從身體裡頭找密碼
生物辨識技術點將錄

談再多防駭防毒，說再多資訊安全控管，如果不做好第一關身分驗證，都是枉然。如何有效的驗證員工身分？如何有效地做好人員控管？本專題將介紹目前最先進的生物辨識技術，協助企業或機關組織用最有效率的方式，作好第一關安全防護。

文／圖　曹乙帆

不論是居家或公司大樓門禁、入出境管理、電腦登錄、銀行取款，抑或犯罪偵防等，都必須進行身分認證，以保障個人權益、資訊安全、打擊犯罪，甚至國家安全。當前因應各種需求及應用領域的身分認證方法及技術甚多，其中尤以能代表個人獨一無二身體密碼的生物辨識，最具方便性與安全性。但各種生物辨識技術，除了設備本身的成本會有不同外，同時在生物特徵樣本採集上的方便性、取樣品質、取樣環境等因素各有不同影響，進而在辨識準確度上會有不同差異存在。生物辨識是個難以避免的趨勢，但企業必須先了解不同技術間的差異，以選擇最符合自身需求及狀況的生物辨識解決方案。

將生理特徵轉換成安全密碼

在現實生活上，會碰到很多要確認身分的情形，例如警察臨檢，受檢人必須拿出駕照及行照來證明自己與車子的確實合法身分。到銀行開戶或申請貸款，身分證會是其中必要的辦理證件之一，之後若要領錢，可以存款簿配合簽章，抑或提款卡配合密碼的方式領取。不過，就身分證、駕照等證件來說，仍然不時聽聞到許多假冒及偽造的案件，尤其是行照，就像公司或居家大樓門禁卡一般，任何人撿到或竊取都可以使用，實在毫無保障及安全性可言。至於簽名或蓋章，也同樣會有遭到假冒及偽造的可能性。

當前電腦使用者最常用到的密碼，被側錄或破解的案例更是不勝枚舉。雖然密碼愈長愈好，不同應用採用不同密碼的安全概念眾所周知，但可行性實在有待商榷。大部分的使用者仍然使用簡單易記的密碼，再不然就是一組密碼行遍天下，所以被暴力破解的機率自然大增。

身分認證的最終目的即在於確認「你是誰」，但為了方便起見，遂有其他替代性的方案，如「你有什麼」、「你知道什麼」來確認身分。所謂「你有什麼」就是前述的身分證、門禁卡等所有物；「你知道什麼」亦指密碼等個人記憶的事物或數字。

事實證明，即使再複雜的密碼，駭客也可透過數以十萬計殭屍電腦所集結而成的平行運算架構，在短短數秒之內便可能加以破解。或許更換成動態密碼，相對來說會比較安全，但是支援動態密碼的Standalone Token，使用上並沒有那麼方便直覺，如果忘記帶在身上或遺失了，都會造成極大的困擾。除此之外，目前已有支援在手機上產生動態密碼的方案，或許使用者攜帶的意願及機率較高，但仍有遺失或沒帶在身上的可能性，而且更換手機時會有點麻煩。

相對而言，生物辨識不論在安全性、唯一性、可靠性及方便性上，都遠比上述種種既有的身分認證機制來得更好。就以大家最熟悉的指紋辨識來說，每個人的指紋皆獨一無二、無可取代，而且它是身體的一部分，根本不會有忘記攜帶或遺失的疑慮發生，只要伸個手指即可完成身分的識別。除了指紋之外，人體身上具備同樣獨一無二的生理特徵，並可用來當做身分辨識的地方還真不少，包括人臉、虹膜、視網膜、靜脈紋、掌形、指形、語音與DNA等。除了生理特徵外，每個人也都有專屬的行為特徵，例如簽名、步伐皆因人而異，這些也可用在生物辨識的應用上。

生物辨識技術基本流程

存在每個人生理或行為上的特徵絕對毫

無問題，所以理論上各種生物辨識的確擁有無與倫比的可靠性、安全性及方便性，但最大的問題就在於這些特徵被擷取成為檔案、樣本的過程中，存在太多影響精確度的變數。在了解這個問題之前，必須先對整個生物辨識系統的比對流程做一番簡單的介紹。（圖1）

不論何種生物辨識，一開始都必須為每一位使用者建立生物特徵範本樣本。其建立方法，不外首先透過專門的掃描器、相機或攝影機等裝置，來擷取指紋、臉形、靜脈紋、虹膜、掌形及筆跡等特定部位或目標的影像。接下來再經過生物辨識演算法（Biometric Algorithm），從影像中萃取出生物特徵數位檔，此亦即可做為日後比對基礎的範本樣本檔。當所有人員的樣本檔皆建立後，並且與各自註冊登錄的個人帳戶密碼等資訊綁定之後，後端範本樣本資料庫即大功告成。

之後人員進出或登錄時，前端感測裝置當場進行同樣的生物特徵影像的擷取動作，該系統會隨即呼叫生物辨識演算法進行特徵擷取作業，接下來再將該特徵檔，與資料庫中的範本樣本檔進行比對。只要相似值到達一定標準時，即通過驗證，反之則登錄失敗，並對相關人員發出警示訊息。

外在影響因素的限制

由上述流程中可以發現，範本樣本檔的建立並非主要問題所在，反而是日後每次進出或登錄之際，同一名合法使用者當場擷取的特

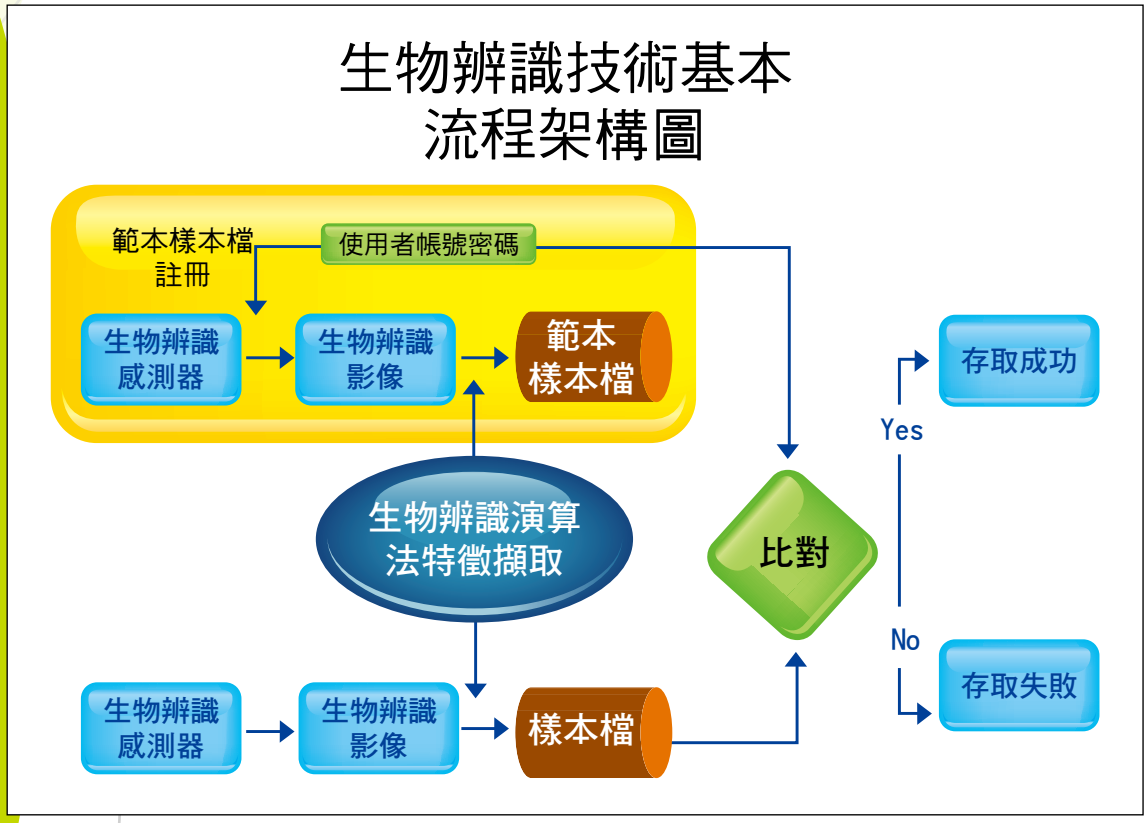

圖1　生物辨識技術基本流程架構圖。

徵樣本是否能夠一致才是關鍵。畢竟，當下環境若不同，例如光線、溫度、濕度、灰塵等變異因素；受測者的行為或姿勢差異，例如人臉或手的擺放角度不同；受測標的發生問題，例如手指損傷、破皮、髒汙、流汗，戴有色或瞳孔放大之隱形眼鏡，感冒破嗓，抑或特定部位病變或老化等因素，這些都可能讓原本合法使用者因誤判而遭到拒絕登錄的可能性。

同時，樣本取樣的難度或條件限制，也會影響每次樣本擷取的一致性，以及該系統的精準度及可行性，當然也會影響建置成本之高低。對此不同生物辨識都各有優缺點，例如虹膜辨識，其相對於指紋或靜脈紋來說，不論在感測裝置的規模、建置成本上皆有過之而無不及，而且不少使用者會有難以消減的心理障礙因素。

此外，人臉辨識對於光線及角度的差異極其敏感，指紋辨識則非常容易受到手指狀況的影響。除此之外，扮演生物辨識系統靈魂角色的運算法，其擷取比對技術之優劣，以及感測裝置本身的性能、品質、耐用度、壽命等，都是左右該機制精確度的考量重點之一。總之，企業在導入生物辨識系統之前，必須綜合自己的需求及環境狀況，來了解各生物辨識的優點及侷限性差異。同時在導入時，也必須儘量將各種負面因素降至最低程度。

降低FAR與FRR交叉誤差率為一致目標

對於生物辨識系統的精確度來說，另有兩個值得一提的參數，一為接受誤差率（FAR；False Acceptance Rate），是指非法使用者異常通過身分辨識的比率；一為拒絕誤差率（FRR；False Rejected Rate），意指合法使用者無法正常通過身分辨識的比率。前者太高會影響安全，後者太高會影響使用者對系統的信任度及使用意願，所以一般會取兩者交集的最小值，亦即交叉誤差率（CER；Crossover Error Rate）做為平衡點。若以指紋辨識來說，關係安全的FAR大約小於0.001%，FRR小於3%。不過實際數值仍要依使用單位的實際需求為準來做調整，通常對安全要求極高的單位，FAR會要求更低的比率。

除此之外，取樣方式也會隨著辨識目標的動靜與否而有所不同。一般門禁乃屬於靜態辨識，採用的方式為被動取樣機制（因為使用者要來到感測裝置前，主動進行操作時才能加以辨識），由於可依需求對既有環境進行適當的調整，並要求使用者依照標準程序及規範進行辨識，所以準確度相對較好。至於針對像是海關入出境、機房等特定區域監控之動態目標辨識，會採用主動取樣方式（所有進入感測範圍者都會自動加以辨識），由於這些環境充滿許多未知因素，而且被辨識目標通常毫無知覺，當然也不能用標準程序加以規範，所以精準度相對較差，比較適用於犯罪偵防及反恐等應用上。

在樣本比對上，過去想對任何人進行身分比對時，必須進入資料庫中對所有樣本一一比對，直到發現相吻合的為止，此即一對多比對機制。如今，為了進一步提升辨識的準確度，並加入了一對一比對。也就是使用者可搭配識別卡感應或專屬密碼的輸入，先「說明」自己的身分，然後再「輸入」自己的生物特徵。此時系統只要調出該身分的生物特徵樣本檔進行比對即可，當前不論是電腦系統採用的生物辨識登錄機制，抑或各國開始採用的電子護照，大致皆屬於一對一比對機制。由於比對範圍縮小成一對一，所以精確度及速度會相對提高許

多。不僅如此，企業可以預先將範本樣本檔載入到前端裝置中，所有比對可以直接在前端完成作業，如此可以減少往後端撈資料的可能安全風險。不過，一對一模式只適合人數較少的公司或部門，畢竟前端裝置可提供的儲存空間有限，自然不能儲存為數龐大的樣本檔。

各類生物辨識全面大直擊

▶指紋辨識（Fingerprint Recognition）

當前生物辨識之中，指紋辨識可說是發展最早也最成熟的技術。若將犯罪偵防領域的自動指紋辨識系統（AFIS；Automated Fingerprint Identification System）市場一併計算的話，當前全球生物辨識市場中有超過6成皆由指紋辨識一口吃下，由此可見其普及的程度。這點可從目前主流的商用筆電，莫不將指紋辨識列為基本配備的普遍趨勢上得知，同時該技術也是第一個全面性成功進駐到電腦系統登錄機制的生物辨識技術。在應用上，指紋辨識應用領域之廣，亦非其他生物辨識技術所能望其項背，舉凡電腦系統登錄、資料加密、手機登錄、門禁差勤管理、金融交易、犯罪偵防、反恐措施與電子護照等領域都可見到該技術的身影。

雖然指紋辨識技術非常成熟，其精準度也達到一定水準，但為了更進一步提升其辨識率，目前該系統提供了一次註冊最多十根手指指紋的機制。除此之外，資料安全上，也有不少廠商將指紋辨識與主機板上的TPM安全晶片相結合，以提供更安全的權限控管及資料加密機制。至於鳳凰科技（Phoenix）更發表BIOS層級的指紋辨識機制，讓該安全機制由Post-OS，延伸至更安全的Pre-OS領域。

過去指紋辨識最令人詬病的地方，莫過於無法支援活體辨識，所以好萊塢電影中會有一些將手指切除以通過指紋辨識的殘忍畫面。而且電影中也不乏許多採用薄膜或黏土採擷指紋機上遺留指紋，進而成功突破門禁的劇情。面對如此不堪一擊的種種疑慮，美國紐約克拉克森（Clarkson）大學將手指汗水列為指紋比對重要參數的研究中，讓指紋偽造問題獲得了一定程度的改善。也因為死人手指不存在汗水，所以也讓支援汗水特徵辨識之指紋辨識技術，能在靜脈紋辨識問世之後，同登活體辨識之林。

不過，令人質疑的是，同一個人的手指汗水狀況，也可能因為季節更迭或身體狀況之不同而有所改變，雖然將汗水特徵加入，有助於FAR之降低，但恐怕也會提升FRR的比率。或許這點會是該學術單位今後需要致力改善的重點。

除此之外，尚有手指一旦因流汗或流血而潮濕、因灰塵而髒污、破損，抑或指紋紋路、隆線不明顯而造成辨識誤差率提高的情況。對此，NEC透過自家開發的高精密度指紋辨識演算法，以及分散式穿透光指紋辨識裝置的兩相搭配，而解決了上述長久以來的困擾。兩技術是隨著該公司於日前推出的全新PU900-10指紋辨識裝置的上市而一起對外發表。

台灣NEC SL推進企劃本部副理林漢坤表示，PU900-10採用分散式穿透光掃描機制，藉由玻璃纖維光束製程打造出具備極佳透光性的特殊玻璃鏡面，能讓手指隆線更亮，凹下部分較暗，形成層次更分明的影像，進而能取得遠比傳統裝置更清晰的指紋影像，即使面對乾燥或潮濕指紋，甚至女性或孩童的細紋隆線，皆能清楚分明地加以辨識。（圖2）

不僅如此，針對掃描取得的圖像，該

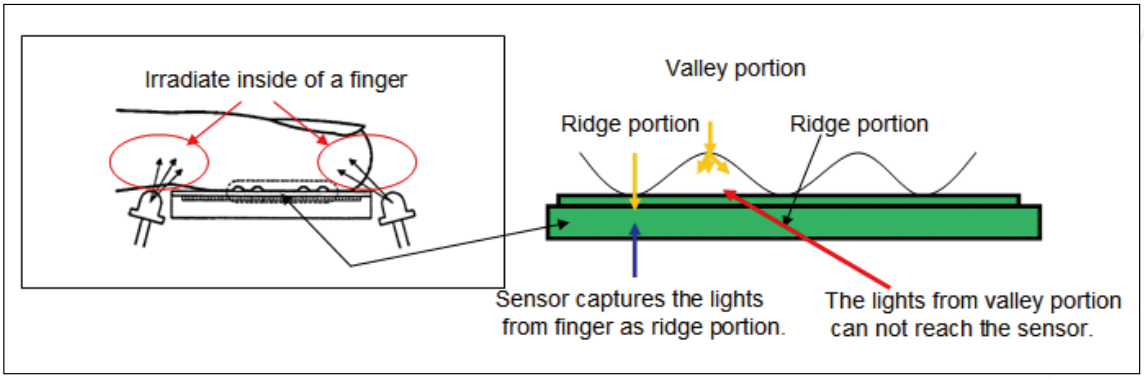

圖2　NEC分散式穿透光指紋辨識掃描機制示意圖。（資料來源：NEC）

圖3　NEC PU900-10指紋辨識裝置。

產品還會藉由自動增益控制（Automatic Gain Control）影像處理技術中的去背、紋樣抽出處理等影像補強機制，由此讓影像更加清晰、整體精準度更高。該產品會對最終擷取出的指紋圖像進行數位化及加密作業，如此可確保即使該指紋特徵檔外流，也無法還原成原先的指紋圖檔，進而保障個人隱私安全。

PU900-10為一款採用USB介面的外接式指紋辨識裝置，除了可供電腦系統登錄權限之控管外，該裝置亦可與RADIUS認證機制搭配，以做為醫院醫療資訊系統（HIS）的權限控管機制。林漢坤表示，未來不排除會將該產品模組化，除了可應用在門禁差勤管理上之外，同時也可內建至筆電或鍵盤之中。（圖3、圖4）

▶人臉（Face Recognition）

人臉辨識可說是繼指紋辨識之後，第二

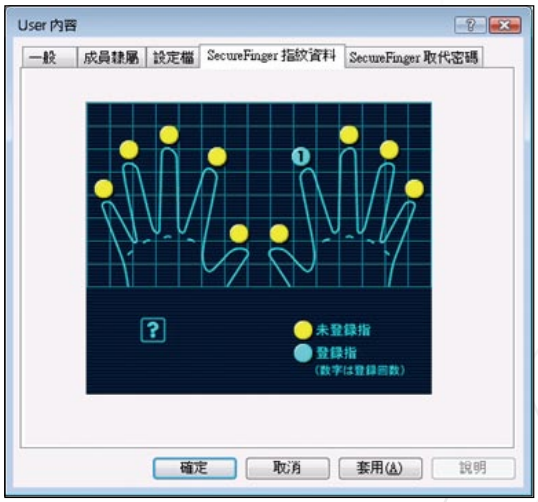

圖4　指紋資料登入設定。

個成功進入到筆電系統，並成為其存取控機制之一的生物辨識技術，再加上該技術早已是國際民航組織（ICAO）唯一指定認可的電子護照生物特徵技術。也因為如此，該技術在當前全球生物辨識市場之占有率，僅次於指紋辨識。相對於指紋、掌靜脈、掌形等接觸性生物辨識技術來說，該技術最大的特點即在於完全不用觸碰到感測器，對於當前肆虐的H1N1疫疾最具安全性。而且使用者也不需抬起手，只要露個臉即可完成身分辨識，相當方便。

目前人臉辨識已成為筆電上的「唯二」生物辨識，透過筆電上的Webcam進行使用者臉部影像擷取，即可做為系統登錄或螢

幕保護程式的輸入密碼。不僅如此，日本NTT DoCoMo也曾將該技術置入到手機中。不過當前筆電的人臉辨識稍嫌陽春兩光，對於環境及臉部變化敏感度過高，再加上參差不齊的Webcam畫素表現，辨識不佳的狀況比比皆是。對此，煇煌科技推出臉鎖反應（FaceAether）人臉辨識Windows登入軟體，宣稱在辨識速度及精確度上提供明顯的改善。

除了系統登錄外，該技術並常見於國境通關、犯罪偵防、遠端安全監控及門禁差勤管理等領域。其中，前三者採用的是動態式主動取樣機制，所以該系統必須具備因應明顯光線變化、行走速度、臉部角度等變因，快速鎖定並擷取出正確的人臉影像。至於門禁系統，則屬於靜態式被動取樣機制，企業可藉由環境控制及使用規範來提高辨識正確率。此外，人臉辨識技術還可進一步衍生出其他不同應用，例如專門針對特定人物照片的搜尋引擎，以及支援人臉自動對焦的數位相機。

會造成人臉辨識失敗的因素頗多，例如單一照明設備故障所造成的光線差異，笑臉等導致扭曲的表情，甚至濃妝、髮型、頭巾、眼鏡等裝飾都可能因為辨識失敗而不得其門而入。但相對地，對於假冒特定人物的面具、照片，甚至雕像，人臉辨識也有被欺騙的可能性。針對照片，倚辰科技自家的活體辨識技術，會結合照片背景之記憶與偵測，來判斷出照片並非活生生的真人。

除了新興的煇煌科技外，當前人臉辨識系統的主要供應商及產品包括，蒙恬科技的FaceMetrix Access Control System及FaceMetrix Logon、威波科技的FaceVACS，倚辰科技（Face-Tek）的NotiFace II，達寶科技（DoubleTech）的Face Hunter、FaceGuard。

▶虹膜（Iris Recognition）

講到虹膜辨識技術，大多數人都會與「尖端高科技」一詞或景像聯想在一起。也因為如此，虹膜辨識也經常成為好萊塢電影中的常客。該技術在準確程度上僅次於視網膜，但視網膜的技術難度不利於商品化，因而使得虹膜辨識成為現有市面上最精準的生物辨識技術，依據Panasonic的「含蓄」說法，其誤判率僅達120萬分之一，試想有哪家企業或單位會有120萬員工，這似乎跟毫無誤判率沒什麼兩樣。

對於人眼來說，大致上是由外圍眼白的鞏膜、正中央的瞳孔，以及兩者之間的虹膜所構成。虹膜內含複雜的紋理結構，其形成是由遺傳基因（DNA）所決定，也因為如此，虹膜具備高度的唯一性及不可更改性，進而成為當前最具權威性的生物辨識技術。

不過虹膜辨識仍存在許多缺點，首先使用者必須接受該裝置對眼睛直接照射的紅外線掃描，使用者難免會興起心理層面的恐懼感或不舒服感。如果機器攝影機無法馬上對到焦，會讓不舒服的心理感受時間更拉長。再者一些人的虹膜仍會因年歲的變化而稍微改變，通常每十年可能會有形體上的些許變化。

此外，身體或心理上的重大創傷，也可能導致虹膜形體的改變，不過這些機率都非常低。另一個最引人詬病的缺點，莫過於該技術整體軟硬設備之造價實在比其他生物辨識高得多，所以應用領域也因而大受限制。原則上，該技術比較鎖定在頂尖的門禁管制市場，例如高機密軍情單位、高科技業或豪宅。

對於虹膜辨識廠商，一般較耳熟能詳的莫過於Panasonic及LG。事實兩家有不少技術及零組件，來自於策略合作的美國Irdian，該公司是當前全球最大的虹膜識別技術與相關產品

供應商。Panasonic所推出的BM-ET200裝置特別強化其對焦系統及辨識速度，（圖5）除了透過語音及指示燈導引使用者取得最佳拍攝距離外，雙鏡頭的設計，也讓眼睛更好對焦，一旦對焦完畢，該裝置能在0.3秒內完成虹膜辨識作業。LG自家的IrisAccess 4000，可雙眼同時認證，並內建人臉辨識功能，提供多重生物辨識機制，整個辨識過程約1秒完成。此外日本沖電氣（OKI）開發出透過手機相機鏡頭即可進行虹膜辨識的技術，搭配手機電子錢包，可提供更安全方便的認證機制。

▶靜脈紋（Vein Recognition）

開啟活體生物辨識新紀元的靜脈紋辨識，目前市面上依不同部位靜脈紋而主要分成三種：手掌靜脈紋、手背靜脈紋及手指靜脈紋，其代表廠商分別為富士通、韓國TechSphere與日立亞細亞（Hitachi）（圖6）。除此之外，尚有較少見的手臂及手腕靜脈紋技術，而Sony也推出專門針對筆電及手機登入的指靜脈認證技術Mofiria。

靜脈紋辨識技術是透過近紅外線（波長700nm至1000nm）對手掌、手背或手指靜脈部位的反射（富士通）或穿透（Hitachi）光線，來形成靜脈影像。由於靜脈紅血球中的血紅素（Hemoglobin）具備吸引近紅外線的特性，因而使得整個靜脈紋的影像得以清楚顯現。（圖7）

每個人的靜脈紋的重複率只有千萬分之八，所以跟獨一無二沒什麼差別，靜脈紋辨識的優點尚包括活體辨識、永久性及無法複製等特性。相對於其他生物辨識技術，像是指紋、人臉都有偽冒的可能性，甚至虹膜也可能造假，像電影天使與魔鬼一片中，某科學家整個眼珠就被挖出來通過虹膜門禁系統。但靜脈紋則不然，即使手被砍下，靜脈紋也無法造假，因為砍下的手掌或手指已非活體。同時掌靜脈紋還具備非接觸式的優點，至於

圖5　Panasonic BM-ET200虹膜辨識裝置。

圖6　Hitachi PC系統登錄用PCT-KC8203指靜脈辨識裝置。

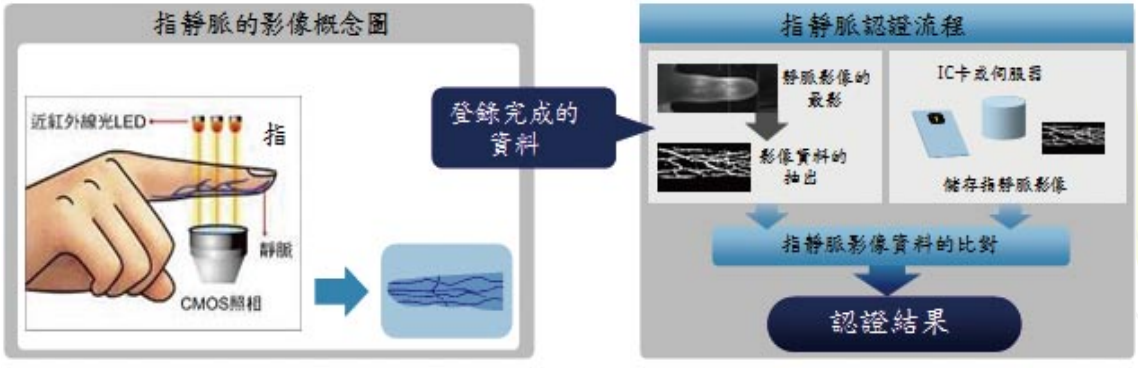

圖7　指靜脈示意圖及認證流程。

圖8　TechSphere VP-II手背靜脈紋。

Hitachi指靜脈紋仍需要接觸感測器，不過只要擺放即可，而不需要像指紋辨識要做按壓的動作。至於TechSphere手背靜脈紋，掃描時還是需要用兩根手指勾往儀器才能辨識，所以仍有碰觸動作。（圖8、圖9）

再者，當前靜脈紋辨識皆擁有極佳的辨識率，例如TechSphere的VP-II之辨識率即達到99.98%。不過在誤判率上各家不一，在接受誤差率上，TechSphere與Hitachi皆為0.0001%左右，而富士通則更低於0.00008%。至於拒絕誤差率富士通與Hitachi皆為0.01%，但TechSphere卻高達0.1%，對於國外人士來說，手背上會有較多的汗毛，或許因此影響其辨識率。此外，在辨識速度上，TechSphere要花上3秒之久，但其他兩家不到0.5秒就能搞定。

Hitachi系統整合事業部Ubiquitous Solution部門兼指靜脈推進中心技術主任吳志宏不諱言地表示，當前靜脈紋辨識仍具備一些缺點，例如掌靜脈會有高度距離調整上的需要，指靜脈會因手指擺放角度之不同而有差異的可能。同時位於末端的手指，也比較會受到低溫的影響，使得血流速度變慢、紅血球數量下降，在紅外線透光量增加的情況下，取得的靜脈紋影像會比較不清楚。再者，一些較嚴重的血管病變也可能影響其辨

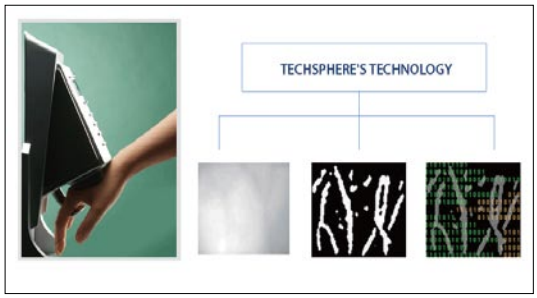

圖9　TechSphere VP-II手背靜脈紋使用情境。

識率，而受傷引起的內出血多少也會影響，不過使用者只要換根沒受傷的手指即可。同時外部強光也可能會影響影像擷取及辨識度，不過，各家產品都有對光線進行各種增益調整機制，來降低這方面的干擾程度。

相對於指紋之於犯罪偵防、人臉之於大流量通關管控，靜脈紋辨識則是以個人身分識別為主，其應用領域偏及銀行ATM、醫院電子病歷存取控制、門禁差勤系統、圖書館借閱、電腦登入、學校成績查詢等。Hitachi系統事業部企業系統部門兼系統整合部經理李昆龍指出，其中尤以銀行ATM為應用上的大宗，在日本有超過八成ATM採用靜脈紋。Hitachi並與JCB合作將指靜脈技術導入到信用卡上，以取代不安全的簽名。同時，該技術並應用在汽車開門及啟動上。在國內，該公司並與遠雄合作，提供更安全方便的指靜脈門禁系統。

▶掌形、聲紋、步伐等其他生物辨識技術

掌形辨識則是另一個相對成熟且方便的生物辨識技術，顧名思義，該技術是透過對手掌幾何形狀與手指長寬度之特徵擷取，來做為身分辨識的一門技術。該技術精準度更達96.5%，誤判率則約在2%上下。會了方便取影的一致性，掌形辨識機上有許多讓手指擺放位置固定的小圓柱，但這也形成了該技術的最大缺點，因為並非所有手掌大小都可適用。而且

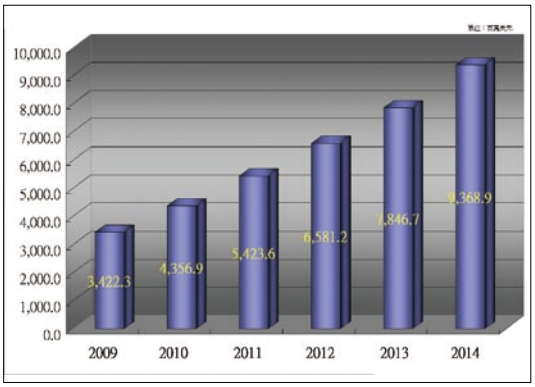

圖10　2009-2014年生物辨識年營收走勢圖。（資料來源：International Biometric Group）

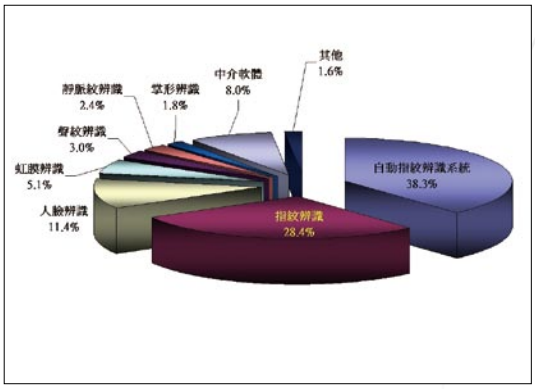

圖11　2009年全球生物辨識各技術市場占有率。（資料來源：International Biometric Group）

在所有接觸式生物辨識中，其接觸面積最大。由掌形辨識也另外衍出其他技術，像是掌紋辨識、指形辨識等，前者是以手掌獨特紋路來做為辨識基礎；後者則是整個掌形的縮小版，而取局部手指的幾何圖形。

此外，還有聲紋辨識，也就是透過錄音來擷取出個人獨有的聲音特徵來識別身分的技術。該技術可應用於門禁、電話客服、犯罪偵防、國防情治等方面。在電腦上人們較熟悉的應用就是語音辨識，使用者只要講個話也可打字。聲紋辨識比較會受到環境噪音的干擾，以及使用者因感冒的因素的聲音變異影響。

有趣的是，之前芬蘭VTT技術研發中心曾推出專門針對手機、PDA及筆電等行動裝置之生物辨識防竊機制。該機制是以每個人獨特的步伐行為特徵做為身分辨識的基礎。內建該技術的行動裝置會偵測使用者步伐特徵並儲存成為樣本檔，若裝置遭竊，會主動對偷竊者的步伐進行比對，一旦不吻合，會自動將裝置關閉而完全無法使用。

方便、安全、物廉價美才是主流技術

當前生物辨識的類型五花八門，除了個人相關識別之應用外，其觸角伸及政府、軍事、法律、金融服務業、醫療業、高科技業、電信業、製造業、遊戲業、零售業，以及旅遊交通業等各個領域之中。應用上更遍及門禁差勤、系統登錄、身分證、電子護照、金融交易、犯罪偵防、裝置及系統存取、遠端安全監控等市場區塊。

也因為如此，國際生物諮詢暨技術服務組織（IBG；International Biometric Group）即預測2009年全年生物辨識產業總產值可破34億美元大關，隔年可望達到43億多美元，到了2014年更進突破達到接近百億（93億美元）之境地，由此可見該產業之前景無限。在全球生物辨識產業中，市場占比最高並達到38.3%的是鎖定犯罪偵防的自動指紋辨識系統（AFIS），而其他類型所應用的指紋辨識居次達28.4%，兩者合力即吃掉了近7成的市場份額。此外，分居三、四的是人臉辨識及虹膜辨識，至於靜脈紋的市場占比仍不到3%。（圖10、圖11）

站在精準度的考量點來看，不論何種生物辨識技術都有其先天與後天上的侷限性（圖12）。所以提昇精準度的最佳做法，莫過於多重生物辨識技術，也就是導入同時整合像是

圖12　各種生物認證系統的比較。（資料來源：Hitachi）

人像、虹膜或靜脈紋等多種技術的身分辨識機制，如此一來，勢必能將CER交叉誤差率降至最低程度。但同集結多種技術，也意味著必須同時建置多種前端感測裝置，光建置成本就會讓人退避三舍，甚至還會影響建物既有裝潢及架構。這類系統大致只有一些對安全有非常極致考量的高機密軍事或高科技單位才會採用。

若將焦點放在資訊安全上，只要是檔案，就難免會有被竊取備份的可能性，同樣地，由生物特徵所轉換的數位樣本檔，當然也可能會有同樣的風險出現。尤其是不支援在前端裝置完成比對作業的生物辨識系統，這類系統多採一對多比對機制，由於會有往後端撈取資料庫樣本檔進行比對的動作，致使樣本檔從資料庫傳送到前端裝置的過程中，難免會出現有心駭客從中攔截竊密的突破點。或許廠商會說，即使資料遭竊也不會造成生物影像檔等個人隱私的外洩，因為駭客頂多只能攔截到生物特徵樣本檔，而並非原始的生物影像檔。站在個人隱私權的立場來看的確如此，但實際上，就算是竊取到原始生物影像檔也毫無用處可言（除非被竊者在另一處的身分識別也採用同樣的特徵擷取演算法，但取樣環境差異太大的話，辨識成功率也是微乎其微），難道駭客會不知道這層道理嗎？駭客的目標當然在樣本檔上，其目的當然是拿來用在下次門禁或電腦系統的登錄之用，所以豈非沒有安全疑慮？

撇開後端樣本資料庫本身的安全性不提，或許支援前端裝置特徵比對的生物識別系統會相對安全得多，這類系統多半採用一對一比對機制（但一對一比對機制的系統不見得支援前端裝置比對），由於範本樣本檔已經預先儲存在安全無虞的前端裝置中，所以比對作業全在前端完成，安全性自然較高。

不僅如此，由於該方案會搭配識別卡，在比對範圍縮小的情況下，精準度自然大增。與多重生物辨識相比，會是最划算又能提升精準性的解決方案。但就如前文所述，由於前端裝置的容量有限，所以無法同時儲存太多的樣本檔，因此比較適合人數較小的公司，或是公司下轄的特定部門。或許中大型企業，可以分別在特定部門裡安裝上述系統，如此才是較安全的做法。當然，如果特定部門也不少，相對較高的建置成本也免不了。以上諸點都是企業在導入生物辨識機制時，務必特別注意的要點。

責任編輯／洪羿漣