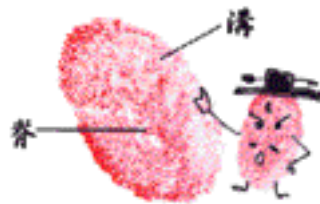


# 啟動人體辨識系統的 生物科技

華銀徵信室 李慧瑜

## 一、前言

阿富汗恐怖份子引爆了震驚全球的911攻擊事件，全球安檢亮紅燈！當鑰匙、密碼、門禁卡再也擋不住這些恐怖攻擊之際，生物辨識技術順勢成了當紅炸子雞！近來層出不窮的提款機詐領事件，讓社會大眾人心惶惶，一般傳統的簽名、印章比對或數字密碼等辨認身份的方法頻頻被仿冒或盜用，加上電腦駭客、針孔攝影入侵事件頻傳，就算設定密碼也不一定安全，因此利用人體獨一無二的「身分密碼」所開發出的「生物辨識系統」，便成為現今業者積極研發的新興領域。電影《將計就計》情節當中，女主角凱薩琳·麗塔瓊斯想進入亞洲金融資訊中心，第一步先是透過指紋、聲紋比對，接著就是眼睛瞳孔、臉部和體溫心跳辨識，經過層層的身體辨識關卡，才能進入金融電腦系統，這就是「生物辨識」。「七」、「不可能的任務」等系列電影中，情報員以錄音的聲紋、拷貝的指紋通過身分辨識系統，取得機密資料的熟悉場景俯拾即是……但，這絕不是電影虛構情節或遙不可及的技術，因為，它已在你我生活中實現了！



指紋辨識系統

(圖片來源：科學小芽子)

## 二、何謂生物辨識系統？

什麼是「生物辨識(Biometric)系統」？生物辨識系統是利用每個人獨一無二的生理或行為特徵來辨識使用者的身分。運用生物辨識技術，你的身體就是密碼，不必再背一長串惱人的數字，不怕遺失或忘記，不易複製，不用擔心遭人盜用，而且「隨身攜帶」。

生物辨識(Biometric)系統，是指透過人體指紋、臉部、聲音或虹膜等身體器官組織的獨特性來辨識使用者身分的一項技術。主要是運用人體身上的特徵做

為識別密碼，因此在技術的開發上必須選擇一些準確度高、容易使用的辨識特徵以利使用。技術開發上，主要可分為生理上的（如臉形、指紋、虹膜）或是獨特的行為模式（如聲音、簽名、密碼）。就準確度來說，「生理特徵」在唯一性及安全性上明顯優於「行為特徵」。目前生物辨識核心技術的發展，指紋辨識佔技術比率54%，簽名辨識佔技術比率21%，臉部辨識佔技術比率16%，虹膜辨識佔技術比率9%。市面上以「指紋辨識」技術較成熟，市場占有率最高，其次則為成長速度最快的「臉部辨識」技術。「虹膜辨識」的準確度最高，但是由於使用上必需以紅外線掃描眼球，在價格及安全性的考慮下，並不容易發展成大眾化的產品，相對的市場占有率也無法迅速拓展。其餘生物辨識科技則仍受一般消費者的使用習慣、可接受度以及經濟價格因素影響，成長較緩慢。

隨著網路安全愈受重視，捨棄煩人密碼、回歸以人體特徵作為辨識主體的「生物辨識系統」已成一股新浪潮，目前包括英特爾、微軟及摩托羅拉等國際大廠，紛紛投入經費，試圖將生物辨識技術整合到未來的網路產品上。雷曼兄弟投資銀行（Lehman Brothers）預測，未來5年生物辨識系統的市場，將自現在每年的5億8千萬美元，以400%的速度快速成長。微軟創辦人比爾·蓋茲更指出，「生物辨識系統將是21世紀最重要的應用技術之一。」

### 三、生物辨識技術的應用

#### 1. 指紋辨識

在過去，指紋的紀錄，是要將十指沾滿油墨，一一拓印到白紙。現在則是以特殊設備來取代以往的不便。使用者只要花四、五千元台幣，買一部像滑鼠大小的光學感應器，搭配相關軟體，就可以儲存自己的指紋檔案。為了提高辨識的準確度，現在更開發出矽晶式的感應設備，藉由偵測指紋上所帶的正負電荷，可以描繪出包含紋路形狀、深淺的3D立體影像。同時為了確保接受辨識的指紋是來自活體，有些感應器還加裝溫度、溼度的感測，以免歹徒惡意剝下他人手指後冒充身分。

基本上，胎兒在六個月大時，指紋就已完全形成，一直到人老死，指紋的紋路和結構幾乎都不會改變。換句話說，要找到相同兩人的指紋的機率微乎其

微，它的發生率約為十億分之一。甚至每個人的十根手指頭的紋路也不相同，加上指紋不易發生變化，則顯示穩定性夠，也就足以讓人採信，成為身分確認的方式之一。

使用者將手指放在專用指紋讀取設備，讀取機拍下指紋圖象後，系統將指紋轉化成為點圖，儲存供日後查詢比對。指紋辨識必須作身體上的接觸，使用者容易產生罪犯嫌疑的刻板印象，有隱私權被侵犯的感覺，而因犯罪技術科技化，指紋膜仍有被複製的風險，且事後反向追查困難，此外指紋判讀需依賴專業機器與人士，因此多用在門禁及犯罪管理等特殊用途。

## 2. 臉部辨識

臉部辨識由於面積較大，加上特徵點也更多樣、複雜，因此技術難度很高，一直停留在實驗室研究的階段，直到最近才有明顯地突破，各種商品化的應用一一出現。

在生物辨識市場中，臉部辨識名列第二位，其獨特性為何？當一個人只露出鼻子和嘴巴時，能不能一眼認出他是誰，似乎不是很肯定。但是，只是露出眼睛，遮住下半張臉孔，卻能很快知道這個人是誰，原因就在於眼睛四周輪廓透露出的訊息。因此，臉部辨識系統設計常以眼睛為主軸，找出眼睛和五官的相對應位置。例如輪廓的凹凸、五官距離的長短等，都是臉部的特徵點，並將這些臉部特徵與存放於特徵資料庫的人臉進行比對，即時確認身分。此外由於是三維物體辨識技術，這也阻止駭客利用照片非法侵入系統，因為照片是平面的，而人臉是立體的。

因為視訊裝置可以在固定距離內，掃描來往的行人，但被掃描者卻不自知，具有最少侵犯性的特點，因此，當警方查緝要犯時，可以在資料庫中輸入要犯的臉部影像，然後在機場、政府大樓或主要幹道掃描可疑人物，以協助辦案或維護安全。臉部辨識系統，在911事件後已廣為人知，這套系統可以在群眾間隨意掃描，並找出符合資料庫中臉部特徵的人，是很好的監視科技。

## 3. 虹膜辨識

放眼世界各地，生物辨識系統早已建置在各個重要出入關卡。像是英國倫敦的希思羅機場就設置虹膜辨識系統，受測者只要在定點距離接受眼睛掃描，就能出入境。有人認為，虹膜辨識的錯誤率是各種生物辨識技術中最低的，道理何在？

事實上，每個人的虹膜結構皆不相同，對同一個人而言，左右兩眼的虹膜區別也十分明顯。此外，科學家指出，人類的視網膜會因為年齡增長而改變，即便虹膜的基本結構是由內在的遺傳基因所決定，但終其一生卻不易發生變化。虹膜組織包含的資訊，比人體任何部位還要多。虹膜共有240個獨特處，相較於臉部則約有80個獨特處、指紋的獨特處只有20至40個。因此，要找出虹膜編碼相同的機率為10的78次方之一，全世界幾乎找不到第二個虹膜相同的人，就連雙胞胎也是。就算現場光線不足或太強、受測者配戴太陽眼鏡、隱形眼鏡，都無所遁形。

使用專用攝影設備來截取虹膜的影像、眼睛的顏色，辨識率很高，但是操作較複雜，價格是所有辨識科技中最昂貴的，使用時較不自然也不舒服，而紅外線直接照射視網膜則有傷害眼睛的疑慮。

#### 4. 聲紋辨識

聲紋辨識可以利用麥克風或電話設備，每一個人的講話速度、聲調及嗓音等獨特特徵來辨識，但容易受使用器材品質、背景聲音或感冒聲音沙啞混淆，準確度不夠高。聲紋辨識同樣也是一種非接觸的識別技術，但是因為聲音變化的範圍太大，加上聲音會隨著音量、速度和音質的變化而影響到收集與比對的結果，因此目前的技術還無法精確分辨錄音的欺騙情形。

#### 5. 簽名辨識

簽名識別技術是目前最常為社會大眾使用的辨識技術。主要的辨識方式是將簽名的力度與特徵轉換為辨識的密碼。並非透過簽名的圖像本身，而是分析筆在每個字與字之間移動的速度、順序、壓力、方向以及筆觸的長度來區分出不同的身份人的簽名。它和聲紋識別一樣，是一種行為測定學。由於人隨著經驗的增長，性情的變化與生活方式的改變，簽名也會隨著而改變。因此在專一性的特徵判別上較容易出現誤判的情形。

#### 6. DNA辨識

DNA比對技術相當複雜，是所有生物辨識方法中非必要不輕易使用的一種，以目前技術來說，需費時甚久才能分析出DNA結構，多用於血緣關係認定及警方辦案上。

#### 7. 靜脈辨識

靜脈辨識是利用紅外線攝影機掃描手背上的靜脈血管溫度，並儲存每個使用者的靜脈特徵，用來做為日後比對的樣本。使用靜脈識別有幾個好處，即使是雙胞胎的靜脈也都不同，而且靜脈特徵幾乎永久不變，除非血管病變或嚴重傷害，跟其他的生物特徵相比，目前的技術很難加以仿造，能讓實體安全等級更進一步。

#### 四、生物辨識系統未來發展趨勢

想想看，未來進出門只要在門禁上壓一下指紋就可以通關；到了辦公室，站在攝影機前進行虹膜辨識比對身分出入；再坐在辦公桌前的電腦，進行臉部辨識，開啟專屬檔案，過程不消幾秒鐘，就可以認證成功，這中間再也不用擔心卡片被偷、或是忘記密碼，只要帶著「本尊」，就可以暢行無阻。這樣的科技不是科幻電影情節，而是漸漸地溶入我們日常生活中。待這一天到來，每個人的身分密碼就是「自己」。有了自己獨一無二的生物辨識識別密碼，過去提款時帳號害怕被盜用、上網購物擔心遭駭客攔截資料、憂慮信用卡被盜刷、手機被盜打，如今拜生物辨識之賜鑑定身分，都可以有效防止偽造的發生。未來生物辨識系統的發展趨勢如下：

(一) 全球的指紋認證應用已如火如荼的展開，亞洲的香港、澳門、新加坡，歐洲的比利時與中東的葉門已決定發行含指紋辨識的身分證。美國多年前即已著手研發生物辨識科技，前年遭遇九一一恐怖攻擊後，更積極推動。九一一事件的十九名劫機歹徒全為外國人，有十五人持學生或觀光簽證入境美國，其中兩人的簽證甚至過期。美國為防911事件再度重演，積極推動國防部軍卡，布希總統並於2002年5月14日簽署H.R. 3525法規，要求美國大使館簽發簽證全部加生物特徵(指紋、臉形)，並且預計2004年元月起將全面採用生物辨識簽證過境系統，對入境者採取收納指紋、瞳孔辨識等措施。歐盟法、德、英、義及西班牙等5個大國內政部長日前也達成協議，準備在發給外國人的簽證中附加簽證持有人的生物資料。

我國入出境管理局近日表示，對於各國通關採行「生物辨識」系統的趨勢，基於各國情報交流的實際運作狀況，我國均已掌握，由於我國海關處理入

出境證照查驗工作，長期人力不足，入出境管理局已著手研擬採行生物辨識系統通關的可行性。境管局認為，我國的證照查驗加入生物辨識系統，實務可行、技術上也不是問題，不過，因為涉及入出境許可簽證政策的變革，恐須各相關部會進一步開會研商。

至於境管局研究方向有二：一為國人入出境的通關、一為外國人入出境的管理；收納的「生物資料」包括指紋、瞳孔、掌紋、血型等。如針對本國人，則未來國人除了申辦護照之外，還必須同時申辦入出境通關所需的IC晶片卡，通關時即可取代護照，只要持卡通過電子閘門，不需再三核對身分。如為針對外國人，則外交部及入出境駐外管處，在受理申辦簽證時，蒐集相關生物資料即列為簽證業務之一。由於配套作業繁複，且涉及政策層次，入出境管理局說，將在未來成立移民署之後，再就入出境簽證政策是否增加「生物辨識」功能提出成熟的政策。

(二) 指紋結合簽名辨識，可應用在提款機、金庫、算命網站或是醫療電子公文系統，只要將指紋資料儲存於金融卡的IC晶片中，提款時將手指按在辨識機上，再在手寫板上簽名，系統就會立即辨認其真偽。

除了身份認證之外，有業者還發明了「離線語音辨識解決方案」，只要使用數位錄音設備，如PDA或是錄音筆，錄下發言，之後再傳輸到電腦上，就能立即辨識成文字；這套產品採用的是IBM的語音辨識核心技術，辨識率達90%。

Microsoft在發表新一代作業系統Windows XP後，即表示：「新一代作業系統將支援語音辨識技術」。為此，微軟在語音辨識技術發展上，特別在中國大陸成立一支團隊，為微軟未來推出的產品作準備。微軟此舉不外乎在為未來的IA產業提前『鋪路』，可預期未來IA相關產品，語音辨識將是很重要的關鍵運用技術之一。

不希望電腦被盜用的人，則可試試加了指尖辨識板的滑鼠和鍵盤，目前這種滑鼠和鍵盤，售價分別在2千8百和5千7百元台幣左右，另外比較便宜的新產品，像是附有指紋比對掃描器的滑鼠墊和電腦卡。

(三) 華南金控用指紋辨識系統管制董事會門禁；君悅飯店（原名凱悅飯店）將指紋系統用在員工考勤。另有公司使用臉部掃描考勤管理系統。考勤系統與含有攝影機及臉部辨識引擎的感應讀卡機結合，員工的刷卡記錄均含有刷卡時被拍攝的照片，容易追蹤並可有效防止員工之間代打卡的情形，出勤記錄

轉存檔功能更可作為員工計算薪資的依據。另外，無數要求更高安全層次的實驗室、機房、資料儲存中心、研發中心或私人俱樂部均急需這項產品來保障安全。臉部辨識技術在門禁與考勤應用的市場潛力，將蓄勢待發。

新光醫院是國內第一家採用臉部辨識技術，進行安全管制系統的醫院，這套系統安裝在員工宿舍。過去醫院曾經嘗試採用指紋辨識和語音辨識的解決方案，但由於指紋辨識必需脫掉手套，醫院工作人員出入使用上不便而做罷，至於語音辨識則會因為醫護人員戴口罩而影響精確度。辨臉技術可以結合其他的門禁管理設備，如刷卡系統，將刷卡者與持卡人的臉部檔案系統資料加以比對記錄，以確認刷卡人是持卡人身分，防止盜刷卡片或企圖闖入，提升醫院的安全控管機制。

長庚醫院已開始將生物辨識系統實際應用於病患同意書，透過醫師隨身攜帶的手持式裝置，如Tablet PC，病患可在數位文件上簽名及按上指紋，做為同意醫師進行醫療動作的證據，以避免可能的醫療糾紛。

## 五、結語

隨著生物辨識技術的不斷改良，結合多種生物特徵識別，以提高系統的精確度的新型辨識系統將漸漸取代傳統的身份辨認方式。生物辨識資料的優點是強調其個人獨特性、不易被仿冒及盜用的特徵，然而由於個人生物辨識資料如虹膜、指紋等乃終身不變，其優點亦可能成為其缺點，原因是當受試者接受生物辨識裝置感測後，測試端裝置需先進行影像分析，然後將影像資料轉換為數位資料，再將該數位資料傳輸回遠端的伺服器系統中，轉換為生物辨識模板並與原先儲存的模板進行比對，才可鑑別使用者的身分，因此，在此數位資料傳輸過程中，一樣有資料傳輸安全的疑慮，尚未經過處理的生物辨識資料一旦被不肖人士侵入、盜用、竄改、截取，將造成無法彌補的損害。此外，伺服器系統每天接受、處理大量的生物辨識資料，轉換為生物辨識模板，這些資料如何轉換、儲存、管理、傳遞是一個很重要的關鍵，如何在大量的資料中快速、準確的比對將實際影響系統的效能。另外，在個人意識高漲的今日，相關廠商如何說服民眾接受此項技術作為身份確認的方法仍有待解決。因此除了克服辨認技術上的困難點之外，如何在政府的協助監督之下建立公正、安全的個人資料庫系統或許才是業者未來行銷上一道待跨越的鴻溝。