數位發展部
Ministry of Digital Affairs

數位發展部數位產業署

AI 產業實戰應用人才淬煉計畫 x 數據創新服務生態系推動計畫

113 年度 AIGO 潛力新星盃

實戰場域人才選拔競賽

申請文件

解題團隊：花生省魔術

題目名稱：詐騙文件印鑑、關防圖章 AI 辨識

出題單位：高雄市政府警察局-刑事鑑識中心、資訊室

中華民國　113　年 5 月 24 日

※申請團隊保證申請文件所列資料及附件均屬實※

※若有偽造不實者或侵權行為，申請團隊須負完全之法律責任※

一、解題團隊基本資料

(團隊成員須與官網上隊伍相同，請於繳件時於系統確認，不符者計畫辦公室有權取消其領獎資格)

<table>
<tr><td colspan="2">團隊名稱</td><td colspan="4">花生省魔術</td></tr>
<tr><td colspan="2">團隊簡介</td><td colspan="4"></td></tr>
<tr><td colspan="6">團隊成員介紹</td></tr>
<tr><td>N</td><td>角色</td><td>姓名</td><td>人才類型</td><td>任職(就學)單位</td><td>經歷與專長</td></tr>
<tr><td>1</td><td>隊長</td><td>陳佳妘</td><td>AI 相關人員</td><td>陽明交通大學</td><td rowspan="2">1. 研究室為深度學習相關
2. 曾經修習機器學習與深度學習
3. 主要學習領域為利用深度學習於醫學影像分析
4. 多次參與過 kaggle 競賽</td></tr>
<tr><td>2</td><td>隊員</td><td>陳奕涵</td><td>AI 相關人員</td><td>陽明交通大學</td></tr>
</table>

二、解題構想說明（頁數建議 4～8 頁）

（一）解題計畫宗旨及目的

條列重點。闡明：1.出題單位遇到的痛點；2.解題構想的摘要；3.解題構想對實證場域的幫助；4.技術面的突破與創新。

1 高雄市政府警察局刑事鑑識中心目前在偵辦詐騙案件時，主要面臨的痛點：

1.1 印鑑、關防圖章辨識難度高：警方在現場阻止詐騙時，常常無法在短時間內辨識印鑑和關防圖章的真偽，需要將文件回傳至警局進行比對，這樣不僅延誤了蒐證的時效性，還增加了案件偵辦的難度。

1.2 現有資料未能妥善運用：警方目前尚未建立完善的印鑑及關防圖章辨識整合系統，導致現有的資料無法被有效利用，限制了警方在案件偵辦中的效率。

1.3 向上溯源困難：詐騙集團成員以車手居多，幕後主使者往往通過設立多層斷點來掩蓋其身份和行蹤，使警方在偵辦過程中面臨重重困難。

2 解題構想的摘要

2.1 本提案旨在開發一套基於 AI 的印鑑和關防圖章辨識系統，利用生成對抗網絡（ GAN ）、 對比學習、遷移學習和 Vision Transformer （ ViT ）等技術，自動識別和分類詐騙文件上的印鑑和圖章，並進行真偽判斷，提供給警方一個高效、準確的工具來蒐證和分析。

3 解題構想對實證場域的幫助

3.1 提高蒐證效率：系統能夠在現場即時判斷印鑑和關防圖章的真偽，大大提高了警方的蒐證效率。

3.2 數據整合和分析：通過整合現有資料，系統能夠提供詳細的數據分析報告，幫助警方更好地理解和應對詐騙手法。

3.3 溯源和偵查：系統能夠幫助警方識別詐騙集團的層級結構，為深入偵查和向上溯源提供有力支持。

4 技術面的突破與創新

4.1 圖像處理和特徵提取：利用先進的圖像處理技術，自動提取印鑑和圖章的特徵。

4.2 生成對抗網絡（ GAN ）：通過生成假樣本來增強數據集，提升模型的泛化能力和準確性。

4.3 對比學習：無需標籤即可學習有效的特徵表示，增強模型的區分能力。

4.4 遷移學習：利用預訓練模型並在目標數據集上進行微調，提高模型在小數據集上的表現。

4.5 Vision Transformer （ ViT ）：利用 Transformer 架構的強大特徵提取能力，提升印鑑和圖章的識別準確性。

（二）解題技術架構及進行步驟

解題技術架構與步驟說明，其中技術方法請詳細說明 1.採用之方法；2.採用本方法之原因；3.技術流程；4.預計可能遭遇之困難及解決途徑…等相關說明

1 採用之方法

1.1 圖像處理：使用 OpenCV 進行圖像預處理，包括灰度化、二值化、邊緣檢測等。

1.2 生成對抗網絡（ GAN ）：使用 GAN 生成更多的訓練樣本，增強數據集。

1.3 Vision Transformer （ ViT ）：使用 ViT 進行特徵提取和分類。

1.4 多任務學習：通過共享不同任務的表示來提高模型的泛化能力。

1.5 對比學習：進行無監督特徵學習，提取有效的特徵表示。

1.6 相似度比較：利用 DNN 分別處理真實與偽造印章的特徵，最後計算兩者的匹配度。

2 採用本方法之原因

2.1 圖像處理：OpenCV 是一個強大的圖像處理庫，能夠高效地進行圖像預處理。

2.2 特徵提取：使用預訓練的 CNN 模型進行特徵提取有助於節省計算資源和時間，改善模型性能，有效處理小數據集，並利用大規模數據集的學習能力。

2.3 生成對抗網絡（ GAN ）：GAN 能夠生成逼真的數據樣本，增強數據集的多樣性，提升模型的泛化能力。

2.4 Vision Transformer （ ViT ）： ViT 能夠捕捉圖像中的全局信息，提升分類的準確性和泛化能力。

2.5 多任務學習：透過共項任務之間的訊息和特徵，優化每個任務的結果。

2.6 對比學習：對比學習能夠在無需標籤的情況下學習有效的特徵表示，適合於標籤數據有限的情況。

2.7 DNN：能夠自動從數據中學習到有用的特徵，而無需手工設計特徵。這在圖像處理任務中尤為重要，因為手工設計的特徵可能無法捕捉到所有的細節和複雜性。

3 技術流程

3.1 數據預處理：

3.1.1 加載和灰度化圖像。

3.1.2 使用 OpenCV 進行二值化和邊緣檢測。

3.2 數據增強

3.2.1 使用生成對抗網絡（GAN）生成更多訓練樣本來增強數據集：通過 GAN 生成更多的印章圖像來擴展訓練數據集。這有助於模型更好地學習印章特徵。

3.2.2 利用 Vision Transformer（ViT）來改進生成模型性能：使用 ViT 來改進 GAN 的性能，生成更高質量和更多樣化的印章圖像。

3.3 多任務模型設計

3.3.1 結合深度神經網絡（DNN）和對比學習（Contrastive Learning）：設計一個多任務模型，主幹網絡使用 DNN 來提取印章的特徵。模型包括兩個主要任務：

3.3.1.1 印章相似度比較：利用 DNN 模型來尋找與給定印章最相似的印章。

3.3.1.2 印章特徵提取：提取印章的特徵表示，這些表示可以用於後續的分類或檢索。

3.4 對比學習模塊

3.4.1 對比學習損失函數：引入對比學習損失函數，例如對比損失（Contrastive Loss）或 InfoNCE 損失，用於在主幹網絡的特徵空間中進行對比學習。

3.4.2 正負樣本選擇：通過數據增強或其他策略生成正負樣本對。正樣本是同一輸入的不同增強版本，負樣本是不同輸入的特徵表示。

3.5 訓練過程

3.5.1 聯合訓練：同時訓練多任務損失函數和對比學習損失函數。總損失是各任務損失和對比損失的加權和。

3.5.1.1 任務損失（Task Loss）：每個任務的標準損失函數（如分類的交叉熵損失、回歸的均方誤差損失等）。

3.5.1.2 對比損失（Contrastive Loss）：用於增強特徵表示的判別能力。

3.5.2 優化器選擇：使用常見的優化器（如 Adam、SGD）來最小化聯合損失函數。

3.6 模型評估與調優

3.6.1 評估指標：根據每個任務的特點選擇合適的評估指標（如相似度比較的準確率、特徵提取的表示質量等）。

3.6.2 模型調優：通過調整模型架構、超參數（如學習率、損失權重）等來優化模型性能。

4 預計可能遭遇之困難及解決途徑

4.1 數據品質問題：可能遇到圖像品質差、噪聲多的問題。解決方法包括圖像增強技術和數據清洗。

4.2 模型準確率不足：初期模型準確率可能不足。解決方法包括增加數據量、進行模型調優和使用生成式 AI 進行數據增強。

4.3 實時性要求：系統需要在現場即時判斷，對運算速度要求高。解決方法包括優化算法和使用高效的硬件設備。

（三）數據應用及作法

請詳述預期使用的數據資料來源、資料類型格式及內容欄位，請包含但不限於：1.出題單位釋出之數據資料欄位；2.自行額外使用的數據資料（包含第三方數據、Open Data 或其他網路公開資訊）與資料集描述；3.數據將會如何處理、疊合混搭與加值方法

1 出題單位釋出之數據資料欄位

1.1 詐騙案件面交文件圖像（JPG 或 PNG 格式）。

1.2 機關關防和公司印鑑影像圖像。

2 自行額外使用的數據資料

2.1 來自公開數據集和網絡的其他印鑑和圖章圖像。

2.2 如政府公開的公章樣本數據庫。

2.3 使用 GAN 生成與正確的印鑑或圖章相似的圖樣來模擬偽造影像

3 數據將會如何處理、疊合混搭與加值方法

3.1 數據清洗：對數據進行去噪、增強和標註。

3.2 數據增強：使用 GAN 生成更多樣本，增強數據集多樣性。

3.3 數據融合：將多來源數據進行融合，擴展數據集規模和覆蓋範圍。

3.4 加值分析：通過數據分析和特徵提取，為每個印鑑和圖章生成詳細的分析報告。

（四）預期完成之工作目標(KPI)

請列述在執行期限內預期完成之工作項目。解題目標內容應完整、明確，並須列出量化指標。

1. 印鑑和關防圖章辨識準確率：達到 90%以上。
2. 圖章重疊比對準確率：達到 95%以上。
3. 系統反應時間：在現場進行即時判斷，反應時間不超過 1 秒。
4. 數據集規模：擴展數據集至 1000 張以上圖像。
5. 使用者滿意度：獲得 85%以上使用者的滿意反饋。

（五）預期工作摘要及進度表（請依解題構想安排自行增減欄位）

月份	預定工作及階段目標
7	確定需要的數據後，開始大量收集，確保擁有不同類型、尺寸和解析度的印章圖片，並利用數據增強生成更多樣化的資料後，透過簡單的分析了解資料的分佈情況，同時閱讀相關文獻。
8	開始建構模型，使用 SimCLR 對資料進行特徵提取，以及對 Pretrained ResNet 模型進行 fine-tune，並將訓練結果記錄下來。
9	利用 fine-tune 後的 ViT 進行初步訓練後，將 SimCLR、ResNet 和 ViT 三個模型結合，訓練特徵提取和分類實驗的模型，並比較不同模型和結合與否的優劣。
10	針對結果進行優化和評估，開發初步的印章真偽判定模型後，不斷地測試並調整模型。

（六）預期成果與效益

預期成果形式如專利、論文、專著、設備、軟體等，須注意產出之智慧財產權歸屬由出題單位與解題團隊共同議定。

1. 開發出一個高效又準確的印鑑真為判定系統，能夠快速的識別和分類各種不同類型的印鑑，提高警方現場辦案的效率。
2. 收集大規模的數據，以及利用數據增強技術，充分挖掘和利用現有的數據庫，減少收集成本以及對於標記資料的依賴。

3. 透過深度學習技術，為警方提供智能化的偵查工具，減少人為錯誤帶來的成本。
4. 透過 AI 的應用，提升警方在偵查時的技能，使其能夠更好的對付日益複雜的犯罪手法。
5. 在實際應用中驗證模型結果，收集反饋並持續優化，確保系統在不同場景下的穩定性後，開發成一個軟體。

（七）其他有利審查項目（選填，無則免填）

如相關產業實績、競賽得獎證明、隊員學經歷、學術、技術證明等，請重點摘要條列。

1. 團隊全體成員均為陽明交通大學統計研究所的研究生。
2. 長期專注於深度學習、生成式 AI、電腦視覺等人工智能前沿技術的研究。
3. 具備參與數據競賽如 Kaggle 等經驗。
4. 擅長將統計理論與深度學習方法相結合,提出創新的解決方案。