利用動作辨識破解 reCAPTCHA

指導教授 ：余執彰 副教授　　組員 ：高偉承、張任宏

摘要

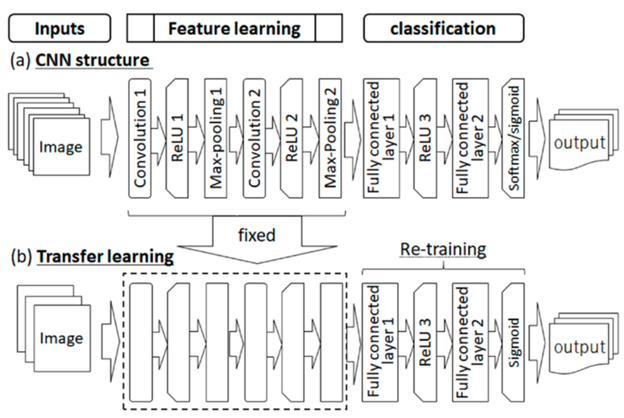
隨著人工智慧的成熟發展，現有的reCAPTCHA圖片驗證已被破解，因此本專題欲提出一解決方案，將物件辨識變更為動作辨識。並嘗試站在攻擊者的角度訓練影像辨識模型，也站在防禦者角度假想不同情境驗證其防禦性。

核心精神是利用Grad-CAM技術得知模型對於圖片的關注區域，重複進行裁切之圖片並優化模型，探討裁切至何種程度的圖片足以區分機器與人類。

技術

Transfer Learning

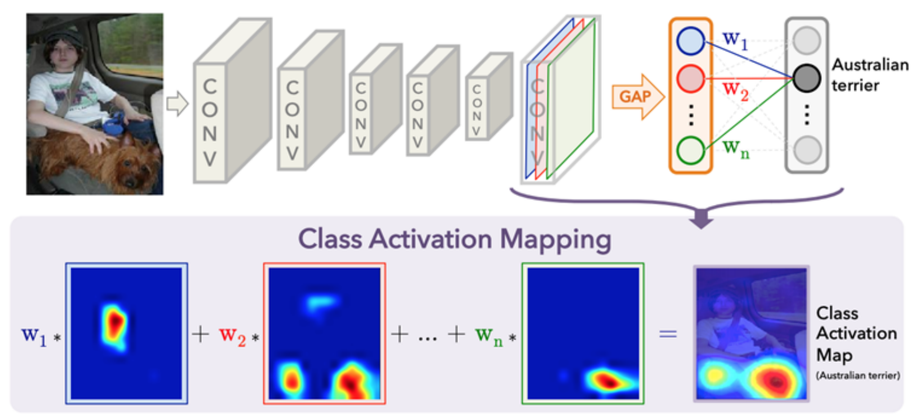
概念是固定神經網路架構中間的卷積層，使模型為圖片作特徵提取，比如圖片的邊邊角角、輪廓，而當模型具備能獲得圖片底層結構的基礎訊息的能力之後，接著重新訓練分類器，再以較低的學習率幫整個模型做微調(Fine-tuning)，來適應新的數據，並為模型帶來更佳的學習成效，帶來的好處是不需要大量訓練資料以及節省訓練時間。



▲ 取自 Convolutional Neural Network Coupled with a Transfer-Learning Approach for Time-Series Flood Predictions

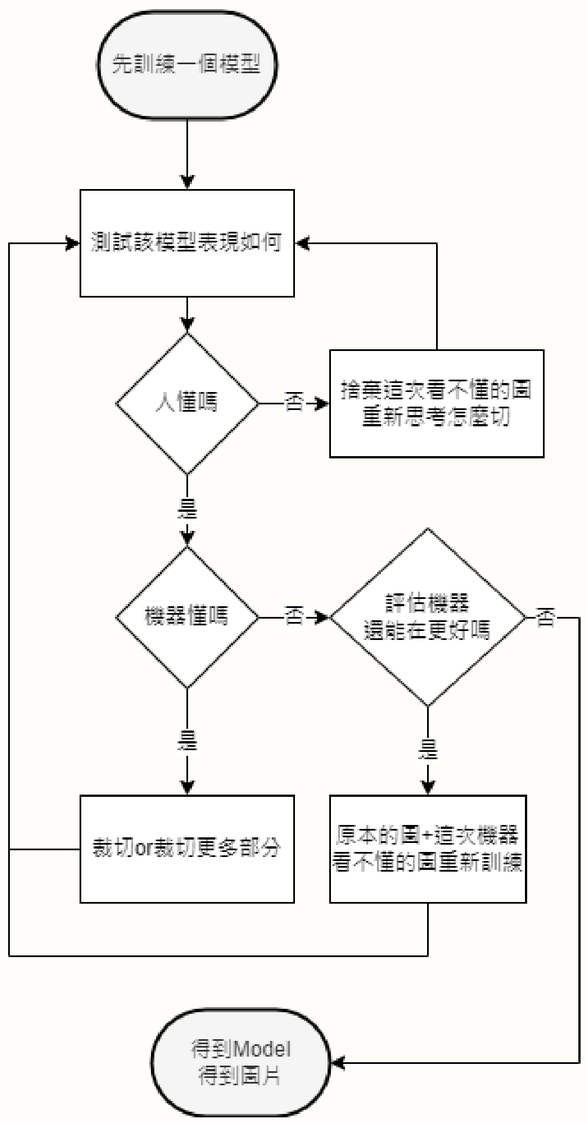
Grad-CAM Picture

此技術用於幫助了解模型專注的區域，其運作原理是利用類似反向傳播(back-propagation)的概念，使得到圖片中各個區域的像素在每一層做運算時的權重，並把這些權重在其對應的像素做堆疊，最後即能得到關注區域熱力圖，只要觀察顏色分布就能幫助理解模型關注的區域。



▲ 取自 Learning Deep Features for Discriminative Localization

流程



結果

	運球	灌籃	投籃	平均
受試人1	99%	77%	94%	90%
受試人2	100%	94%	94%	96%
受試人3	100%	95%	86%	93.67%
受試人4	100%	73%	97%	90%
受試人5	100%	80%	91%	90.33%
受試人6	97%	52%	92%	80.33%
受試人7	99%	68%	86%	84.33%
受試人8	100%	90%	95%	95%
受試人9	99%	98%	89%	95.33%
受試人10	100%	77%	91%	89.33%
受試人11	99%	54%	90%	81%
受試人12	99%	86%	97%	94%
受試人13	98%	72%	92%	87.33%
受試人14	99%	70%	84%	84.33%
受試人15	98%	90%	93%	93.67%
受試人16	100%	74%	79%	84.33%
受試人17	100%	45%	84%	76.33%
受試人18	96%	90%	93%	93%
Model_Fin	94%	64%	70%	76%

▲ 人類與機器辨識結果比較表

本專題實驗驗證，像上圖Level 3一樣，此類去除大量身體部位的圖片能做為reCAPTCHA的防禦機制，且不易被現正流行的圖像辨識攻破。但因為本專題只有三種類別，未來若是能增加同樣是籃球運動中的不同運動，或是增加不同的運動種類，並套用如一樣的實驗過程，相信一定能為這類測試更完整的解釋。