บทความวิจัย

ทดสอบความปลอดภัยของ แคปท์ช่ารูปเรขาคณิต โดยใช้ Deep Learning

Test the safety of captcha geometry Using Deep Learning

ฑิตยา ไชยฤทธิ์

สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

บทคัดย่อ

งานวิจัยนี้ได้นำเทคโนโลยีการประมวลผลภาพด้วยวิธีการเรียนรู้เชิงลึก ที่สามารถจำลองการมองเห็นของ มนุษย์พัฒนาแบบจำลองสำหรับตรวจสอบและจำแนกรูปเรขาคณิต จากแคปท์ช่าออกได้ โดยดำเนินการเก็บรวบรวมข้อมูล จากการจำลองภาพขึ้นมาใหม่ และเก็บข้อมูลการจำแนกแคปท์ช่ารูปเรขาคณิตฯ ออกเป็น 60 ชุดข้อมูล ประกอบด้วย วงกลม สามเหลี่ยม สีเหลี่ยม ห้าเหลี่ยม หกเหลี่ยม และแบ่งออกเป็น 12 สี โดยงานวิจัยอาศัยการประมวลผลภาพ (Image Processing) และนำข้อมูลเข้าไปสู่ขบวนการเรียนรู้ที่เป็นการเรียนรู้เชิงลึก ด้วยอัลกอริทึมโครงข่ายประสาทเทียมแบบสังวัตนาการ (Convolutional Neural Network: CNN)

คำสำคัญ : CNN , Captcha , Image Processing

1. บทนำ

ปัจจุบันเทคโนโลยีมีบทบาทมากมายสำหรับชีวิตประจำวันของทุกคน ไม่ว่าจะเป็นการติดต่อสื่อสาร อ่านข่าว การหาข้อมูลต่าง ๆ ล้วนผ่านทางอินเตอร์เน็ต เนื่องจากมีการจัดการข้อมูลต่าง ๆ ผ่านทางอินเทอร์เน็ตเพื่อให้สามารถติดต่อสื่อสารกันได้อย่างสะดวก รวมถึงการสร้างเว็บเพื่อแลกเปลี่ยนข้อมูล ทำให้ผู้คนมากมายสามารถพูดคุยแลกเปลี่ยนความคิดกันผ่านทางอินเตอร์เน็ตได้ จะเห็นได้ว่าอินเตอร์เน็ตสามารถช่วยให้ทุกคนสามารถสื่อสารกันได้อย่างสะดวกเนื่องจากอินเตอร์เน็ตทำให้หลาย ๆ อย่างสะดวกสบายมากขึ้น จึงเป็นการเปิดช่องทางให้ผู้ไม่ประสงค์ดีสามารถโจมตีหรือที่เรียกกันว่า การสแปม เว็บไซต์ต่าง ๆ อย่างง่ายดาย โดยเฉพาะการโจมตีที่ถูกส่งโดยโปรแกรมคอมพิวเตอร์แบบอัตโนมัติ (bot) ซึ่งก่อให้เกิดปัญหาเนื้อหาบางส่วนของเว็บไซต์ของคุณนั้นมีคุณภาพต่ำ ซึ่งอาจส่งผลต่อการทำ SEO ได้ จึงจำเป็นต้องมีการป้องกันเพื่อไม่ให้โปรแกรมสามารถโจมตีคอมพิวเตอร์ได้ โดยการป้องกันการโจมตีของโปรแกรมคอมพิวเตอร์เราเรียกว่า แคปท์ช่า

แคปท์ช่า (CAPTCHA) คือ กลไกหรือกระบวนการทดสอบความแตกต่างระหว่างมนุษย์กับคอมพิวเตอร์ เพื่อให้โปรแกรมคอมพิวเตอร์ไม่สามารถโจมตีเว็บไซต์ต่าง ๆ จึงจำเป็นต้องมีการทดสอบที่สามารถตรวจสอบผู้เข้าใช้งานว่าเป็นมนุษย์ไม่ใช่คอมพิวเตอร์ โดยแคปท์ช่าถูกออกแบบขึ้นมาเพื่อให้มนุษย์สามารถเข้าใจแบบทดสอบได้อย่างงายและทำให้คอมพิวเตอร์ไม่สามารถแก้แบบทดสอบได้

เนื่องจากปัจจุบันเทคโนโลยีมีการพัฒนามากขึ้นอย่างรวดเร็วจนทำให้โปรแกรมคอมพิวเตอร์สามารถผ่านการทดสอบแคปท์ช่าที่เคยออกแบบไว้ได้ จึงจำเป็นต้องมีการพัฒนาแคปท์ช่ามากขึ้นเพื่อป้องกันไม่ให้โปรแกรมคอมพิวเตอร์สามารถโจมตีเว็บไซต์ต่าง ๆ ได้ แต่หลังจากแคปท์ช่าถูกพัฒนาให้มีความซับซ้อนมากขึ้น ทำให้ยากต่อการทำความเข้าใจของมนุษย์

ส่งผลให้มนุษย์เสียเวลาในการทำแคปท์ช่ามากขึ้น หรืออาจจะถึงขั้นไม่ผ่านการทดสอบของแคปท์ช่า

2. ทฤษฎีที่เกี่ยวข้อง

การประมวลผลภาพ(Image Processing)

การประมวลผลภาพ (Image Processing) คือ เทคโนโลยี คอมพิวเตอร์ที่สามารถนำภาพมาประมวลผลผ่านกระบวนการ เช่นการทำให้ภาพมีความคมชัดมากขึ้น การกำจัดสัญญาณ รบกวนออกจากภาพ หรือการแบ่งส่วนของวัตถุเป็นต้น เพื่อให้ ได้ข้อมูลเชิงปริมาณไปวิเคราะห์และสร้างเป็นระบบ โดยการ ประมวลผลภาพสามารถนำไปใช้ประโยชน์ในงานด้านต่าง ๆ เช่น ระบบแยกประเภทไข่มุกด้วยวิธีการประมวลผลภาพ [1] และการตรวจจับและจดจำโมเดลรถยนต์ด้วยข้อมูลเชิงจุดภาพ [2] เป็นต้น

Deep Learning

Deep Learning หรือการเรียนรู้เชิงลึกคือการพัฒนาเทคโนโลยี คอมพิวเตอร์ให้สามารถเลียนแบบการทำงานของมนุษย์ ซึ่ง Deep Learning จะมีกระบวนการคิดคำนวณคล้ายกับระบบ โครงข่ายประสาท (Neurons) ของสมองมนุษย์เรียกว่าโครงข่ายประสาทเทียม (Neural Network: NN) [3] ข้อดีของ Deep Learningคือเมื่อต้องการใช้งานอย่างเช่น การประมวลผลภาพเพื่อคัดแยกคุณภาพของรูปเรขาคณิตการใช้งานไม่จำเป็นต้องให้ความรู้พื้นฐานกบั ระบบล่วงหน้า ความสามารถ ของ Deep Learning ก็สามารถสร้างแบบจำลองและหาคำตอบ ได้ ด้วยการนำ NN หลายๆ ชั้นเรี ยกว่า Hidden Layer มาใช้วิเคราะห์และหาคำตอบดังรูปที่ 1 ซึ่งคำว่า Deep Learning ก็มา จากการใช้ NN มากกว่า 2 ชั้น เพื่อให้เกิดการเรียนรู้และสร้าง แบบจำลอง ดังนั้นจึงเปรียบเทียบได้ว่าแต่ละชั้นของ NN ยิ่งถูก ใช้จำนวนมากในขั้นตอนการประมวลผลยิง่ ทำให้มีโครงสร้าง การเรียนรู้ที่ลึก(Deep) มากขึ้น

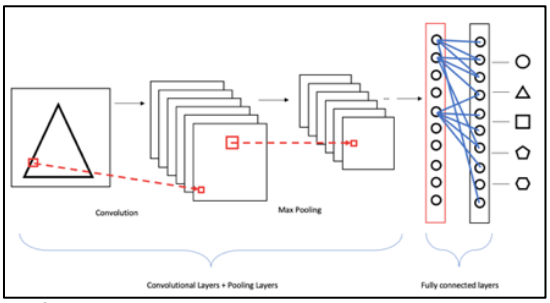
โครงข่ายประสาทเทียมแบบสังวัตนาการ (Convolutional Neural Network: CNN)

โครงข่ายประสาทเทียมแบบสังวัตนาการ (Convolutional Neural Network: CNN) [4] เป็นวิธีหนึ่งในวิธีการเรียนรู้แบบ Deep Learning เป็นการจำลองการมองเห็นของมนุษย์ที่ สามารถแยกแยกคุณลักษณะ (Feature) ของวัตถุที่มองเห็น เช่น สี ขอบภาพ การตัดกันของสี แล้วนำคุณลักษณะต่าง ๆ มา ประกอบกันเพื่อระบุคุณสมบัติของสิ่งที่มองเห็นแล้วคัดแยกว่า สิ่งนั้นมีคุณสมบัติเป็นอะไรเช่นเมื่อมองเห็นรูปเรขาคณิต คำนวณของ CNN สามารถแสดงคำตอบ ได้ว่ารูปเรขาคณิตนั้นเป็นรูปใดเป็นต้น ซึ่ง Deep Learning เป็นการประยุกต์ใช้ วิธีการของ NN หลายๆ ชั้นเรียกว่า Hidden Layer ดังรูปที่ 1 สำหรับค้นหาคุณลักษณะและทำซ้ำหลายๆ รอบจนกระทั่ง ได้คำตอบของคุณคุณลักษณะที่มีความแม่นยำของการคัดแยกโดย การทำงานของ CNN จะพิจารณ าจากความสัมพันธ์ของ คุณลักษณะที่สกัดได้ในแต่ละชั้นกับผลลัพธ์มากที่สุด หลักการ ทงานของ CNN มี 3 ส่วนดังนี้

Input: รับเข้าข้อมูลหรือวัตถุเหมือนกับการมองเห็นของมนุษย์ ตัวอย่างเช่นรูปเรขาคณิต

Hidden Layer: ส่วนการประมวลผลเป็นชั้น ๆ ซึ่งเหมือนกับการทำงานสมองของมนุษย์ เพื่อเรียนรู้ (Training) และและการคัดแยกประเภทของภาพ

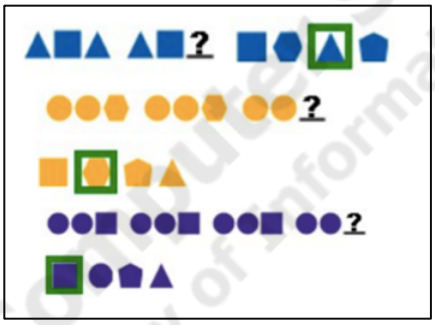
Output: ส่วนแสดงผลลัพธ์การคัดแยกคุณสมบัติเป็นผลมาจากใช้ Hidden Layerจำนวนหลายชั้นมาวิเคราะห์จน ได้คำตอบแสดงคุณลักษณะของแต่ละภาพที่มองเห็นเช่น รูปเรขาคณิตนั้นเป็นรูปใดเป็นต้น



รูปที่ 1 Convolutional Neural Network

งานวิจัยที่เกี่ยวข้อง

แคปท์ช่าที่ถูกพัฒนาโดย อาจารย์ ธวัชวงศ์ ลาวัลย์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยสารคาม โดยงานวิจัยที่เสนอให้เห็นว่า แคปท์ช่ารูปแบบใหม่หรือแคปท์ช่ารูปเรขาคณิตนั้นมีความเข้าใจง่ายต่อมนุษย์และมีความปลอดภัยจากโปรแกรมอัตโนมัติ[6]



รูปที่ 2 แคปท์ช่ารูปเรขาคณิต

3. แผนการดำเนินงาน

การเก็บข้อมูลและเตรียมข้อมูล

ในงานวิจัยนี้ดำเนินการเก็บรวบรวมข้อมูลจากการจำลองรูปเรขาคณิตขึ้นมา โดยที่มี วงกลม สามเหลี่ยม สีเหลี่ยม ห้าเหลี่ยม หกเหลี่ยม และแบ่งออกมาอีก 12 สี

การวัดประสิทธิภาพ

การวัดประสิทธิภาพเพื่อเปรียบเทียบค่าความแม่นยำเพื่อสร้าง แบบจำลองในงานวิจัยนี้ใช้การวัดค่าความแม่นยำ (Accuracy) [5] เป็นค่าที่ได้จากวิธีการทดสอบเพื่อหาค่าพยากรณ์ความถูกต้องของข้อมูลโดยคิดเป็นค่าร้อยละ (%) ใช้สูตรการคำนวณ ดังนี้

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

โดย

TP คือ ค่าที่พยากรณ์ถูกต้องเชิงบวก

TN คือ ค่าที่พยากรณ์ถูกต้องเชิงลบ

FP คือ ค่าที่พยากรณ์ผิดพลาดเชิงบวก

FN คือ ค่าที่พยากรณ์ผิดพลาดเชิงลบ

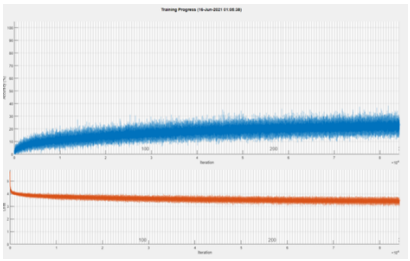
การสร้างแบบจำลอง

ในส่วนของการสร้างแบบจำลองมีการเตรียมขั้นตอน 2 ขั้นตอน คือ ขั้นตอนของการเรียนรู้(Train) เพื่อสร้างแบบจำลองและขั้นตอนของการทดสอบ (Test) แบบจำลองการสร้างแบบจำลองเป็นขั้นตอนการสร้างการเรียนรู้โดยใช้ข้อมูล รูปเรขาคณิตที่ได้จัดกลุ่ม กลุ่มละ 600 รูป รวม 36,000 รูป สำหรับใช้ในการเรียนรู้ (Training Dataset) และกลุ่มละ 400 รูป สำหรับใช้ทดสอบ (Testing Dataset)แบบจำลอง จากนั้นเมื่อได้แบบจำลองจึงนำภาพ 400 ภาพ ทดสอบความถูกต้องของการจำแนกรูปเรขาคณิต

4. ผลการวิจัย

ผลการสร้างแบบจำลอง (Model CNN)

การพัฒนาระบบเพื่อจำแนกรูปเรขาคณิตโดยใช้ Matlab ในการพัฒนา Model CNN โดยใช้ไลบรารีสำหรับพัฒนา Deep Learning



รูปที่ 3 กราฟแสดงค่า loss และ accuracy ของ model ที่สร้างขึ้น

จากรูปที่ 3 แสดงค่าความแม่นยำ (TrainAcc) และค่า ความผิดพลาด (TrainLoss) ในการทดสอบสร้างแบบจำลองจะ เห็นว่าการเรียนรู้ในแต่ละรอบ (Round) มีค่าความแม่นยำที่แตกต่างกัน โดยผลการทดลองสร้างแบบจำลองได้ค่าความ แม่นยำสูงสุดคือ 27.7% แสดงถึงประสิทธิภาพในการจำแนก รูปเรขาคณิตโดยใช้วิธี Deep Learning ด้วย อัลกอริทึม CNN

การนำแบบจำลองไปใช้งาน

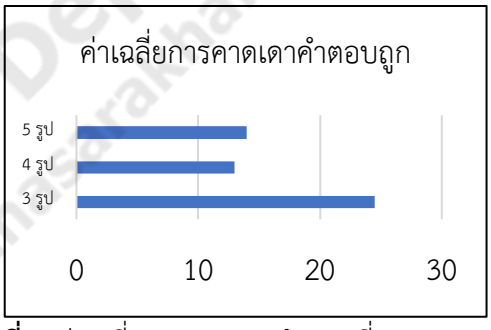
จากการสร้างแบบจำลองเพื่อจำแนกรูปเรขาคณิต งานวิจัยนี้ได้นำแบบจำลองที่สร้างขึ้นใช้สำหรับพัฒนา ระบบเพื่อใช้ประมวลผลภาพจำแนกรูปเรขาคณิต พัฒนาด้วยใช้ Matlab ใช้ไลบรารีสำหรับพัฒนา จากนั้นนำระบบที่พัฒนาโดยเป็นการนำรูปที่ 3 ส่วนที่ 2 มาใช้นำการทำนายหาคำตอบ

รูปที่ 4 ตัวอย่างแบบจำลอง

5. บทสรุปและอภิปราย

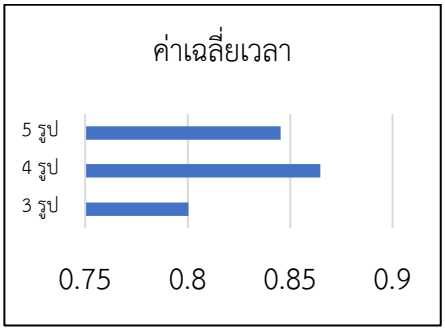
โครงการนี้นำเสนอโปรแกรมที่ใช้สำหรับการทดสอบความปลอดภัยของ แคปท์ช่ารูปเรขาคณิต โดยใช้ Deep Learning ซึ่งใช้การประมวลผลภาพ และการเรียนรู้เชิงลึก มีเป้าหมายเพื่อการตรวจสอบความปลอดภัยของแคปท์ช่ารูปแบบเรขาคณิต จากโปรแกรมอัตโนมัติ (บอท)

จากการทดลองวัดประสิทธิภาพการจำแนกรูปเรขาคณิต โดยให้โครงสร้าง CNN ที่สร้างโดยให้ชุดข้อมูลประกอบไปด้วยภาพวงกลม สามเหลี่ยม สี่เหลี่ยม ห้าเหลี่ยม หกเหลี่ยม และแบ่งออกอีก 12 สี ทั้งหมด 60,000 ภาพ แบ่งเป็นข้อมูลในการเรียนรู้ 60% คิดเป็น 36,000 ภาพ และข้อมูลในการทดสอบ 40% คิดเป็น 24,000 ภาพ จากโครงสร้างที่ทำ ทำให้ค่า Accuracy คือ 27.7%



รูปที่ 5 ค่าเฉลี่ยการคาดเดาคำตอบที่ถูก

จากรูปที่ 5 แสดงให้เห็นว่า แคปท์ช่าที่มี 3 รูป มีค่าเฉลี่ยการคาดเดาคำตอบที่ถูกมากกว่าแคปท์ช่าที่มี 4 รูป และแคปท์ช่าที่มี 5 รูป



รูปที่ 6 ค่าเฉลี่ยเวลาที่ใช้ในการคาดเดาคำตอบ

จากรูปที่ 6 แสดงให้เห็นว่า แคปท์ช่าที่มี 3 รูป มีค่าเฉลี่ยเวลาที่ใช้ในการคาดเดาคำตอบน้อยกว่า แคปท์ช่าที่มี 4 รูป และแคปท์ช่าที่มี 5 รูป

อ้างอิง

[1] J. Jaroenjit, A. Panpanasakul, P. Chaisri, P. Promduang, and S. Prompongusawa, "Classification pearls using image processing," in Proceedings of the 9th Hatyai National and International Conference, Thailand, 2014, pp. 1679-1691.

[2] A. Tungkastan and K. Leewun, "Pixel-Based Car Model Detection and Recognition," Engineering Journal of Siam University, vol. 19, January-June, pp. 90–102, 2018.

[3] S. Sarraf and G. Tofighi, "A hybrid sequential feature selection approach for the diagnosis of Alzheimer's Disease," in Proceedings of International Joint Conference on Neural Networks, 2016, pp. 1216-1220.

[4] E. Humphrey and J. Bello, "Rethinking Automatic Chord Recognition with Convolution Neural Networks," in Proceedings of the 11th International Conference on Machine Learning and Application, 2012.

[5] B. Tilmann, "The Business Impact of Predictive Analytics," ed. IGI Global, September-December 2007.

[6] Application of Pattern for New CAPTCHA Generation Idea. [Online]. Available: https://www.researchgate.net/publication/324063212_Application_of_Pattern_for_New_CAPTCHA_Generation_Idea