看戲還是看人——現代川劇變臉秀

◆ 社團法人台灣 E 化資安分析管理協會、屏東大學電腦科學與人工智慧學系博士 — 翁麒耀

人臉辨識技術已廣泛應用於生活中，例如差勤打卡、金融交易與汽車駕控等。這些應用對人臉辨識準確度有極高要求，不過其究竟要如何知道所用的臉是真的？還是偽造的？

關於 AI 技術的大小事

人工智慧（Artificial Intelligence, AI）一詞是由美國約翰・麥卡錫（John McCarthy）於 1955 年首度提出，隔年在達特矛斯會議（The Dartmouth Workshop）受到大家熱烈討論，與會人士均相信 AI 終有一天能勝過人類的頭腦；不過，在當時 AI 技術只是紙上談兵。

約翰 · 麥卡錫於 1956 年的達特矛斯會議提出「人工智慧」一詞，被稱為「人工智慧之父」，而在會議前後，他主要的研究方向是電腦下棋。（Photo Credit: Trustees of Dartmouth College, https://250.dartmouth.edu/highlights/artificial-intelligence-ai-coined-dartmouth; HAI, Stanford University, photo by Chuck Painter, https://hai.stanford.edu/news/stanford-ais-legacy-through-decades）

2017 年底，美國電動車特斯拉公司研發的自駕車已能從洛杉磯一路開到紐約，無需任何人工操作。執行長馬斯克更聲稱，能全自動駕駛的電動車即將全面上市。然而，究竟特斯拉公司是如何達成全自動駕駛呢？其關鍵核心即在於 AI 技術。

一般而言，AI 技術就是在建立仿人類行為，其過程包含感知、學習、推論及校正等四個階段。感知階段：把感知的動作或行為運用數據的方式來描述這些特徵，例如，人類的喜歡表情，使用數值 123 至 777 來表示；學習階段：利用學習模式來量測與分類特徵；推論階段：將學習階段所獲得的特徵直接測試並得到結果，舉例來說，就是把一個軍人經過長期的訓練，通過了軍中考核，能獨當一面的作戰；校正階段：為自我調整階段，當無法自我調整到最佳結果時，可再返回學習階段或推論階段。

當以 AI 技術把電腦或機器訓練成與人類思考模式一模一樣時，其將可能超越人類智慧。最典型案例就是在 2016 年的 AlphaGo 電腦與南韓圍棋棋王間展開的世紀對決。結果，南韓棋王不敵 AI 電腦而落敗，這讓企業家發現 AI 的重要性，而願意投入更多資金來發展。

目前我國已於臺南沙崙打造出全臺首座自駕車實驗場域，能供國內各界共同研發無人車技術，不讓進口車專美於

2016 年，AlphaGo 電腦與南韓圍棋棋王展開世紀對決，結果南韓棋王以 1：4 不敵 AI 電腦落敗。（Photo Credit: DeepMind, AlphaGo, https://www.alphagomovie.com/gallery）

我國已於臺南沙崙打造出首座自駕車實驗場域，能供國內各界共同研發無人車技術。（圖片來源：臺南市政府，https://www.tainan.gov.tw/news_content.aspx?n=13370&s=3742042#）

前。工研院指出，從 Google 搜尋引擎、Facebook 貼文推播、Netflix 影片推薦，到自駕車、無人機創新應用，AI 演算法無所不在。為管理 AI 帶來風險，各國開始將 AI 治理納入法規。數位發展部唐鳳部長強調 AI 跟我們的關係就像哆啦 A 夢跟大雄般，人才是主體，AI 只是輔助，應讓 AI 配合民主社會價值，而不是受 AI 控制。

人工智慧的應用

近年來 AI 迅速發展，已有為數眾多的 AI 技術應用在生活中。

一、搜尋建議

當消費者在網頁上搜尋，AI 技術就可運用過去的搜尋資訊和消費者的消費資訊來協助探索資料，以開發或設計出最佳的銷售策略。舉例來說，網路上的零售商，可在顧客瀏覽商品網頁時，根據瀏覽過的商品提出優惠商品組合給消費者選擇。

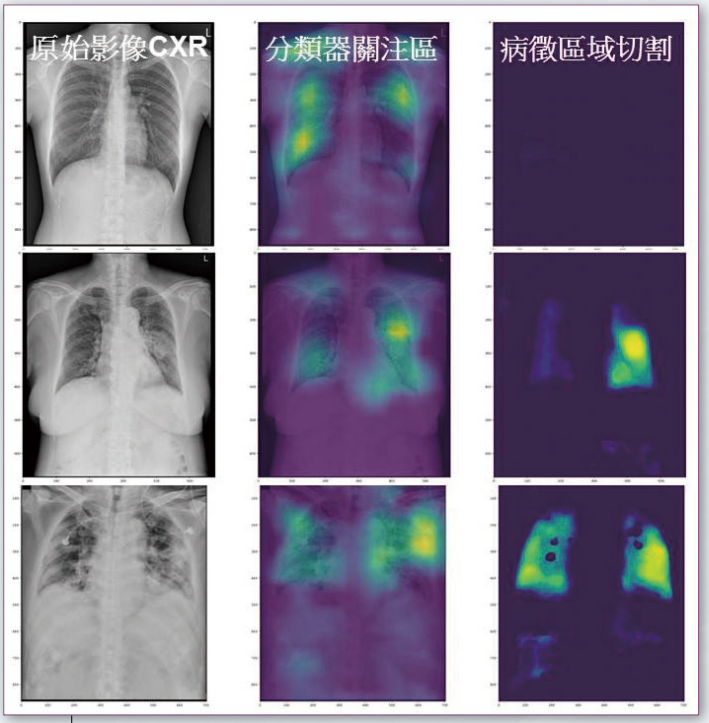
二、線上客服

過去服務人員親自在線上答覆，改以聊天機器人取代。聊天機器人可以制式地回覆某些客人問題，例如常見問題（FAQ）、個人化推薦與建議顧客尺寸等，像是 Netflix 會推薦您喜愛的類型影片等亦屬之。

三、自動化交易

適用於股市交易市場。設計專門的股票投資組合，從投資組合中找出最佳的投資策略，並設計以 AI 驅動的交易平臺，讓電腦每天自動完成數千筆或數百萬筆的股票交易。

現今許多行動裝置已將語音辨識功能納入系統中，以便使用語音搜尋功能。



成大醫院研發團隊開發肺炎之 X 光片自動判讀輔助系統，透過 AI 演算法輔助並找出疑似新冠肺炎病徵，加速醫師判讀時間；圖為正常（上）、肺炎（中）、新冠肺炎（下）之肺部 X 光片影像。（圖片來源：財團法人生技醫療科技政策研究中心，https://innoaward.taiwan-healthcare.org/award_detail.php?REFDOCTYPID=0mge2qqssdm4fd72&num=2&typeId=&REFDOCID=0qls5ajbsi3fqpfs）

四、語音辨識

能將人類語音轉成文字。現今許多行動裝置已將語音辨識功能納入系統中，以便使用語音搜尋功能，例如 Apple 裝置中的 Siri。

五、電腦視覺

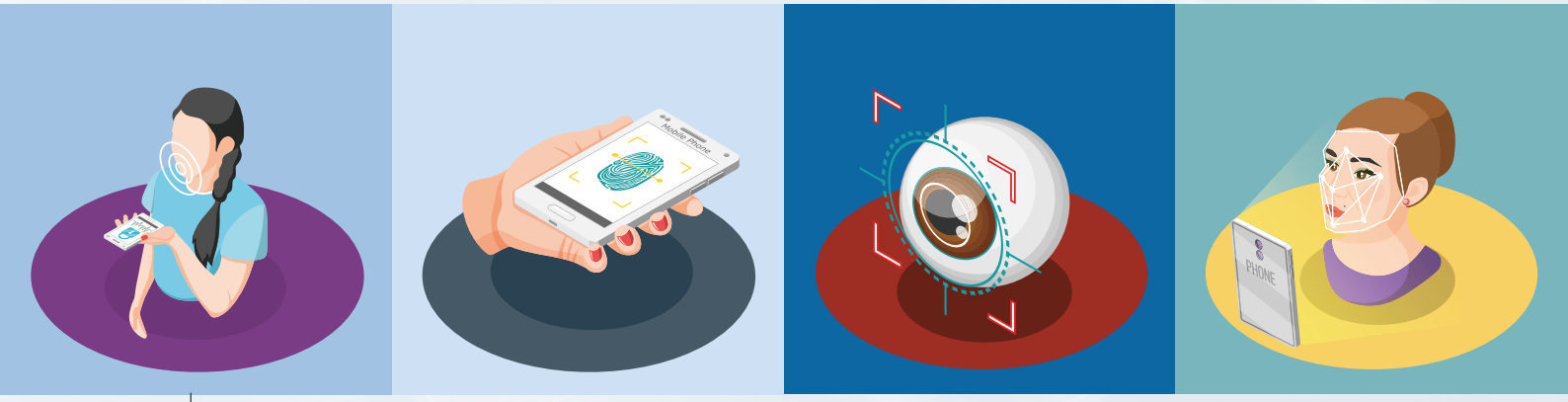
AI 技術可以從數位影像中獲得有意義的資訊，以供使用者採取行動。例如，新冠肺炎的 X 光片或是腫瘤影像，能結合社群媒體來標記照片，進行病理預測，成就醫療技術的智慧轉型。

解密人臉辨識手法

許多程式及系統的驗證機制是以人臉辨識系統為主，像是 Apple 裝置使用 Face ID 作為臉部解鎖依據。人臉辨識系統是 AI 技術範疇之一，其如何成為大部分系統所使用的技術呢？

人臉辨識系統使用的就是生物辨識技術。所謂「生物辨識」是以統計方式對生物外相進行分析，多利用人體本身的生物特徵，如：聲音、臉部、指紋、掌靜脈、虹膜、視網膜等。某些生物特徵會因其他因素而被破壞，因而導致辨識失敗。以指紋為例，當手指面受傷，指紋特徵即被毀損而難以辨識。

人臉辨識是擷取不同狀態的人臉影像來分析比對（如側臉、微笑或戴眼鏡等），相較於指紋或虹膜等生物特徵辨識方式，人臉辨識不需要近距離接觸，且其特徵被破壞的機率較少，故辨識的準確率也高於



「生物辨識」是以統計方式對生物外相進行分析，多利用人體本身的生物特徵，如：聲音、指紋、虹膜、臉部等。

其他生物特徵。各項生物特徵辨識的優缺點如表 1。

臉部辨識的基礎概念是「身分識別」，因為每個人的臉部特徵都不一樣（即使是雙胞胎也會不一樣），系統可將每個人的特徵建立資料庫來管理。當系統進行臉部辨識時，是將人臉影像轉成電腦可識別的資訊（如臉部特徵值），再從資料庫中篩選與比對結果相符的資料，以辨識真實身分。惟當不同廠商使用不同的系統時，即使是同一張臉或同一張照片，也有可能出現不同的識別結果。

雖然人臉辨識系統的精準度很高，然仍會受以下因素影響：

一、資料量多寡

臉部辨識正確與否，決定於臉部資料庫中是否能找到正確的身分。若資料庫多是西方白色人種，缺少亞洲人的臉部資料，在進行亞洲人臉辨識時，錯誤率就會偏高。

二、圖像解析度

當進行人臉辨識時，臉部的拍攝角度及光源的明亮度都會影響臉部擷取的資訊，辨識精準度也會受影像的解析度影響。

表 1　生物辨識的優缺點整理

類型	人臉	虹膜與網膜	指紋
辨識方式	利用臉部器官間距、臉部骨骼等作為判別依據	利用虹膜與視網膜的影像作為判別依據	利用手指指腹紋線交叉情形作為判別依據
優　　點	・不必接觸辨識機器 ・應用領域廣	・不必接觸辨識機器 ・程序簡單	・準確性高 ・認證程序簡易 ・適用多樣化的設備
缺　　點	・辨識時間較久 ・易受外部干擾	・設備昂貴 ・使用者易產生抗拒心態	・被偽造的可能性高 ・毀損時難以辨識

三、特徵的變化

因疫情關係，民眾隨時需配戴口罩，亦有民眾喜歡配戴墨鏡或是帽子等，這些情況都可能影響臉部辨識的精準度。此外，隨著年齡的增長，臉部特徵也會跟著變化。

臉部辨識應用範圍

一、快速通關

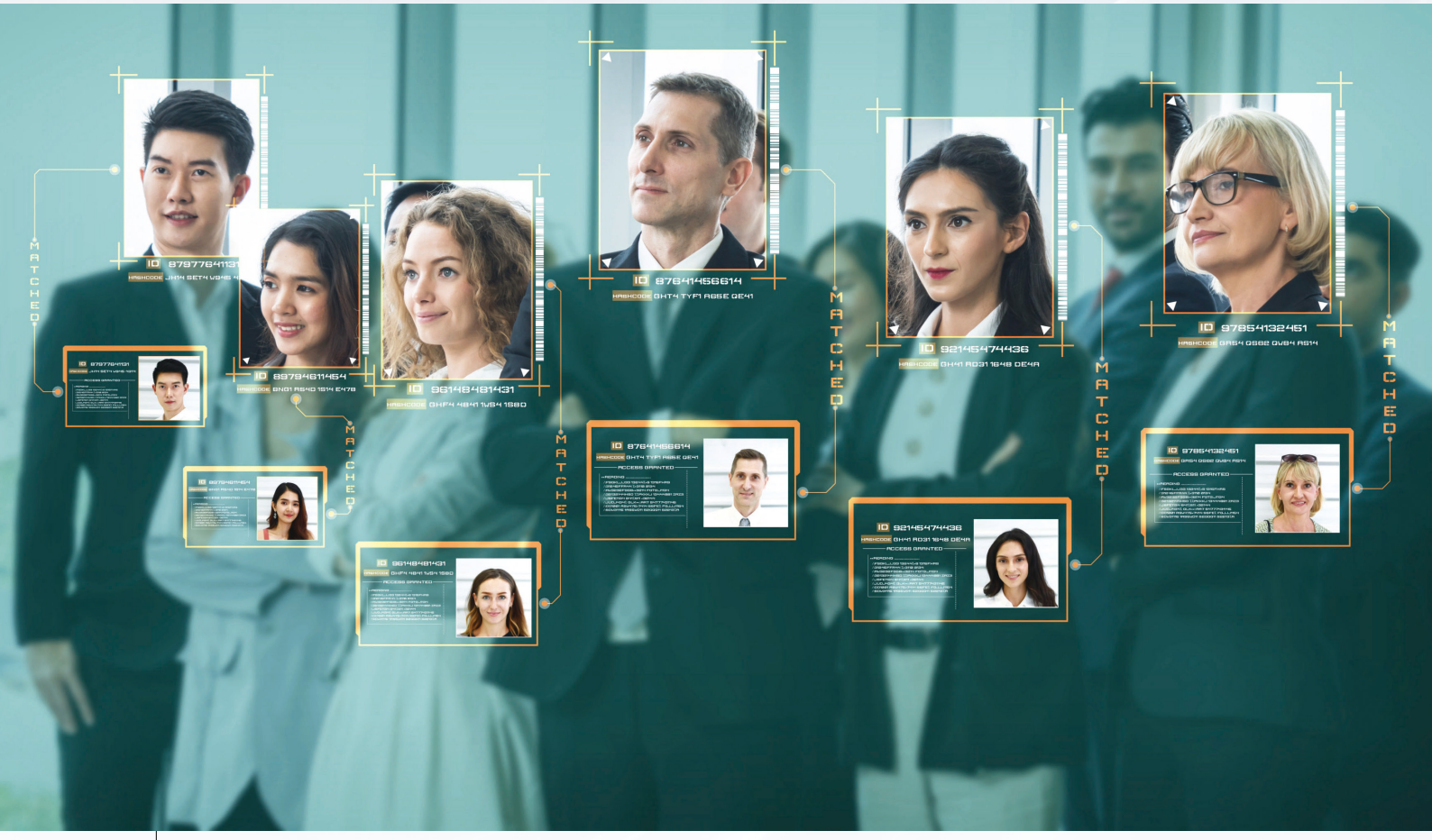
最常見的例子就是政府設置於國際機場內之出入身分驗證關卡。民眾可透過臉部辨識、指紋感應再加上掃描護照來快速通關，以節省通關時間。

二、門禁系統

門禁系統是最常見的應用方式。早期門禁系統是刷員工證後才得以進入公司，然刷員工證易產生弊端。因此，現今許多企業或政府機關都使用人臉辨識進行差勤管理，亦能防止非法人士任意進出，有遏止犯罪的效果。

三、交易付款

中國大陸的支付寶、微信已從電子支付到支援刷臉付款的技術。消費者至店家消費，進行臉部辨識就能快速完成付款，能縮短結帳時間。



雖然人臉辨識系統的精準度很高，但仍會受資料量多寡、圖像解析度以及特徵的變化等因素影響辨識度。

機場設置的快速通關主要透過臉部辨識或指紋感應來驗證身分。（圖片來源：桃園國際機場 FB，https://www.facebook.com/photo/?fbid=557316669528979&set=pcb.557317109528935）

中國大陸市場上支援刷臉付款的技術已普及運用，然其存在的隱私權爭議與資安風險仍備受矚目。

四、Face ID

Face ID 臉部解鎖功能已漸漸成為行動裝置中的必備技術之一。其解鎖速度更快，且可避免因生物特徵的改變，像是手指潮濕、手指有異物等而影響手機解鎖。

人臉辨識系統之美麗與哀愁

雖然 AI 技術提供人臉辨識系統，便利人類生活，但 AI 技術卻也被有心人士運用，以牟取不法利益。例如，當運用 AI 的 DeepFake 技術，惡意偽造某人臉孔，做其未做的事或說其未說的話，便會造成當事人名譽或金錢損失，嚴重者甚至會引發國家安全危機。

網路上曾流傳一則美國前總統歐巴馬被 DeepFake 的影片。事實上，這個影片是由好萊塢導演 Jordan Peele 和美國網路新聞媒體公司 Buzzfeed 所共同製作的，目的是在提醒民眾，眼見不為憑，以警示偽造訊息所帶來的威脅。

臉部辨識系統在當今生活已占有一席之地，對企業而言，人臉辨識系統能節省人力、提升業績與增加收益，然其仍存在隱私權爭議與資安風險；若沒有完善的安全機制，倘遭惡意者竊取，致使公司員工甚至顧客資料遭濫用，恐怕企業將得不償失。

社團法人台灣 E 化資安分析管理協會（ESAM）