แบบเสนอหัวข้อโครงงานวิศวกรรม
หลักสูตรวิศวกรรมซอฟต์แวร์ สาขาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา
ปีการศึกษา 2/2568

รหัสโครงงานวิศวกรรม .....SE02.....

(สำหรับอาจารย์ประจำวิชา)

ชื่อโครงงานวิศวกรรม (ไทย) แอปตรวจจับภาพหลอกลวงด้วยปัญญาประดิษฐ์ (AI)
(อังกฤษ) App Scam Image Detection for AI

ชื่อหัวหน้าโครงงานวิศวกรรม (ไทย) นาย ภานุวัฒน์ ต๋ำคำ
(อังกฤษ) panuwat takham
รหัสนักศึกษา 67543210044-3 ชั้นปี วศบ.ซว.(เทียบโอน) ปี 2

ลายเซ็น.....

ชื่ออาจารย์ที่ปรึกษา อาจารย์ ปิยพล ยืนยงสถาวร

ลายเซ็น .....

วันที่เสนอโครงงานวิศวกรรม ..... พศ. 2568

กรรมการ

1.....
(อาจารย์สัญญา อุทโยธา)

2.....
(อาจารย์รุจิพันธุ์ โกษารัตน์)

3.....
(อาจารย์อรษา สิระษากมล)

4.....
(อาจารย์ปิยพล ยืนยงสถาวร)

5.....
(อาจารย์นริศ กำแพงแก้ว)

6.....
(อาจารย์ธนิต เกตุแก้ว)

2. สารบัญ

หน้า

3. คณะผู้ดำเนินงาน

หัวหน้าโครงงาน:

ชื่อ: นาย ภานุวัฒน์ ต๋ำคำ

รหัสนักศึกษา: 67543210044-3

ชั้นปี: วิศวกรรมซอฟต์แวร์ ปี 2 (หลักสูตร เทียบโอน)

ความเชี่ยวชาญ: fullstack , unity , linux

ความรับผิดชอบ: ทั้งโปรเจค

สัดส่วนความรับผิดชอบ: 100%

สถานที่ติดต่อ: มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา เชียงใหม่ ดอยสะเก็ด

โทรศัพท์: 0839230703

อีเมล: panuwattakham2002@gmail.com

อาจารย์ที่ปรึกษา: อาจารย์ ปิยพล ยืนยงสถาวร

4. บทคัดย่อ

ในปัจจุบัน อาชญากรรมทางไซเบอร์ในรูปแบบการหลอกลวงผ่านสื่อรูปภาพ (Image-based Scams) มีแนวโน้มทวีความรุนแรงขึ้นอย่างต่อเนื่อง ทั้งการใช้รูปโปรไฟล์ปลอม การโฆษณาสินค้าเท็จ และการปลอมแปลงหลักฐานการโอนเงิน ซึ่งสร้างความเสียหายต่อทรัพย์สินและความเชื่อมั่นของผู้ใช้งานในวงกว้าง อย่างไรก็ตาม เครื่องมือตรวจสอบที่มีอยู่ในปัจจุบันมักมีความซับซ้อนและเข้าถึงได้ยากสำหรับบุคคลทั่วไป

โครงงานนี้จึงมีวัตถุประสงค์เพื่อพัฒนาแอปพลิเคชันบนอุปกรณ์เคลื่อนที่ที่สามารถประเมินความเสี่ยงของรูปภาพที่น่าสงสัยได้อย่างรวดเร็วและแม่นยำ โดยประยุกต์ใช้ หลักการวิเคราะห์แบบหลายชั้น (Multi-layer Analysis) ซึ่งบูรณาการเทคนิคการตรวจสอบ 3 ด้านเข้าด้วยกัน ได้แก่ 1) การวิเคราะห์ข้อความ (Textual Analysis) โดยใช้เทคโนโลยี OCR ร่วมกับ NLP เพื่อตรวจจับคำสำคัญหรือรูปแบบประโยคที่มิจฉาชีพนิยมใช้ 2) การตรวจสอบแหล่งที่มา (Source Verification) ด้วยการค้นหาภาพย้อนกลับ (Reverse Image Search) เพื่อระบุบริบทที่แท้จริงของภาพ และ 3) การวิเคราะห์ความผิดปกติทางทัศนภาพ (Visual Anomaly Detection) โดยใช้โมเดลการเรียนรู้เชิงลึก (Deep Learning) เพื่อตรวจจับร่องรอยการตัดต่อและการสร้างภาพด้วยปัญญาประดิษฐ์ (AI-Generated Image)

5. คำสำคัญ

5.1 ภาษาไทย:

1. การตรวจจับภาพหลอกลวง – ระบุปัญหาหลักของโครงงาน
2. การวิเคราะห์แบบหลายชั้น – ระบุวิธีการแก้ปัญหาที่เป็นจุดเด่น (Text + Source + Visual)
3. การเรียนรู้เชิงลึก – ระบุเทคโนโลยีหลักที่ใช้สร้างโมเดล AI
4. นิติวิทยาศาสตร์ภาพดิจิทัล – ศัพท์ทางเทคนิคของการตรวจสอบการตัดต่อภาพ
5. การรู้จำอักขระด้วยแสง – ระบุเทคโนโลยี OCR ที่ใช้ตรวจข้อความ

5.2 ภาษาอังกฤษ:

1. Scam Image Detection
2. Multi-layer Analysis
3. Deep Learning
4. Digital Image Forensics
5. Optical Character Recognition (OCR)

6. ความสำคัญและที่มาของปัญหาที่ทำการวิจัย(หลักการ เหตุผล)

สภาพการณ์ปัจจุบันและภัยคุกคามทางไซเบอร์ ในยุคปัจจุบัน เทคโนโลยีดิจิทัลได้เข้ามามีบทบาทสำคัญในชีวิตประจำวัน ทั้งการทำธุรกรรมทางการเงิน การซื้อขายสินค้าออนไลน์ (E-commerce) และการติดต่อสื่อสารผ่านโซเชียลมีเดีย อย่างไรก็ตามความสะดวกสบายนี้ได้นำมาซึ่งช่องทางใหม่สำหรับมิจฉาชีพในการก่ออาชญากรรมทางไซเบอร์ โดยเฉพาะอย่างยิ่ง "การหลอกลวงผ่านสื่อรูปภาพ" (Image-based Scams) ซึ่งเป็นวิธีการที่สร้างความเสียหายเป็นวงกว้าง เนื่องจากมนุษย์มีธรรมชาติที่จะเชื่อถือสิ่งที่มองเห็น (Visual Trust) มิจฉาชีพจึงใช้รูปภาพเป็นเครื่องมือหลักในการสร้างความน่าเชื่อถือ

ผลกระทบจากเทคโนโลยีปัญญาประดิษฐ์ (Generative AI) สถานการณ์ทวีความรุนแรงขึ้นเมื่อเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) และ Generative AI (เช่น GANs, Stable Diffusion) มีความก้าวหน้าอย่างก้าวกระโดด ทำให้ผู้ไม่หวังดีสามารถสร้างภาพใบหน้าบุคคลที่ไม่มีอยู่จริง (AI-Generated Faces) หรือตัดต่อภาพหลักฐานต่างๆ ได้อย่างแนบเนียนในเวลาอันรวดเร็ว จนสายตาของมนุษย์ทั่วไปไม่สามารถแยกแยะความแตกต่างระหว่างภาพจริงและภาพที่ถูกสร้างขึ้นได้อีกต่อไป ส่งผลให้สถิติคดีอาชญากรรมทางเทคโนโลยี โดยเฉพาะคดีหลอกลวงซื้อขายสินค้าและคดีหลอกให้โอนเงิน มีแนวโน้มสูงขึ้นอย่างต่อเนื่อง สร้างความเสียหายทางเศรษฐกิจและสังคมมหาศาล

ช่องว่างของเครื่องมือตรวจสอบในปัจจุบัน แม้ว่าจะมีเครื่องมือทางนิติวิทยาศาสตร์ (Digital Forensics) สำหรับตรวจสอบการตัดต่อภาพอยู่บ้าง แต่ส่วนใหญ่มักเป็นซอฟต์แวร์ที่มีความซับซ้อน ใช้งานบนคอมพิวเตอร์และต้องอาศัยผู้เชี่ยวชาญในการตีความผลลัพธ์ ทำให้ประชาชนทั่วไปที่เป็นผู้ใช้งานสมาร์ทโฟน ไม่สามารถเข้าถึงเครื่องมือเหล่านี้ได้ทันทีที่ประสบเหตุ หรือก่อนที่จะตัดสินใจโอนเงิน/ส่งข้อมูลส่วนตัว

ความจำเป็นในการพัฒนาระบบ จากปัญหาและข้อจำกัดข้างต้น คณะผู้จัดทำจึงเล็งเห็นถึงความจำเป็นเร่งด่วนในการพัฒนา "แอปพลิเคชันมือถือสำหรับตรวจจับภาพหลอกลวงด้วย AI" ที่บูรณาการเทคนิคการตรวจสอบแบบหลายชั้น (Multi-layer Analysis) เข้าด้วยกัน ทั้งการวิเคราะห์ความผิดปกติจากการตัดต่อ (Image Splicing), การตรวจจับภาพที่สร้างด้วย AI (AI-Generated), และการตรวจสอบแหล่งที่มาของภาพ (Reverse Image Search) โดยมุ่งเน้นการออกแบบให้ใช้งานง่าย สะดวก และประมวลผลได้รวดเร็ว เพื่อทำหน้าที่เป็นเกราะป้องกันด่านแรก (First Line of Defense) ให้แก่ประชาชน ช่วยลดความเสี่ยงและมูลค่าความเสียหายจากการถูกหลอกลวงในโลกออนไลน์ได้อย่างมีประสิทธิภาพ

7. วัตถุประสงค์ของโครงงานวิศวกรรม

7.1. เพื่อพัฒนาแอปพลิเคชันบนอุปกรณ์เคลื่อนที่สำหรับคัดกรองและตรวจจับรูปภาพที่มีความเสี่ยงในการหลอกลวง (Scam Image Detection) ที่อำนวยความสะดวกให้ผู้ใช้งานทั่วไปสามารถเข้าถึงและใช้งานได้ง่าย

7.2. เพื่อศึกษาและประยุกต์ใช้ เทคโนโลยีการเรียนรู้เชิงลึก (Deep Learning) และการประมวลผลภาพดิจิทัล (Digital Image Processing) ในการตรวจจับร่องรอยการตัดต่อภาพ (Image Forgery) และการสร้างภาพด้วยปัญญาประดิษฐ์ (AI-Generated Image)

7.3. เพื่อพัฒนาระบบวิเคราะห์ความเสี่ยงแบบบูรณาการ (Multi-layer Analysis) ที่สามารถประมวลผลข้อมูลจากองค์ประกอบของภาพ (Visual Features), ข้อความที่ปรากฏในภาพ (Textual Information), และแหล่งที่มาของภาพ (Image Source) ร่วมกันเพื่อเพิ่มความแม่นยำในการตรวจสอบ

7.4. เพื่อทดสอบและประเมินประสิทธิภาพ ของระบบตรวจจับในด้านความถูกต้อง (Accuracy), ความแม่นยำ (Precision), และระยะเวลาในการประมวลผล (Processing Time) รวมถึงประเมินความพึงพอใจของผู้ใช้งานที่มีต่อแอปพลิเคชัน

8. ผลกระทบเชิงเศรษฐศาสตร์

8.1. การลดความสูญเสียทางการเงินระดับบุคคล (Reduction of Individual Financial Loss)
ปัญหาอาชญากรรมไซเบอร์สร้างความเสียหายต่อทรัพย์สินของประชาชนโดยตรง การมีเครื่องมือคัดกรองที่มีประสิทธิภาพจะช่วยระงับยับยั้งการทำธุรกรรมที่ผิดพลาดได้ทันท่วงที

8.1.1 ป้องกันการโอนเงินให้มิจฉาชีพ ช่วยลดมูลค่าความเสียหายจากการถูกหลอกซื้อสินค้า และการหลอกลงทุน ซึ่งเป็นมูลค่าความเสียหายสะสมหลักพันล้านบาทต่อปีในประเทศไทย

8.2. การสร้างความเชื่อมั่นในระบบเศรษฐกิจดิจิทัล (Enhancing Digital Economy Confidence)
ความหวาดระแวงต่อภัยไซเบอร์เป็นอุปสรรคสำคัญที่ชะลอการเติบโตของ E-Commerce การมีกลไกตรวจสอบที่เข้าถึงง่ายจะช่วยฟื้นฟูความเชื่อมั่นของผู้บริโภค

8.2.1 กระตุ้นการบริโภคออนไลน์: เมื่อผู้บริโภคมั่นใจว่าสามารถตรวจสอบความน่าเชื่อถือของผู้ขายได้ (ผ่านการสแกนรูปสินค้า/โปรไฟล์) จะเกิดความกล้าในการจับจ่ายใช้สอย ส่งผลให้มูลค่าตลาด E-Commerce เติบโตขึ้น

8.3. การลดต้นทุนการดำเนินงานของภาคธุรกิจและรัฐ (Operational Cost Reduction)
แอปพลิเคชันนี้สามารถทำหน้าที่เป็นเครื่องมือทุ่นแรง (Automation Tool) ให้กับหน่วยงานที่เกี่ยวข้อง

8.3.1 ลดภาระงานของเจ้าหน้าที่ตำรวจและธนาคาร การป้องปรามเหตุตั้งแต่ต้นทาง (Prevention) ช่วยลดจำนวนคดีความที่เข้าสู่ระบบ ทำให้เจ้าหน้าที่สามารถจัดสรรทรัพยากรไปจัดการกับคดีที่มีความซับซ้อนสูงกว่าได้

8.3.2 ลดต้นทุนการตรวจสอบสำหรับแพลตฟอร์ม สำหรับ Marketplace หรือ Social Media การใช้ AI ช่วยคัดกรองรูปภาพหลอกลวง ช่วยลดต้นทุนในการจ้างแอดมิน (Human Moderator) จำนวนมากเพื่อมาตรวจสอบเนื้อหาทีละรายการ

8.4. การป้องกันการรั่วไหลของเม็ดเงินออกนอกประเทศ (Prevention of Economic Leakage)
อาชญากรรมไซเบอร์ส่วนใหญ่มักเป็นขบวนการข้ามชาติ (Transnational Crime) ซึ่งเงินที่ถูกหลอกลวงไปมักถูกโอนออกนอกประเทศผ่านบัญชีม้าหรือ Cryptocurrency การสกัดกั้นการหลอกลวงตั้งแต่ต้นทางจึงเป็นการช่วยรักษาเม็ดเงินให้หมุนเวียนอยู่ภายในระบบเศรษฐกิจของประเทศ

9. ผลกระทบเชิงสังคม

9.1. การสร้างภูมิคุ้มกันทางดิจิทัล (Digital Immunity Enhancement)

แอปพลิเคชันนี้ไม่ได้ทำหน้าที่เพียงแค่ "ตรวจจับ" แต่ยังทำหน้าที่ "ให้ความรู้" ผ่านฟีเจอร์การอธิบายผลลัพธ์ (Explainability) ว่าทำไมรูปภาพนี้จึงน่าสงสัย

9.1.1 ลดการแพร่กระจายข่าวปลอม ช่วยสกัดกั้นการแชร์ข้อมูลเท็จหรือภาพบิดเบือน (Disinformation) ที่อาจสร้างความตื่นตระหนกหรือความเกลียดชังในสังคม

9.1.2 การเรียนรู้จากการใช้งานจริง ผู้ใช้งานจะเกิดการเรียนรู้และจดจำรูปแบบกลโกง (Scam Patterns) ได้โดยอัตโนมัติจากการใช้งานแอปพลิเคชันอย่างต่อเนื่อง ส่งผลให้สังคมมีความตระหนักรู้และรู้เท่าทันสื่อ (Media Literacy) เพิ่มมากขึ้น

9.2. การลดความเหลื่อมล้ำในการเข้าถึงเทคโนโลยี (Bridging the Digital Divide)

กลุ่มเปราะบาง เช่น ผู้สูงอายุ เยาวชน หรือประชาชนในพื้นที่ห่างไกล มักตกเป็นเหยื่อของอาชญากรรมไซเบอร์เนื่องจากขาดความชำนาญทางเทคโนโลยี

9.2.1 เครื่องมือสำหรับทุกคน การออกแบบแอปพลิเคชันที่ใช้งานง่าย (User-friendly) เปรียบเสมือนการมอบ "ผู้ช่วยส่วนตัว" ให้กับกลุ่มเปราะบางเหล่านี้ ทำให้พวกเขามีเครื่องมือในการปกป้องตนเองทัดเทียมกับผู้ที่มีความเชี่ยวชาญด้านไอที

9.2.2 ความปลอดภัยที่เท่าเทียม ช่วยกระจายโอกาสในการเข้าถึงความปลอดภัยทางไซเบอร์ (Cybersecurity Accessibility) ไปสู่ประชาชนทุกระดับชั้น ไม่จำกัดเฉพาะในกลุ่มองค์กรขนาดใหญ่

9.3. การส่งเสริมสุขภาวะทางจิต (Mental Health Promotion)

การตกเป็นเหยื่อของการหลอกลวงไม่ได้ส่งผลเสียเพียงแค่ทรัพย์สิน แต่ยังส่งผลกระทบโดยตรงต่อสภาพจิตใจ

9.3.1 ลดความเครียดและความวิตกกังวล การมีเครื่องมือช่วยตรวจสอบก่อนตัดสินใจ ช่วยลดความกังวลใจในการใช้งานโซเชียลมีเดียและการทำธุรกรรมออนไลน์

9.3.2 ป้องกันปัญหาสุขภาพจิตจาก Romance Scam การตรวจจับรูปโปรไฟล์ปลอมช่วยป้องกันความเสียหายทางจิตใจที่รุนแรงจากการถูกหลอกให้รัก ซึ่งมักนำไปสู่ภาวะซึมเศร้าหรือเหตุโศกนาฏกรรม

10. การพัฒนาเทคโนโลยี

10.1. การบูรณาการปัญญาประดิษฐ์แบบพหุรูปแบบ (Multi-modal AI Integration)
โครงงานนี้มุ่งเน้นการพัฒนากระบวนการวิเคราะห์ข้อมูลที่ไม่ได้จำกัดอยู่เพียงรูปแบบเดียว (Single Modality) แต่เป็นการบูรณาการข้อมูลจากหลายมิติเข้าด้วยกัน (Multi-modal Learning) ได้แก่

10.1.1 Computer Vision สำหรับวิเคราะห์องค์ประกอบภาพและร่องรอยการตัดต่อ

10.1.2 Natural Language Processing (NLP) สำหรับวิเคราะห์ความหมายของข้อความ (Text Semantics) ที่ปรากฏบนภาพ

10.1.3 Information Retrieval สำหรับการสืบค้นข้อมูลย้อนกลับจากแหล่งข้อมูลภายนอก การนำเทคโนโลยีทั้ง 3 ส่วนมาทำงานร่วมกันและประมวลผลออกมาเป็นค่าความเสี่ยงเดียว (Unified Risk Score) ถือเป็นการพัฒนากระบวนการตัดสินใจของระบบอัตโนมัติให้มีความใกล้เคียงกับการพิจารณาของมนุษย์มากที่สุด

10.2. การประยุกต์ใช้เทคโนโลยีการเรียนรู้เชิงลึกขั้นสูง (Advanced Deep Learning Application)
โครงงานนี้มีการนำเทคนิคการเรียนรู้ของเครื่องสมัยใหม่มาปรับใช้เพื่อแก้ปัญหาเฉพาะทาง

10.2.1 Transfer Learning: การนำโมเดลที่ผ่านการเทรนมาแล้ว (Pre-trained Models) เช่น EfficientNet หรือ Vision Transformers (ViT) มาทำการเรียนรู้ต่อ (Fine-tuning) ด้วยชุดข้อมูลภาพหลอกลวง เพื่อลดระยะเวลาในการสอนโมเดลและเพิ่มความแม่นยำแม้มีข้อมูลจำกัด

10.2.2 Explainable AI (XAI): การพัฒนาให้ระบบไม่เพียงแค่ "ทำนายผล" แต่ต้อง "อธิบายผล" ได้ โดยการใช้เทคนิคเช่น Grad-CAM เพื่อสร้างแผนที่ความร้อน (Heatmap) แสดงจุดที่โมเดลให้ความสนใจ ซึ่งช่วยลดปัญหาความเป็น "กล่องดำ" (Black Box) ของระบบ AI แบบดั้งเดิม

10.3. การพัฒนาสถาปัตยกรรมซอฟต์แวร์แบบคลาวด์เนทีฟ (Cloud-Native Software Architecture)
เพื่อรองรับการประมวลผล AI ที่มีความซับซ้อนแต่ยังคงไว้ซึ่งความรวดเร็วในการตอบสนองต่อผู้ใช้งานมือถือ โครงงานนี้จึงเลือกใช้สถาปัตยกรรมแบบ Microservices ร่วมกับเทคโนโลยี Containerization (เช่น Docker)

10.3.1 Scalability: ช่วยให้ระบบสามารถรองรับผู้ใช้งานจำนวนมากได้พร้อมกัน โดยสามารถขยายทรัพยากรเฉพาะส่วนที่ทำงานหนัก (เช่น ส่วนประมวลผลภาพ) ได้อย่างอิสระ

10.3.2Cross-Platform Availability: การพัฒนาส่วนติดต่อผู้ใช้ด้วย Flutter ช่วยให้เทคโนโลยีนี้สามารถเข้าถึงผู้ใช้งานได้ครอบคลุมทั้งระบบปฏิบัติการ iOS และ Android ด้วยฐานโค้ดเดียวกัน

10.4. การสร้างชุดข้อมูลสังเคราะห์เพื่อต่อต้านภัย AI (Synthetic Data Generation for Adversarial Defense)

ในกระบวนการพัฒนาโมเดล โครงงานนี้ได้นำแนวคิด "หนามยอกเอาหนามบ่ง" มาใช้ โดยการใช้ Generative AI สร้างภาพจำลองสถานการณ์การหลอกลวง (Synthetic Datasets) เพื่อนำมาใช้สอนโมเดลตรวจจับ (Detector) วิธีการนี้ช่วยแก้ปัญหาการขาดแคลนข้อมูลภาพหลอกลวงจริง และช่วยให้ระบบเรียนรู้ที่จะตรวจจับภาพที่สร้างจาก AI รุ่นใหม่ๆ ได้อย่างมีประสิทธิภาพ (Adversarial Training)