



สวทช
NSTDA



โครงการ เปิดล็อกเกอร์ด้วยระบบสแกนใบหน้า OPEN THE LOCKER WITH FACE SCAN SYSTEM

เสนอมูลนิธิเทคโนโลยีสารสนเทศตามพระราชดำริ
สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี

โดย

นางสาวศุภาพิชญ์ ชุมผล
นางสาวกนกวรรณ อักษรกุล

โรงเรียนราชประชานุเคราะห์ ๑๙ จังหวัดนครศรีธรรมราช
สำนักบริหารงานการศึกษาพิเศษ
สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
กระทรวงศึกษาธิการ

ชื่อโครงการ เปิดล็อกเกอร์ด้วยระบบสแกนใบหน้า

Open the locker with face scan system

ประเภทโครงการ โครงการสิ่งประดิษฐ์เพื่อพัฒนาคุณภาพชีวิตและชุมชน

ผู้จัดทำ

1. นางสาว ศุภาพิชญ์ ชุมผล ระดับชั้น มัธยมศึกษาปีที่ 4
Email : am0854757627@gmail.com
2. นางสาว กนกวรรณ อักษรกุล ระดับชั้น มัธยมศึกษาปีที่ 4
Email kanokwanaksonkoon@ gmail.com

ครูที่ปรึกษา

1. นางสาวอาริษา มะ
2. นางสาวจันทร์รัตน์ ยงเอื้องคง

บทคัดย่อ

การเปิดล็อกเกอร์ด้วยระบบสแกนใบหน้าเป็นเทคโนโลยีที่ใช้การตรวจสอบลักษณะใบหน้าเพื่อยืนยันตัวตนของผู้ใช้ ระบบนี้ช่วยเพิ่มความสะดวกสบายและความปลอดภัยในการใช้งานล็อกเกอร์ โดยไม่จำเป็นต้องใช้กุญแจหรือรหัสผ่าน ซึ่งมีความเสี่ยงในการสูญหายหรือถูกขโมย การใช้เทคโนโลยีสแกนใบหน้าไม่เพียงแต่ช่วยให้การเข้าถึงข้อมูลหรือพื้นที่ต่าง ๆ เป็นไปอย่างรวดเร็วและแม่นยำ แต่ยังช่วยลดความเสี่ยงในการเข้าถึงของผู้ที่ไม่พึงประสงค์ ด้วยการใส่ระบบที่มีความปลอดภัยสูงและสามารถตรวจจับใบหน้าของผู้ใช้งานได้อย่างมีประสิทธิภาพ

คำสำคัญ ล็อกเกอร์ (locker), สแกนใบหน้า (face scan), ปลอดภัย (safe)

บทนำ

ในปัจจุบัน เทคโนโลยีการสแกนใบหน้ากำลังได้รับความนิยมในหลาย ๆ ด้าน ทั้งในเรื่องของความปลอดภัยและการเข้าถึงข้อมูลที่มีความสำคัญ โดยเฉพาะในระบบล็อกเกอร์ที่ต้องการการยืนยันตัวตนเพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต การเปิดล็อกเกอร์ด้วยระบบสแกนใบหน้าเป็นการนำเทคโนโลยีนี้มาประยุกต์ใช้เพื่อเพิ่มความปลอดภัยในการใช้งาน ระบบดังกล่าวสามารถตรวจสอบและยืนยันตัวตนของผู้ใช้ได้อย่างรวดเร็ว โดยไม่ต้องพึ่งพากุญแจหรือรหัสผ่าน ซึ่งมีความเสี่ยงในการสูญหายหรือถูกขโมย การใช้ระบบสแกนใบหน้าไม่เพียงแต่ทำให้การเปิดล็อกเกอร์มีความปลอดภัยสูง แต่ยังสามารถเพิ่มความสะดวกในการใช้งานและลดความยุ่งยากในการจัดการรหัสหรือกุญแจต่าง ๆ ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์

1. เพื่อพัฒนาระบบเปิดล็อกเกอร์ด้วยการสแกนใบหน้า ซึ่งสามารถยืนยันตัวตนของผู้ใช้ได้อย่างปลอดภัย
2. เพื่อลดความเสี่ยงจากการสูญหายหรือถูกขโมยของกุญแจหรือรหัสผ่านที่ใช้ในการเปิดล็อกเกอร์
3. เพื่อเพิ่มความสะดวกในการใช้งานและลดขั้นตอนที่ซับซ้อนในการเปิดล็อกเกอร์
4. เพื่อเสริมสร้างระบบรักษาความปลอดภัยในการเข้าถึงข้อมูลหรือทรัพย์สินที่อยู่ภายในล็อกเกอร์

ขอบเขตการวิจัย

1. ขอบเขตด้านเทคโนโลยีและการประมวลผลระบบสแกนใบหน้า

ศึกษาความแม่นยำและประสิทธิภาพของเทคโนโลยีการสแกนใบหน้าด้วยเครื่องมือ การประเมินผลการตรวจจับใบหน้าในสภาพแวดล้อมต่าง ๆ เช่น แสงสว่างน้อย, มุมของใบหน้า
2. ขอบเขตการทดสอบผู้ใช้ที่สวมแว่นตาหรือหมวก

ปัญหาที่อาจเกิดขึ้น : การสำรวจปัญหาที่ผู้ใช้พบ เช่น ความล้มเหลวในการเปิดล็อกเกอร์หรือการไม่สามารถสแกนใบหน้าได้
3. ขอบเขตด้านความปลอดภัยและความเป็นส่วนตัว

การปกป้องข้อมูลใบหน้า : การศึกษาเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล เช่น การจัดเก็บและเข้ารหัสข้อมูลใบหน้าในระบบ
4. ขอบเขตด้านการทดสอบระบบ

การทดสอบประสิทธิภาพของระบบ : การทดสอบประสิทธิภาพของระบบในด้านต่าง ๆ เช่น เวลาในการตรวจจับใบหน้า, ความแม่นยำในการเปิดล็อกเกอร์
5. การทดสอบในสถานการณ์จริง

การทดสอบระบบในสภาพแวดล้อมจริง เช่น โรงเรียน, ฟิตเนส, หรือสถานที่เก็บของ

การทบทวนวรรณกรรม

การทบทวนวรรณกรรม (Literature Review) เกี่ยวกับ ระบบเปิดล็อกเกอร์ด้วยการสแกนใบหน้า มีความสำคัญในการศึกษาความรู้พื้นฐานและความก้าวหน้าของเทคโนโลยีที่เกี่ยวข้อง เพื่อสร้างความเข้าใจในกระบวนการและความท้าทายที่เกี่ยวข้องในการพัฒนาระบบดังกล่าว รวมถึงการประยุกต์ใช้เทคโนโลยีการจดจำใบหน้าในหลากหลายแวดวง เช่น การรักษาความปลอดภัย การยืนยันตัวตน และการเข้าถึงระบบต่าง ๆ

1. เทคโนโลยีการจดจำใบหน้า (Face Recognition Technology) การจดจำใบหน้าคือกระบวนการทางคณิตศาสตร์ที่ใช้ในการวิเคราะห์ลักษณะเฉพาะของใบหน้ามนุษย์เพื่อยืนยันตัวตน ระบบการจดจำใบหน้า มักจะถูกใช้ในหลายแอปพลิเคชัน เช่น การรักษาความปลอดภัยของอุปกรณ์มือถือ การตรวจสอบตัวตนในอุตสาหกรรมการเงิน และการควบคุมการเข้าถึงในสถานที่ต่าง ๆ

2. การใช้เทคโนโลยีในระบบการเปิดล็อกเกอร์ ที่ใช้การจดจำใบหน้ามีความสำคัญในหลายแง่มุม โดยเฉพาะในเรื่องความสะดวกสบายในการใช้งานและความปลอดภัย ระบบนี้สามารถใช้ในหลายสถานที่ เช่น การเข้าถึงห้องส่วนตัว ล็อกเกอร์ในโรงเรียน หรือห้องที่มีความลับสำคัญในองค์กร

- การใช้ Arduino ในการพัฒนาระบบที่สามารถควบคุมการเปิดล็อกเกอร์ผ่านคำสั่งจากโปรแกรมที่ทำงานบน Arduino ซึ่งเชื่อมต่อกับระบบจดจำใบหน้าเพื่อเปิดล็อกเกอร์โดยอัตโนมัติเมื่อยืนยันตัวตนสำเร็จ

- การประมวลผลภาพแบบเรียลไทม์: การใช้ระบบการจดจำใบหน้าสำหรับการปลดล็อกล็อกเกอร์ต้องใช้การประมวลผลภาพแบบเรียลไทม์ เพื่อให้การยืนยันตัวตนทำได้ทันที Pixcobox เป็นเครื่องมือที่มีความสามารถในการจับภาพจากกล้อง Webcam และตรวจสอบใบหน้าได้อย่างรวดเร็ว ระบบดังกล่าวช่วยลดเวลาในการเข้าถึงและเพิ่มความความสะดวกสบายให้แก่ผู้ใช้งาน

3. ปัญหาและข้อจำกัดของการใช้ระบบจดจำใบหน้า แม้ว่าเทคโนโลยีการจดจำใบหน้าจะมีความสะดวกและปลอดภัยสูง แต่ก็ยังมีข้อจำกัดที่อาจเป็นอุปสรรคในการใช้งาน:

- สภาพแสงและมุมมอง: ระบบการจดจำใบหน้าอาจมีปัญหาหากสภาพแสงไม่เหมาะสม เช่น ในที่มีมืดหรือมีแสงจ้าเกินไป หรือถ้าผู้ใช้งานอยู่ในมุมมองที่ไม่เหมาะสมจากกล้อง .

- การปลอมแปลงใบหน้า: ระบบจดจำใบหน้าอาจมีความเสี่ยงจากการใช้ภาพถ่ายหรือวิดีโอปลอมแปลงเพื่อหลอกระบบให้รับรู้ว่า เป็นใบหน้าของผู้ใช้ . ปัญหานี้สามารถลดลงได้ด้วยการใช้เทคโนโลยี 3D Face Recognition หรือการใช้เทคนิคอื่นๆ เพื่อเพิ่มความปลอดภัย

- ความแม่นยำของระบบ: แม้ว่า LBPH และ CNN จะมีความแม่นยำสูงในหลายกรณี แต่การใช้งานในสถานการณ์ที่ซับซ้อน เช่น การเปลี่ยนแปลงลักษณะใบหน้าหรือการมีเครื่องประดับที่ปิดบังใบหน้า (เช่น แว่นตา หรือหมวก) อาจทำให้ระบบตรวจจับใบหน้าได้ยากขึ้น

4. การประยุกต์ใช้งานในอนาคต ระบบเปิดล็อกเกอร์ที่ใช้การจดจำใบหน้าอาจขยายการใช้งานไปในหลายๆ ด้าน เช่น:

- การใช้งานในบ้านและสำนักงาน ระบบที่สามารถใช้สำหรับเปิดประตูหรือพื้นที่ต่าง ๆ ในบ้านหรือสำนักงาน โดยไม่ต้องใช้กุญแจหรือรหัสผ่าน

- การรวมกับเทคโนโลยีการยืนยันตัวตนหลายรูปแบบ (Multimodal Authentication) โดยการใช้เทคนิคหลาย ๆ อย่าง เช่น การจดจำใบหน้าและการสแกนลายนิ้วมือ เพื่อเพิ่มความปลอดภัย
- การใช้เทคโนโลยี 3D Face Recognition: เพื่อเพิ่มความแม่นยำในการตรวจจับใบหน้าในมุมที่หลากหลายและในสภาพแสงที่เปลี่ยนแปลง

จากการทบทวนวรรณกรรมเกี่ยวกับการใช้ระบบสแกนใบหน้าในการเปิดล็อกเกอร์ พบว่าเทคโนโลยีการจดจำใบหน้ามีความแม่นยำและสะดวกสบายในการใช้งาน แต่ก็ยังมีข้อจำกัดที่ต้องพัฒนาเพิ่มเติม เช่น การปรับปรุงการทำงานในสภาพแสงและมุมมองต่าง ๆ รวมถึงการใช้เทคโนโลยีเสริมเพื่อเพิ่มความปลอดภัยในระบบ นอกจากนี้ การใช้งานร่วมกับ **Arduino** ช่วยลดต้นทุนในการพัฒนาและทำให้การใช้งานง่ายขึ้น

วิธีดำเนินการวิจัย

- 1) การศึกษาทฤษฎีและแนวทางการวิจัยที่เกี่ยวข้องเริ่มต้นด้วยการศึกษางานวิจัยและเอกสารที่เกี่ยวข้องกับระบบสแกนใบหน้าและการใช้งานในระบบล็อกเกอร์ รวมถึงการศึกษาความปลอดภัยของเทคโนโลยีนี้และข้อดีข้อเสียที่อาจเกิดขึ้นจากการใช้งาน
- 2) การเลือกและออกแบบระบบการสแกนใบหน้าเลือกเทคโนโลยีที่เหมาะสมสำหรับการสแกนใบหน้า เช่น ระบบที่ใช้ AI หรือ Machine Learning ในการตรวจจับและยืนยันใบหน้า จากนั้นทำการออกแบบและตั้งค่าระบบให้สามารถใช้งานได้ในสถานการณ์จริง
- 3) การทดสอบและประเมินผลการทำงานของระบบดำเนินการทดสอบระบบสแกนใบหน้าในสถานการณ์ต่าง ๆ เช่น การทดสอบความแม่นยำในการสแกนใบหน้า, เวลาในการยืนยันตัวตน, และความสามารถในการป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต
- 4) การเก็บข้อมูลและการวิเคราะห์ผลเก็บข้อมูลจากการทดสอบการใช้งานระบบจากกลุ่มผู้ทดลอง (ผู้ใช้งาน) และวิเคราะห์ผลการทำงานของระบบ เช่น ความแม่นยำในการตรวจสอบใบหน้าและความสะดวกในการใช้งาน
- 5) การสรุปผลการวิจัยและข้อเสนอแนะวิเคราะห์ผลการทดสอบและประเมินประสิทธิภาพของระบบสแกนใบหน้า จากนั้นสรุปผลการวิจัยและนำเสนอข้อเสนอแนะสำหรับการปรับปรุงระบบเพื่อเพิ่มประสิทธิภาพและความปลอดภัยในการใช้งาน
- 6) การจัดทำรายงานวิจัยสุดท้าย รวบรวมข้อมูลและสรุปผลทั้งหมดในรูปแบบของรายงานวิจัย เพื่อเผยแพร่ให้กับผู้ที่สนใจและนำไปใช้ประโยชน์ต่อไป

ผลการวิจัย

ผลการวิจัยพบว่า OpenCV และ Pixcobox เป็นเครื่องมือที่สามารถนำมาประยุกต์ใช้ในการจับภาพใบหน้าและประมวลผลภาพได้อย่างมีประสิทธิภาพ โดยเฉพาะในการใช้ฟังก์ชัน Haar Cascade Classifier ที่เป็นอัลกอริธึมในการตรวจจับใบหน้าในภาพ โดยมีข้อดีที่สามารถทำงานได้รวดเร็วและแม่นยำในสภาพแสงปกติการเก็บข้อมูลใบหน้าเป็นขั้นตอนที่สำคัญที่สุดในการสร้างระบบจดจำใบหน้า โดยฐานข้อมูลจะต้องมีภาพใบหน้าของผู้ใช้เพื่อให้ระบบสามารถเรียนรู้และตรวจจับใบหน้าได้อย่างแม่นยำในทุกสภาพแสงและมุมมอง โดยการเก็บภาพใบหน้าในสภาพแสงต่าง ๆ และมุมต่าง ๆ จะช่วยเพิ่มความแม่นยำในการตรวจจับใบหน้าของผู้ใช้งานอย่างไรก็ตาม ข้อจำกัดของการเก็บข้อมูลใบหน้าคือต้องมีการถ่ายภาพใบหน้าผู้ใช้งานหลากหลายมุมมองและในหลาย ๆ สถานการณ์เพื่อให้การจดจำใบหน้ามีประสิทธิภาพสูงสุด การเก็บข้อมูลแบบนี้จะต้องใช้เวลาและทรัพยากรในการดำเนินการระบบการเปิดล็อกเกอร์ด้วยการสแกนใบหน้ามีประสิทธิภาพที่ดีในกรณีที่ผู้ใช้สามารถยืนยันในตำแหน่งที่เหมาะสมและในสภาพแสงที่ไม่เพียงพอ โดยเฉพาะในสภาพแสงที่ไม่ต่ำหรือสูงเกินไป ระบบสามารถจดจำใบหน้าได้ภายในเวลาไม่กี่วินาที และสามารถเปิดล็อกเกอร์ได้ทันทีหลังจากยืนยันตัวตนระบบการเปิดล็อกเกอร์ด้วยการสแกนใบหน้าให้ความปลอดภัยสูง เนื่องจากการใช้ใบหน้าของแต่ละบุคคลที่เป็นเอกลักษณ์ ซึ่งยากที่จะปลอมแปลงหรือคัดลอก การจดจำใบหน้าช่วยลดปัญหาที่เกิดจากการลืมรหัสผ่านหรือการใช้กุญแจที่สามารถสูญหายได้อย่างไรก็ตาม การใช้ใบหน้าในการยืนยันตัวตนยังคงมีความเสี่ยงหากมีการโจมตีจากเทคโนโลยีการปลอมแปลงใบหน้า เช่น การใช้ภาพถ่ายหรือวิดีโอในการหลอกหลวงระบบ ในการวิจัยพบว่า เทคโนโลยี 3D Face Recognition หรือการตรวจจับการเคลื่อนไหวของใบหน้าจะช่วยเพิ่มความปลอดภัยได้มากขึ้น

ข้อดี: ระบบสามารถทำงานได้รวดเร็วในสภาพแสงที่เหมาะสมและไม่ต้องการอุปกรณ์เสริมเช่นกุญแจหรือรหัสผ่าน

ข้อจำกัด: ระบบอาจมีความล้มเหลวในการจดจำใบหน้าในสภาพแสงที่ไม่เพียงพอหรือใบหน้าที่มีการเปลี่ยนแปลง (เช่น การใส่แว่นตาหรือหมวก)

สรุปผลการวิจัย และอภิปรายผล

1. ประสิทธิภาพของการจดจำใบหน้า

- ระบบสามารถตรวจจับใบหน้าได้แม่นยำในสภาพแสงที่เหมาะสม โดยใช้เทคนิค Haar Cascade Classifier ในการตรวจจับใบหน้า

- เมื่อมีการเก็บภาพใบหน้าผู้ใช้งานหลายมุมมองและสภาพแสง ระบบสามารถจดจำใบหน้าได้อย่างมีประสิทธิภาพในส่วนใหญ่

- การใช้ LBPH Face Recognizer หรือ Deep Learning Models (CNN) ช่วยเพิ่มความแม่นยำในการจดจำใบหน้าและลดอัตราความผิดพลาด

2. การเก็บข้อมูลใบหน้าและความปลอดภัย

- ฐานข้อมูลใบหน้าของผู้ใช้มีความสำคัญในการสร้างระบบที่มีความปลอดภัยสูง การเก็บภาพใบหน้าในหลายมุมมองช่วยให้ระบบทำงานได้แม่นยำในสถานการณ์ต่าง ๆ

- ความปลอดภัยสูงขึ้นเนื่องจากการใช้ใบหน้าที่เป็นเอกลักษณ์ แต่ยังคงมีช่องโหว่จากการปลอมแปลงใบหน้า

3. การควบคุมระบบล็อกเกอร์

- ระบบเปิดล็อกเกอร์ทำงานได้ดีโดยการเชื่อมต่อกับ Arduino ซึ่งส่งคำสั่งเปิดล็อกเกอร์ผ่าน Serial Communication

- การใช้ระบบนี้ไม่ต้องการการใช้กุญแจหรือรหัสผ่าน ช่วยเพิ่มความสะดวกสบายและลดความเสี่ยงจากการลืมรหัสหรือการสูญหายของกุญแจ

4. ข้อจำกัดและปัญหาที่พบ

- ปัญหาที่พบในระบบคือการที่ระบบไม่สามารถทำงานได้ดีในสภาพแสงที่ไม่เหมาะสมหรือเมื่อใบหน้าผู้ใช้งานเปลี่ยนแปลงอย่างเห็นได้ชัด (เช่น การสวมแว่นตาหรือหมวก)

- ความแม่นยำอาจลดลงหากผู้ใช้ยืนห่างจากกล้องหรือมีการเคลื่อนไหวอย่างรวดเร็ว

ข้อดีของระบบ

- ระบบที่ใช้การสแกนใบหน้าที่มีความสะดวกในการใช้งาน เนื่องจากผู้ใช้ไม่ต้องจำรหัสผ่านหรือพกพากุญแจ

- ระบบมีความปลอดภัยสูง เนื่องจากการใช้ใบหน้าที่เป็นเอกลักษณ์ของแต่ละบุคคลการประมวลผลภาพด้วยเครื่องมือ

ข้อจำกัด

- ความแม่นยำในการจดจำใบหน้าอาจลดลงในบางกรณี เช่น สภาพแสงไม่เหมาะสม หรือผู้ใช้มีการเปลี่ยนแปลงลักษณะใบหน้า (เช่น ใส่แว่นตาหรือหมวก)

ข้อเสนอแนะ

-

เอกสารอ้างอิง

- Jain, A. K., & Li, S. Z. (2005). Handbook of Face Recognition. Springer.
- Kumar, A., & Mahajan, A. (2017). Face recognition using deep learning techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 7(2), 7-14.
- Zhao, W., Chellappa, R., & Phillips, P. J. (2003). Face recognition: A literature survey. ACM Computing Surveys (CSUR), 35(4), 399-458.

ภาคผนวก

อุปกรณ์อิเล็กทรอนิกส์ที่ใช้

ลำดับ	รายการ	จำนวนตัว/ชุด
1	บอร์ด Arduino	1
2	Servo Motor	1
3	สายจัมเปอร์	5
4	กล้องกล้องwebcam	1
5	ตู้ล็อกเกอร์	1

ตัวอย่างโค้ดการทำงาน

The image shows a software interface for a face recognition project. On the left, a 'Recognition Window' displays a video feed of a woman. Below the video, two progress bars show recognition results: 'jajah' at 0% and 'pan' at 100%. The 'pan' bar is green, while 'jajah' is grey. Below the progress bars are various code blocks for an Arduino Uno, including 'play tone on', 'get timer value', 'reset timer', 'cast', 'map', and 'Initialise LCD Display 16x2'.

On the right, a block of code is shown in a Scratch-like environment. The code starts with a 'when clicked' event, followed by setting variables 'BK', 'Person1', and 'Person2' to 0. It then opens the 'recognition window' and enters a 'forever' loop. Inside the loop, it 'analyse image from web camera'. It then checks if the 'is identified class - pan?' is true. If true, it sets 'Person1' to the 'get confidence of class pan'. If false, it checks if 'is identified class - jajah?' is true. If true, it sets 'Person2' to the 'get confidence of class jajah'. If false, it sets 'BK' to the 'get confidence of class pan'. After the loop, it checks if 'Person1 > 0.8'. If true, it sets 'servo on 11' to '160 angle'. If false, it sets 'servo on 11' to '0 angle'.

```
when clicked
  set BK to 0
  set Person1 to 0
  set Person2 to 0
  open recognition window
  forever
    analyse image from web camera
    if is identified class - pan ? then
      set Person1 to get confidence of class pan
    else
      if is identified class - jajah ? then
        set Person2 to get confidence of class jajah
      else
        set BK to get confidence of class pan
    if Person1 > 0.8 then
      set servo on 11 to 160 angle
    else
      set servo on 11 to 0 angle
```

แนวคิด หลักการ และข้อคิดทางวิชาการที่จะใช้

แนวคิดเกี่ยวกับการยืนยันตัวตน (Authentication) และความปลอดภัย (Security): การยืนยันตัวตนผ่านระบบสแกนใบหน้าเป็นเทคโนโลยีที่ใช้ลักษณะทางชีวภาพของผู้ใช้งาน (Biometric Authentication) เพื่อรับรองตัวตนและเข้าถึงข้อมูลหรือสถานที่ที่มีความปลอดภัย โดยการใช้คุณสมบัติที่ไม่สามารถเปลี่ยนแปลงได้ เช่น ลักษณะใบหน้าเป็นตัวแปรสำคัญ แนวคิดนี้ช่วยให้การรักษาความปลอดภัยมีประสิทธิภาพสูงขึ้นและลดความเสี่ยงจากการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต

หลักการของเทคโนโลยีสแกนใบหน้า (Facial Recognition Technology): หลักการของเทคโนโลยีสแกนใบหน้าเกี่ยวข้องกับการจับและวิเคราะห์ลักษณะใบหน้าของบุคคลโดยใช้เทคโนโลยีการรู้จำลักษณะใบหน้าด้วยระบบประมวลผลภาพ (Image Processing) และอัลกอริทึมที่ช่วยแยกแยะลักษณะเด่น เช่น ตำแหน่งของดวงตา จมูก และปาก เพื่อนำมาประมวลผลและเปรียบเทียบกับฐานข้อมูลของใบหน้าในระบบ แนวคิดทางวิชาการเกี่ยวกับการใช้เทคโนโลยีสแกนใบหน้าในระบบรักษาความปลอดภัย: การใช้ระบบสแกนใบหน้าสำหรับการเปิดล็อกเกอร์มักถูกมองในด้านการเพิ่มประสิทธิภาพในการรักษาความปลอดภัยและสะดวกในการใช้งาน ความสำคัญของการใช้ระบบนี้คือการลดข้อผิดพลาดที่อาจเกิดจากการใช้รหัสผ่านหรือกุญแจ ซึ่งอาจสูญหายหรือถูกขโมยได้ ดังนั้น การใช้เทคโนโลยีสแกนใบหน้าจึงเป็นการยกระดับการรักษาความปลอดภัยและลดความเสี่ยงจากการถูกเข้าถึงข้อมูลที่ไม่พึงประสงค์

ข้อคิดทางวิชาการเกี่ยวกับผลกระทบของการใช้งานเทคโนโลยีสแกนใบหน้าในขณะที่การใช้เทคโนโลยีสแกนใบหน้ามีข้อดีในการเพิ่มความสะดวกและความปลอดภัย แต่ก็มีข้อควรระวังเกี่ยวกับความเป็นส่วนตัว (Privacy) และความถูกต้อง (Accuracy) ของระบบ สภาพแวดล้อมหรือสภาพแสงอาจส่งผลต่อการทำงานของระบบ และมีข้อกังวลเกี่ยวกับการเก็บข้อมูลใบหน้าของผู้ใช้งาน การควบคุมและการใช้ข้อมูลดังกล่าวต้องได้รับการดูแลอย่างรอบคอบเพื่อป้องกันการละเมิดสิทธิส่วนบุคคล

ข้อเสนอแนะในการพัฒนาและประยุกต์ใช้เทคโนโลยี: การวิจัยควรพิจารณาเรื่องการปรับปรุงและพัฒนาเทคโนโลยีสแกนใบหน้าให้มีความแม่นยำสูงขึ้น โดยเฉพาะในแง่ของการทำงานในสภาพแวดล้อมที่แตกต่างกัน เช่น สภาพแสงที่ไม่ดีหรือการสวมใส่สิ่งปกปิดใบหน้า (เช่น หมวกหรือแว่นตา) นอกจากนี้ยังควรมีการพัฒนาในด้านการปกป้องข้อมูลและความเป็นส่วนตัวของผู้ใช้งาน รวมทั้งการตรวจสอบมาตรฐานความปลอดภัยในระดับสากล

ภาพกิจกรรม





(ภาพเหนือศีรษะจากดาวเทียม)