jayashree, R. (2020). *Analysis of Aadhaar Card Dataset Using Big Data Analytics*. In: Emerging Trends in Computing and Expert Technology. COMET 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 35. Springer, Cham. https://doi.org/10.1007/978-3-030-32150-5_123

Kantardzic, M. (2020). DATA MINING Concepts, Models, Methods, and Algorithms Third Edition, IEEE Press, Wiley

Kim, H., Cui, X., Kim, M.-G., & Nguyen, T. H. B. (2019). "*Fingerprint Generation and Presentation Attack Detection using Deep Neural Networks*," 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 2019, pp. 375-378, doi: 10.1109/MIPR.2019.00074.

Lardinois, F. (2021, October 27, 2021). Delta Air Lines partners with TSA PreCheck to launch biometrics-based bag drops. https://techcrunch.com/2021/10/27/delta-air-lines-partners-with-tsa-precheck-to-launch-biometrics-based-bag-drops/

Macdonald, A. (2022). Interpol program for fighting terrorism through biometrics deployed in Cameroon. *Biometric.Update.com*. https://www.biometricupdate.com/202201/interpol-program-for-fighting-terrorism-through-biometrics-deployed-in-cameroon

Mahdavinejad, M.S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., Sheth, A.P.(2018). Machine learning for internet of things data analysis: a survey. *Digital Communications and Networks*, p 161-175. https://doi.org/10.1016/j.dcan.2017.10.002

Marsico, M. D., Petrosino, A., & Ricciardi, S. (2016). Iris Recognition through Machine Learning Techniques: a Survey. *Pattern Recognition Letters*. https://doi:10.1016/j.patrec.2016.02.001

Manjunatha, V., Ramalingam, S., Marks, T., Davis, L. (2018). *Class Subset Selection for Transfer Learning using Submodularity*. https://arXiv:1804.00060v1 [cs.CV] 30 Mar 2018

Matsumi, S., Nozaki, Y., Yoshikawa, M. (2018). Feature Extraction Driven Modeling Attack Against Double Arbiter PUF and Its Evaluation, AICCC '18, December 21–23, 2018, Tokyo, Japan. DOI: https://doi.org/10.1145/3299819.3299835

Nguyen, H. T., & Nguyen, L. T. (2019). Fingerprints Classification through Image Analysis and Machine Learning Method. https://doi.org/10.3390/a12110241

Noh, N. S. M., Jaafar, H., Mustafa, W. A., Idrus, S. Z. S., & Mazelan, A. H. (2020). Smart Home with Biometric System Recognition. *Journal of Physics: Conference Series, 1529 042020*. doi:10.1088/1742-6596/1529/4/042020

Phillips, T., Zou, X., Li, F., & Li, N. (2019). *Enhancing Biometric-Capsule-based Authentication and Facial Recognition via Deep Learning*. Paper presented at the the 24th ACM Symposium,SACMAT '19, June 3–6, 2019, 141-146, Toronto, ON, Canada. https://doi.org/10.1145/3322431.3325417

Seffers, G. I. (2020). FBI Upgrades Biometric Technologies. *Signal*. doi:https://www.afcea.org/content/fbi-upgrades-biometric-technologies

Seven Bank, L. (2019). Introducing a Next-generation ATM with face recognition and QR code reader. https://www.sevenbank.co.jp/english/ir/pdf/2019/20190912_E1.pdf

Shepard, S. (2016). Dallas Area Rapid Transit to Increase Security with Cameras. *Security Today*. doi:https://securitytoday.com/articles/2016/02/19/dallas-area-rapid-transit-to-increase-security-with-cameras.aspx?admgarea=ht.networkcentric&m=1

Smith-Creasey, M., Albalooshib, F. A., & Rajarajana, M. (2018). Continuous face authentication scheme for mobile devices with tracking and liveness detection. *Microprocessors and Microsystems, 63*, 147-157. https://doi.org/10.1016/j.micpro.2018.07.008

Tarare, S., Anjikar, A., & Turkar, H. (2015). *Fingerprint Based Gender Classification Using DWT Transform*. 2015 International Conference on Computing and Communication Control and Automation. February 26 - 27, 2015. Pune, India. doi: 10.1109/ICCUBEA.2015.141

Tobji, R., Di, W., & Ayoub, N. (2019). FMnet: Iris Segmentation and Recognition by Using Fully and Multi-Scale CNN for Biometric Security. *Applied Sciences, 9*(2042), 1-17. https://mdpi-res.com/d_attachment/applsci/applsci-09-02042/article_deploy/applsci-09-02042.pdf?version=1558088546

Yang, X-S .(2019). *Introduction to Algorithms for Data Mining and Machine Learning*. Academic Press. United Kingdom

Zulfiqar, M., Syed, F., Khan, M. J., & Khurshid, K. (2019). *Deep Face Recognition for Biometric Authentication*. Proceeding of the 1st International Conference on Electrical, Communication and Computer Engineering (ICECCE), 24-25 July 2019, Swat, Pakistan. https://doi.org/10.1109/ICECCE47252.2019.8940725