PyTorch 人臉辨識模型實作

■ 課程介紹

人臉辨識(Face Recognition)是電腦視覺中最重要的應用之一，已廣泛運用於機場自動通關、智慧門禁、手機解鎖，到社群媒體中自動標記功能等場景。隨著深度學習技術快速進展，人臉辨識在多項公開測評中表現優異，數據顯示其精準度已跨越人類辨識的門檻，具備高度可靠的實務應用價值。然而，要建立一套穩定且高效的人臉辨識系統，仍需理解背後複雜的模型架構、訓練方法與系統設計等實作流程。

本課程將以「深度學習基礎影像分類模型」開始，帶領學員剖析人臉辨識的演進脈絡，逐步介紹目前最主流的人臉辨識技術。從早期基於 Softmax Loss 的人臉分類模型，到後來能有效提升辨識能力的 Triplet Loss 與 Angular Margin Loss 系列方法(SphereFace、CosFace、ArcFace)，再進一步介紹近年提出的 CurricularFace、ElasticFace 與 AdaFace 等更先進的 loss function，使模型在不同品質與難度的人臉影像下仍能保持良好的辨識能力。

人臉偵測(Face Detection)方面，本課程將介紹從早期的 Dlib 與 MTCNN，到目前業界廣泛使用的 RetinaFace 與 SCRFD 等高效能人臉偵測模型，說明如何利用 YOLO 系列模型訓練專用的人臉偵測器。透過這些模型，學員將了解完整的人臉辨識系統是如何從一張影像中偵測人臉、進行對齊(Face Alignment)，再輸入人臉辨識模型產生人臉特徵向量(Face Embedding)，並利用距離度量完成身份辨識。

此外，本課程也將介紹近年逐漸興起的 Transformer 架構在人臉辨識中的應用，例如 Face Transformer 與 SwinFace 等模型，說明 CNN 與 Transformer 在人臉辨識任務中的差異與優勢。

除了辨識技術，本課程亦關注近年備受重視的「隱私與安全議題」。在社群媒體盛行的當下，日常照片分享正無形中洩露您的生物特徵。近年來的研究顯示，透過對抗攻擊(Adversarial Attack)或生成模型，可以在幾乎不影響人類視覺的情況下，使人臉辨識模型無法正確辨識身份。本課程將介紹 FGSM 與 PGD 等對抗攻擊方法，以及如何利用生成模型(如 StyleGAN)進行人臉影像修改與 StyleGAN inversion 技術，以達到隱私保護或模型攻擊的目的。

■ 課程目標

1. 熟悉 Python 與 PyTorch 深度學習框架
2. 瞭解人臉辨識技術的演進、架構與核心理論
3. 建立完整的人臉辨識系統（Face Detection → Recognition）
4. 訓練與比較不同的人臉辨識 loss function
5. 瞭解 Transformer 在電腦視覺中的應用
6. 掌握生成模型與對抗攻擊在人臉辨識中的應用

■ 課程對象

1. 影像處理、電腦視覺與安控系統相關從業者
2. 欲了解 CNN 與 Transformer 於視覺任務差異與應用的開發者
3. 對生物特徵資訊安全與個人隱私防護有需求的資安人員
4. 未來可銜接進階生成式 AI 或多模態技術的工程與研究人員
5. 具 Python 程式基礎、希望透過完整專案實作進入 AI 領域的學生與轉職者

■ 課程大綱

Day1.人臉辨識系統核心技術

課程大綱	內容
深度學習影像分類模型	■ 深度學習影像辨識的基礎與發展： – AlexNet – VGG – GoogLeNet – ResNet – EfficientNet – Vision Transformer (ViT) ■ CNN 與 Transformer 架構比較與應用
人臉偵測模型（Face Detection） <各世代的人臉偵測技術>	■ 早期方法 – Haar Cascade – Dlib ■ 深度學習人臉偵測模型 – MTCNN – RetinaFace – SCRFD ■ 即時物件偵測模型 – YOLOv1 – YOLOv13 – YOLO-based Face Detection ■ 實作： – 使用 WIDER FACE dataset 訓練 YOLO 人臉偵測模型 – 比較 MTCNN、RetinaFace、SCRFD 與 YOLO 的效果差異

課程大綱	內容
人臉對齊（Face Alignment）	■ 介紹人臉關鍵點偵測與對齊技術 – 5-point alignment – 68-point landmarks – similarity transform ■ 說明對齊對人臉辨識精度的重要影響

Day2.人臉辨識模型與損失函數

課程大綱	內容
人臉辨識模型（Face Recognition）	■ 介紹人臉辨識模型的核心概念： – Face embedding – cosine similarity – identity verification vs identification ■ 常見 backbone： – ResNet – MobileFaceNet – ConvNeXt ■ Transformer-based face recognition： – Face Transformer – SwinFace
人臉辨識 Loss Function 發展 <分類 到 metric learning 的演進	■ 基礎方法 – Softmax Loss ■ Metric Learning: – Triplet Loss ■ Angular Margin Loss: – SphereFace – CosFace – ArcFace ■ 新一代人臉辨識 Loss: – CurricularFace – ElasticFace – AdaFace ■ 實作： • 使用 CASIA-WebFace 訓練不同 loss function 的模型並比較效果
人臉辨識資料集與評估方法	■ 常見資料集 – CASIA-WebFace – MS1M – VGGFace2 ■ 評估資料集 – LFW

課程大綱	內容
	– MegaFace – IJB-C ■ 評估指標 – Verification accuracy – ROC curve – TAR / FAR

Day3.人臉生成與隱私保護模型

課程大綱	內容
生成模型與人臉影像生成	■ 生成式模型基礎： – GAN-based models • DCGAN • StyleGAN • StyleGAN2 / StyleGAN3 – Diffusion-based models • DDPM • DDIM • Latent Diffusion Model • Stable Diffusion
StyleGAN inversion 與人臉影像編輯	■ 介紹 StyleGAN inversion 技術： – GAN inversion – latent space editing – identity manipulation ■ 應用： – 年齡修改 – 表情修改 – 人臉辨識攻擊 – 隱私保護
對抗攻擊（Adversarial Attack）	■ 介紹對抗攻擊在人臉辨識中的應用： – FGSM – PGD ■ 實作： – 攻擊圖片分類模型 ■ 攻擊人臉辨識模型
基於生成模型的人臉隱私保護	■ 生成模型在人臉隱私保護中的應用： – CLIP2Protect – adversarial identity perturbation – privacy-preserving face modification

★ 本課程所有實作均使用 PyTorch 深度學習框架，並在 Google Colab 雲端環境 上進行。

★ 課程將提供完整資料集與程式範例，使學者能在短時間掌握人臉辨識系統設計與實作方法。

■ 講師簡介-林哲聰 老師

學歷：

台灣大學應用力學研究所碩士/清華大學資訊工程研究所博士

現職：

瑞典自駕車軟體開發公司 Zenseact(Volvo Cars)深度學習工程師

經歷：

馬來西亞偉特科技公司(ViTrox)研發顧問
馬來西亞 10 EPOCH 科技公司研發顧問
工研院機械所副研究員/研究員/資深研究員
加州大學聖塔芭芭拉分校資工系訪問研究員
上奇資訊-計算機概論 共同譯者
2010 伽利略創新大賽 台灣區季軍
2011 伽利略創新大賽 特別獎(GNSS Living Lab)得主
2013 伽利略創新大賽 瑞士區冠軍
2016 日本立命館大學英文演講比賽 清華大學代表
2017 CVGIP 行人偵測競賽 亞軍
2017 MOST 生成式對抗網路競賽 佳作
2018 第八屆兩岸清華研究生學術論壇 清華大學代表
2019 IEEE ICIP Three Minute Thesis Competition (3MT®): Finalist
2020 AI 智慧應用新世代人才培育計畫-人才解題實證(倒車攝影機影像識別-障礙物與逼近偵測)：佳作
2020 中華民國影像處理與圖形識別學會第十三屆博碩士論文獎博士論文佳作

專長：

Computer Vision, Image Processing, Pattern Recognition, Machine Learning, Deep Learning, Python/C/C++ Programming 已於電腦視覺/深度學習/駕駛輔助/自駕車領域中發表過 37 篇國際論文，15 篇國內論文，以及 13 篇專利

【 開 課 資 訊 】

- **主辦單位**：工研院產業學院 台北學習中心
- **舉辦地點**：線上直播會議室 (使用 WEBEX 線上會議室，將於課前寄發信件通知)
- **上課時間**：115/08/01、08/08、08/15 (六)，13:00~17:00 (每天 4 小時，共三天 12 小時)
- **招生人數**：本班預計 20 人為原則，最低開課門檻為 12 人
- **課程費用**：

報名方案	費用
課程原價	每人 10,800 元
早鳥價 (開課前 3 週)	每人 9,800 元
團報價 (三人以上)	每人 9,200 元

- **課程洽詢**：02-2370-1111 *316 李小姐
- **注意事項**：
  1. 為確保您的上課權益，報名後若未收到任何回覆，敬請來電洽詢方完成報名。
  2. 若原報名者因故不克參加，但欲更換他人參加，敬請於開課前三工作日通知。
  3. 配合講師時間或臨時突發事件，主辦單位有調整日期或更換講師之權利。
  4. 報名時請註明欲開立發票完整抬頭，以利開立收據；**未註明者，一律開立個人抬頭**，恕不接受更換發票之要求。
  5. 為尊重講師之智慧財產權，課程進行中請勿錄音及錄影。