ใบขอรับเป็นว่าที่ ที่ปรึกษาโครงงานวิศวกรรม

ชื่อโครงการ ภาษาไทย แอปตรวจจับภาพหลอกลวงด้วยปัญญาประดิษฐ์ (AI)

English App Scam Image Detection for AI

ชื่อนักศึกษา 1 นาย ภานุวัฒน์ ต๋าคำ รหัส 67543210044-3 ชั้นปี 2

สรุปสาระสำคัญเกี่ยวข้อง

1. ความเป็นมาของปัญหา
2. แนวคิดและหลักการ

บันทึกผลการรับนักศึกษา

……

……

……

……

ลงชื่อ

……..

(…… ……..)

ว่าที่ที่ปรึกษา

ความเป็นมาของปัญหา

สภาพการณ์ปัจจุบันและภัยคุกคามทางไซเบอร์ ในยุคปัจจุบัน เทคโนโลยีดิจิทัลได้เข้ามามีบทบาทสำคัญในชีวิตประจำวัน ทั้งการทำธุรกรรมทางการเงิน การซื้อขายสินค้าออนไลน์ (E-commerce) และการติดต่อสื่อสารผ่านโซเชียลมีเดีย อย่างไรก็ตาม ความสะดวกสบายนี้ได้นำมาซึ่งช่องทางใหม่สำหรับมิจฉาชีพในการก่ออาชญากรรมทางไซเบอร์ โดยเฉพาะอย่างยิ่ง "การหลอกลวงผ่านสื่อรูปภาพ" (Image-based Scams) ซึ่งเป็นวิธีการที่สร้างความเสียหายเป็นวงกว้าง เนื่องจากมนุษย์มีธรรมชาติที่จะเชื่อถือสิ่งที่มองเห็น (Visual Trust) มิจฉาชีพจึงใช้รูปภาพเป็นเครื่องมือหลักในการสร้างความน่าเชื่อถือ เช่น การปลอมแปลงสลิปโอนเงิน, การใช้รูปโปรไฟล์ปลอมเพื่อหลอกให้รัก (Romance Scam), หรือการนำรูปสินค้าจริงจากแหล่งอื่นมาแอบอ้างขาย (Fake Marketplace Listings)

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 ใช้งานบนคอมพิวเตอร์ และต้องอาศัยผู้เชี่ยวชาญในการตีความผลลัพธ์ ทำให้ประชาชนทั่วไปที่เป็นผู้ใช้งานสมาร์ทโฟน ไม่สามารถเข้าถึงเครื่องมือเหล่านี้ได้ทันทีที่ประสบเหตุ หรือก่อนที่จะตัดสินใจโอนเงิน/ส่งข้อมูลส่วนตัว

ความจำเป็นในการพัฒนาระบบ จากปัญหาข้างต้น คณะผู้จัดทำจึงเล็งเห็นถึงความจำเป็นเร่งด่วนในการพัฒนา "แอปพลิเคชันมือถือสำหรับตรวจจับภาพหลอกลวงด้วย AI" ที่สามารถวิเคราะห์ความผิดปกติของรูปภาพ ทั้งจากการตัดต่อ (Image Splicing), การสร้างด้วย AI (AI-Generated), และการตรวจสอบแหล่งที่มาของภาพ (Reverse Image Search) โดยเน้นการใช้งานที่ง่าย สะดวก และประมวลผลได้รวดเร็วบนสมาร์ทโฟน เพื่อเป็นเกราะป้องกันด่านแรกให้แก่ประชาชน ช่วยลดความเสี่ยงและมูลค่าความเสียหายจากการถูกหลอกลวงในโลกออนไลน์ได้อย่างมีประสิทธิภาพ

แนวคิดและหลักการ

การพัฒนาแอปพลิเคชันตรวจจับรูปภาพหลอกลวง (Scam Image Detection) อาศัยการบูรณาการองค์ความรู้ทางด้านคอมพิวเตอร์วิทัศน์ (Computer Vision) และปัญญาประดิษฐ์ (Artificial Intelligence) โดยมีหลักการสำคัญ 4 ด้าน ดังนี้

1. นิติวิทยาศาสตร์ภาพดิจิทัล (Digital Image Forensics)

หลักการนี้ใช้สำหรับตรวจจับการดัดแปลงหรือตัดต่อภาพ (Image Manipulation) โดยไม่ต้องอาศัยภาพต้นฉบับมาเปรียบเทียบ (Blind Forensics) โดยมุ่งเน้นไปที่การหาสิ่งผิดปกติที่เกิดขึ้นจากกระบวนการประมวลผลภาพ

- Error Level Analysis (ELA): เป็นเทคนิคที่ใช้ตรวจสอบระดับการบีบอัดของไฟล์ภาพ JPEG หลักการคือ เมื่อมีการนำภาพส่วนหนึ่งมาตัดต่อใส่ในอีกภาพหนึ่ง ระดับ Error หรือ Quality ของการบีบอัดในส่วนที่ถูกตัดต่อจะแตกต่างไปจากพื้นหลังอย่างชัดเจนเมื่อมีการบันทึกไฟล์ซ้ำ
- Metadata Analysis: การวิเคราะห์ข้อมูลจำเพาะของไฟล์ (EXIF Data) เช่น รุ่นกล้อง, วันที่ถ่าย, ซอฟต์แวร์ที่ใช้บันทึก หากพบว่าข้อมูลขัดแย้งกัน หรือมีการใช้ซอฟต์แวร์แก้ไขภาพ (เช่น Photoshop) ระบบจะประเมินความเสี่ยงเพิ่มขึ้น

2. การเรียนรู้เชิงลึก (Deep Learning) สำหรับจำแนกภาพ

ระบบใช้โครงข่ายประสาทเทียม (Neural Networks) ในการเรียนรู้ลักษณะเด่น (Features) ของภาพทั้งที่เป็นภาพจริงและภาพหลอกลวง

- Convolutional Neural Networks (CNN): เป็นโครงสร้างหลักที่ใช้ในการ "มอง" ภาพ โดยโมเดล (เช่น EfficientNet หรือ ResNet) จะทำการสกัดคุณลักษณะของภาพ (Feature Extraction) ตั้งแต่ระดับพื้นฐาน (เส้น, ขอบ, สี) ไปจนถึงระดับซับซ้อน (รูปร่างหน้าตา, วัตถุ) เพื่อจำแนกประเภท (Classification) ว่าภาพนี้มีความเสี่ยงหรือไม่
- Attention Mechanism: การใช้กลไกความสนใจ (Attention) เพื่อให้โมเดลโฟกัสไปที่จุดผิดปกติเล็กๆ ในภาพ เช่น รอยต่อบริเวณคอ เงาที่ไม่สมจริง หรือความผิดปกติของดวงตา ซึ่งเป็นจุดสังเกตสำคัญของภาพ Deepfake

3. การตรวจจับภาพที่สร้างด้วย AI (AI-Generated Image Detection)

เนื่องจากภาพที่สร้างจาก Generative AI (เช่น GANs หรือ Diffusion Models) มักทิ้งร่องรอยทางคณิตศาสตร์เฉพาะตัว (Artifacts) ที่ตามนุษย์มองไม่เห็น

- Frequency Domain Analysis: การแปลงภาพจากโดเมนเวลา (Spatial Domain) เป็นโดเมนความถี่ (Frequency Domain) โดยใช้ Fourier Transform มักจะพบแพทเทิร์นผิดปกติในสเปกตรัมความถี่ของภาพที่สร้างจาก AI ซึ่งแตกต่างจากภาพถ่ายธรรมชาติ
- Semantic Consistency: การตรวจสอบความสมเหตุสมผลทางกายภาพ เช่น ทิศทางของแสงเงา การสะท้อนในดวงตา หรือรายละเอียดทางกายวิภาค (เช่น จำนวนนิ้วมือ รูปทรงหู) ที่ AI มักจะทำผิดพลาด

4. การค้นคืนภาพด้วยเนื้อหา (Content-Based Image Retrieval - CBIR)

หลักการนี้ใช้สำหรับการฟีเจอร์ "ค้นหารูปซ้ำ" (Reverse Image Search) เพื่อตรวจสอบว่ารูปนี้เคยปรากฏที่อื่นมาก่อนหรือไม่

- Image Embeddings: การแปลงรูปภาพให้เป็น "เวกเตอร์" (Vector) หรือชุดตัวเลขที่ระบุเอกลักษณ์ของภาพนั้นๆ โดยใช้โมเดลเช่น CLIP (Contrastive Language-Image Pre-Training)
- Similarity Search: การนำเวกเตอร์ของรูปที่ผู้ใช้สแกน ไปคำนวณหาระยะห่าง (เช่น Cosine Similarity) เปรียบเทียบกับฐานข้อมูลรูปภาพมิจฉาชีพหรือรูปภาพสาธารณะ หากเวกเตอร์มีความคล้ายคลึงกันสูง แสดงว่าอาจเป็นการนำรูปเก่ามาเล่าใหม่หรือขโมยรูปมาใช้

5. การวิเคราะห์ข้อความในภาพ (OCR & Text Analysis)

ใช้เทคโนโลยี Optical Character Recognition (OCR) เพื่อแปลงข้อความในรูปภาพให้เป็นตัวอักษรดิจิทัล จากนั้นนำไปประมวลผลด้วย Natural Language Processing (NLP) เพื่อตรวจจับคำหลัก (Keywords) ที่มักใช้ในการหลอกลวง เช่น "โอนด่วน", "หลุดจำนำ", "ราคาถูกเกินจริง" หรือตรวจสอบเลขบัญชีธนาคารกับฐานข้อมูล Blacklist