美軍生物辨識技術之發展與應用

作者／李建鵬中校、周兆龍中校

提要

一、生物辨識技術是根據人類臉部、指紋、掌紋、虹膜、掌/指靜脈、聲音、簽名和步態等各種生理及行為特徵來進行使用者的身分認證。目前已被廣泛應用在門禁管制、行動支付、機場通關、網路金融、犯罪調查、無人商店等領域。

二、2001 年美國發生 911 恐怖襲擊事件後，美軍開始思考如何利用生物辨識技術有效支援反恐任務。自 2008 年以來，美軍透過生物辨識技術的協助，已逮捕或擊斃超過 1 萬多名敵軍，並阻止了數萬人次試圖闖進美軍基地的事件，成效斐然。

三、本文將以美軍近年來在生物辨識技術方面的發展現況與應用實例，探討在軍事方面的應用，以提供國軍未來相關政策發展與技術研究之參考。

關鍵詞：生物辨識技術、身分認證、行動支付、反恐任務。

前言

隨著資訊科技與網路的快速發展，現今愈來愈多人仰賴各種行動裝置(如智慧手機、平板電腦、穿戴式裝置、筆電…等)作為資料儲存及傳輸的主要媒介，無論是在社交溝通、資訊傳遞、工作學習等，都與人們的日常生活密不可分。為了維護資訊安全，當使用各種資訊設備時，最基本就是要採取適當的存取控制(Access Control)。所謂存取控制是一種透過實體管制(Physical Control)或制定管控措施(Policy-driven Control)，以允許或禁止某人使用某項資源，以確保系統重要資源(包括資料、軟硬體、應用系統、網路等)免遭非授權人員的誤用或攻擊。

各種存取控制措施當中，身分認證是第一線也是最基礎的防護機制。在使用電腦、網路或行動裝置之前，要求使用者輸入帳號密碼，以確認使用者的身分。然而，這種使用密碼的傳統方式有幾個明顯的缺點，第一，密碼易遭受竊取或暴力法攻擊破解；第二，為了防止密碼遭破解，要求使用者採用高安全度密碼或定期更換密碼，然而過於複雜或頻繁的更換密碼讓人不容易記憶；第三，各種系統對於帳號密碼都有不同程度的要求規範，若在不同系統之間設定帳號相同密碼，則一旦密碼遭竊，所有系統都面臨相同風險，但若設定不同密碼，又會增加使用者的不便。

為了改善傳統密碼的缺點，近年來開始採用所謂的「雙因子認證(Two Factor

Authentication, 2FA)」機制。顧名思義，雙因子認證就是除了密碼之外，還必須加上另一個驗證因素，例如 PIN 碼或個人生物特徵等方式，當同時兩種因子都通過驗證才能允許存取，可大幅提高身分認證機制的安全性。

採用 PIN 碼的方式通常是由 IC 晶片整合在個人的工作證、金融卡、信用卡或健保卡等身分證件上，但仍可能存在因遭竊或遺失而遭到冒用的風險。採用生物辨識技術的方式，使用者無需額外攜帶各種 IC 晶片，也無遭竊的風險，只需以個人身上的指紋、人臉或虹膜辨識，即可確認使用者的真實身分，相較於採用 PIN 碼的方式具有更佳便利性與安全性的顯著優勢。

在古代沒有先進的科學技術，身分認證方式大多是採用獨特的識別物件，如皇族與官員身分象徵的腰牌、令牌、金印、印璽，調用軍隊的虎符，官員遷調的魚符等[1]，其形式和作用都類似於現今使用的身分證。而自 1910 年法國里昂成立全球第一間警局犯罪鑑識實驗室之後，人類的各種生物特徵便開始被大量應用在犯罪偵查的相關依據，包括毛髮、皮膚、血液、指紋、牙齒、人臉(繪圖或照片)、簽名、DNA 等，直至今日生物特徵仍是鑑識科學(Forensic Science)中最不可或缺的一環。

生物辨識技術是根據人類臉部、指紋、掌紋、虹膜、掌/指靜脈、聲音、簽名和步態(Gait)等各種生理(Physical)及行為(Behavioral)特徵來進行使用者的身分識別。生物特徵具備下列特性：

一、普遍性(Universality)：只要是人類就擁有生物特徵。

二、獨特性(Distinctiveness)：任何人的生物特徵都會呈現相當程度的差異。

三、不變性(Permanence)：不易隨時間而改變，或者改變非常的緩慢。

四、易蒐集(Collectability)：方便蒐集和測量。

五、高效能(Performance)：可快速蒐集，穩定度與精確度高。

六、可接受性(Acceptability)：使用者接受度高，不排斥使用。

七、不可欺性(Circumvention)：不容易偽冒。

基於前述特性，生物辨識技術已被應用在各種範疇，舉例如下：

一、門禁管制

例如個人住家社區、辦公大樓、飯店，常可見到利用指紋或人臉等生物特徵進行管制。

二、系統登入

微軟 Windows 10 作業系統中的 Windows Hello 生物辨識認證功能，支援使用者在使用電腦或筆電時，可透過臉、眼睛或虹膜執行登入或解鎖。各種高階智慧型手機，

[1] 邱建華、馮敬、郭偉、周淑娟，《生物特徵識別》(北京：清華大學出版社，2016 年)，頁 2~3。

也幾乎會搭載指紋感測器，方便使用者快速登入解鎖。

三、行動支付

韓國三星電子的 Samsung Pay 服務，搭配三星高階手機，可支援指紋或虹膜的方式進行行動支付。蘋果手機自 iPhone 6 開始，也推出 Apple Pay 服務，支援 TouchID 指紋進行行動支付；2017 年推出的 iPhone X 則改採 Face ID 的 3D 人臉辨識技術進行款項支付。

四、機場通關

美國全球入境計畫(Global Entry)，對於無犯罪紀錄或風險的旅客，可透過自助登機專櫃掃描護照及指紋，便能享受快速通關的便利服務無需排隊使用傳統人工查驗櫃檯，我國自 2017 年 11 月 1 日起成為美國第 8 個加入全球入境計畫的國家。

五、網路金融

國內已有多家銀行推出數位分行，導入生物辨識技術，例如靜脈無卡提款機、人臉辨識迎賓互動牆、電話客服語音辨識…等，目前還在發展階段，只要風險管控良好，未來生物認證將成為金融應用不可或缺的主流技術。

六、犯罪調查

2013 年所發生的美國波士頓馬拉松爆炸案，美國聯邦調查局發現疑似嫌犯的監視器圖像，接著運用了臉部辨識技術比對犯罪紀錄資料庫，確認了嫌犯的身分，並成功逮捕到嫌犯。

七、無人商店

2016 年 12 月美國亞馬遜宣布推出無人商店「Amazon Go」，透過專用 APP 掃描二維條碼(QR Code)辨識身分，讓消費者不用排隊結帳，離開商店就能自動從帳戶扣款。2017 年 8 月上海更進一步開設了第一間「刷臉」無人商店，透過專用的 APP 進行臉部辨識後，系統會自動識別使用者身分與購買的商品，並自動完成線上帳戶扣款。相較於現行的行動支付與「Amazon Go」，更加提升便利性。

八、晶片身分證

我國現正推動國民晶片身分證(eID)換發作業，內政部也規劃未來將具備自然人憑證功能，可整合報稅、駕行照、悠遊卡、電子投票等多種功能，並將提供指紋及虹膜辨識功能。

從上述個人、企業、政府、商業或犯罪調查的應用案例可以看出，生物辨識技術的發展與應用方興未艾。實際上，生物辨識技術近年來也開始被大量應用在軍事事務上，例如基地防護、人員管理、人道救援、目標識別、反恐任務…等。根據美國國防部統計，自 2008 年以來，透過生物辨識技術的協助，美軍已經逮捕或擊斃超過 1 萬 7 千名敵軍，並阻止了 9 萬 2 千人次試圖闖進美軍基地的事件。

2001 年美國發生 911 恐怖襲擊事件之後，美軍開始思考如何利用生物辨識技術來鎖定具有犯罪紀錄的人員或辨識可疑的恐怖份子，以有效支援反恐任務。他山之石，可以攻錯。本文將回顧說明生物辨識技術的基本特性與發展現況，並介紹美軍近年來在生物辨識技術方面的軍事應用與發展，提供國軍未來相關政策發展與技術研究之參考。

生物辨識技術介紹

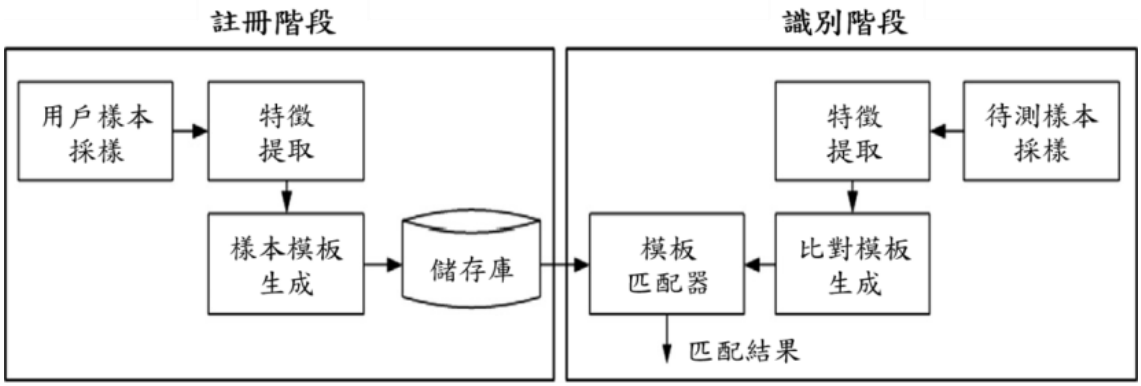
在 1963 年 Mitchell Trauring 於自然期刊中發表了一篇運用指紋匹配作為自動生物辨識的研究論文，這是在生物特徵自動識別研究領域發表的第一篇論文，自此之後，運用其他特徵(如語音、虹膜、臉部和簽名)的自動生物辨識系統也在 20 世紀 60 年代開始陸續研究開發。[2]

生物辨識系統的作業原理是將感測器獲取生物特徵樣本(圖像)中的顯著或可鑑別特徵，與預先儲存的模板樣本相匹配，以識別用戶之身分。基於上述作業原理，生物辨識系統必須包括「圖像採樣模組」: 結合感測器以獲取測試者的生物特徵原始圖像；「特徵提取模組」: 處理所獲取的圖像，從中提取顯著或可鑑別的特徵;「匹配器模組」: 將待測樣本中提取的鑑別特徵與模板樣本特徵進行匹配，所獲得匹配分數提供系統決定接受或拒絕待測者所聲明的身分；「資料庫模組」: 儲存模板樣本資料，提供匹配器模組特徵匹配使用。

一、系統架構

典型的生物辨識系統區分為兩個階段的操作架構，即「註冊階段」和「識別階段」(如圖一)，簡述如下：

圖一 典型生物辨識系統的操作架構圖



資料來源：作者繪製。

[2] Anil K. Jain, Karthik Nandakumar, Arun Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," Pattern Recognition Letters 79, 2016, pp.80 – 105.

(一)註冊階段

此階段的操作流程係由生物辨識系統的採樣模組獲取欲註冊用戶的生物特徵樣本，再由特徵提取模組從樣本中提取顯著或可鑑別的特徵集，以生成樣本特徵模板，並將模板與用戶關聯產生識別碼後儲存在資料庫中，以作為後續識別匹配使用，此階段是建立用戶身分必須要完成之程序。

(二)識別階段

生物辨識系統係使用相同的採樣模組，再次獲取待測者的生物特徵樣本，並由特徵提取模組中，提取鑑別所需的特徵集，並將該特徵集與資料庫中的模板樣本特徵進行關聯匹配，以便確定匹配結果後，提供識別系統決定接受或拒絕待測者所聲明的身分。

二、運作方式

生物辨識系統通常以下列其中一項方式運作：

(一)使用者認證(Verification)[3]

使用者主動向系統感測器提交生物辨識特徵，並聲明以某特定身分登錄系統，生物辨識系統則依使用者提交的生物特徵，與所聲明特定身分註冊登記的生物辨識特徵模板進行一對一(1：1)的匹配比較，最後將驗證結果回應使用者是否通過授權或拒絕存取。這是以驗證所聲明的個人身分為目的，只要所得到的匹配分數(也稱為相似度值)高於預設門檻值，則接受所聲稱的身分，在這種情況下，生物辨識系統即是以使用者認證方式運行，亦稱為主動識別方式，相關應用包括電腦用戶登錄、ATM 操作、電子商務、行動裝置的存取控制及用戶認證。

(二)不明身分識別(Identification)[4]

操作者將待測人員的生物特徵提交給生物辨識系統(非待測者主動配合提交)，而系統嘗試在待測者沒有聲明某特定身分的情況下，將待測生物特徵與資料庫中所有註冊登記的生物辨識特徵模板進行一對多(1：N)的匹配比較，以識別待測人員的真實身分。身分識別方式的使用時機通常是在受測者否認擁有特定身分時，採取被動提交特徵以認證真實身分的主要作法，可阻止個人使用多重身分，相關應用包括身分證、護照、駕駛執照等證件申請核發、出入境過境費及社會福利應用。

(三)篩選(Screen)[5]

此種運作方式是屬於身分識別的延伸應用，在特定場所部署生物辨識系統，運用

---

[3] A. Jain, A. Kumar, "Biometric recognition: an overview," in: E. Mordini, D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context, vol. 11, Springer, Netherlands, 2012, pp49 - 59.

[4] Ibid 3, pp59-79。

[5] A K. Jain, S. Pankanti, S. Prabhakar, H. Lin, A. Ross, "Biometrics: a grand challenge," in: Proceedings of the 17th International Conference on Pattern Recognition, 2004, pp935 - 942.

此系統對該場所範圍活動的人口逐一採樣，結合特定身分觀察列表的資料庫實施一對多(1：N)的身分識別匹配，以掌握特定對象(如恐怖份子)是否在此場所出現，相關應用包括機場安全、政府機構安全和公眾活動維安監控。

三、效能評估

生物辨識系統的效能評估通常受外在環境和系統性能因素的影響，環境因素包括系統周圍的溫度、濕度和照明條件，而性能因素包括拍攝圖像品質、註冊與識別階段的時間間隔及識別演算法的設計，所以生物辨識系統的效能經常使用採樣誤差(Sample Acquisition Errors)和性能誤差(Performance Errors)據以量化評估，如下所述：

(一)採樣誤差

意即受系統周圍的環境條件影響導致採樣錯誤之比率，在需要使用自動成像模態的識別系統中，這種錯誤是普遍存在的。例如識別系統因採樣的圖像品質過差或外在雜訊，而拒絕用戶的登錄失敗比率(登錄失敗率)，或者是成像感測器無法拍攝有效的生物特徵樣本圖像比率(採樣失敗率)，皆屬於採樣誤差之計算方式。

(二)性能誤差

主要適用於測量真實環境中生物辨識系統的準確性，茲針對各項性能誤差指標簡要說明如下：

1.假匹配率(False Match Rate, FMR)或假接受率(False Accept Rate, FAR)，識別系統將未經授權的用戶識別為合法用戶的比率，這屬於無效匹配的測量值，也稱為「類型 I 錯誤」。就生物辨識系統的匹配能力而言，此類型的錯誤率必須盡可能地低。

2.假不匹配率(False Non-Match Rate, FNMR)或假拒絕率(False Reject Rate, FRR)，識別系統將授權用戶識別為冒名頂替者的比率，這屬於拒絕有效輸入的測量值，也稱為「類型 II 錯誤」。從用戶的便利性角度來看，此類型的錯誤率同樣必須盡可能地低。

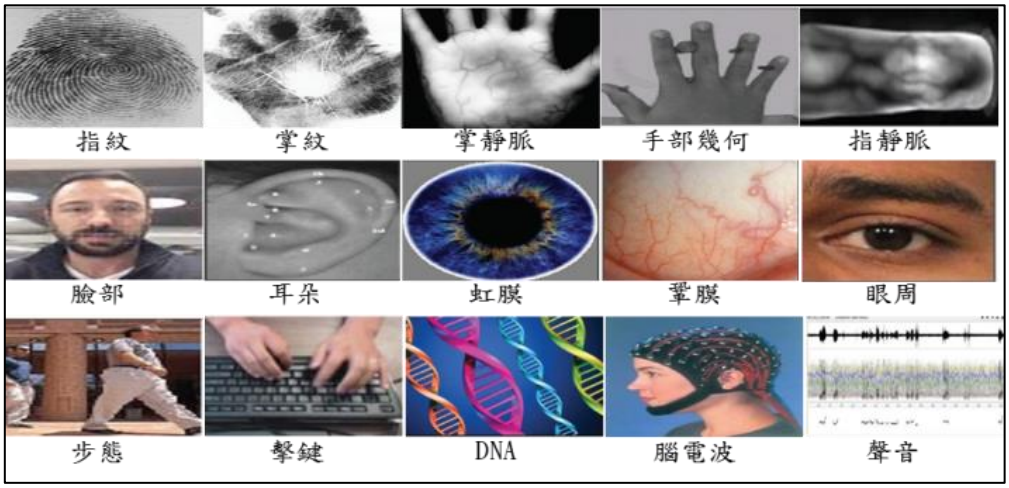
3.等誤差率(Equal Error Rate, EER)，它指的是假接受率和假拒絕率彼此相等的點，在系統設計時，針對「錯誤」接受或拒絕之間的權衡考量，而訂定的門檻值。如果系統設計成容忍輸入變化和雜訊(降低門檻值)，則將使假接受率增加而使假拒絕率降低；相反的，將系統設計成不允許輸入變化和雜訊(提高門檻值)，則會使假接受率降低，而增加假拒絕率。所以，在實務上等誤差率常做為設計生物辨識系統準確度的測量標準。

設計生物辨識系統的採樣模組及特徵提取模組時，主要應該要考量選用合適的感測器、設計較佳的特徵表示方式，和運用相似性測量將識別誤差最小化等面向的問題，在解決這些問題的同時也須注意不可降低在生物特徵中所隱含的身分資訊，尤其要注意以下原則：從同一位受測者採樣同類型生物特徵的不同樣本，其相似性應該非常高；從不同受測者採樣同類型生物特徵的不同樣本，其相似性應該非常低。

四、各類型生物特徵模式

常見的生物特徵包括有臉部、指紋、虹膜、聲音、簽名、掌紋、手靜脈、DNA 步態、耳朵、視網膜/鞏膜、擊鍵(Keystroke)和腦電波圖信號…等。(如圖二)指紋、臉部及虹膜是目前最盛行的三種生物辨識特徵。指紋和臉部識別應用普及的原因，主要是因為世界各國的執法機關和其他政府機構在業務需求下，長期蒐集並累積了許多大型的指紋或臉部資料庫(例如駕駛執照和移民資料庫)，運用前述資料庫結合新開發的辨識技術，大幅提升了此類型生物特徵的可用性。而虹膜識別受限於傳統的虹膜資料庫較少，且其應用需要將重複數據刪除以確保高精確度，相比於指紋和臉部識別部署的應用範圍較小，但因其高精確度的特性，也開始部署在越來越多的大規模識別應用中，例如阿拉伯聯合大公國的虹膜識別過境系統。

圖二 運用於生物辨識的各類型生物特徵示意圖



資料來源：作者繪製。

本文僅針對指紋、臉部及虹膜三種生物辨識特徵模式作一簡略的介紹。

(一)指紋辨識

指紋辨識應該算是歷史最久遠的生物辨識技術，在中國古代就常以按壓拇指指印的方式簽署重要文件或買賣契約，當時雖未使用相關科技識別技術，但其概念即屬於最早的指紋辨識雛型。

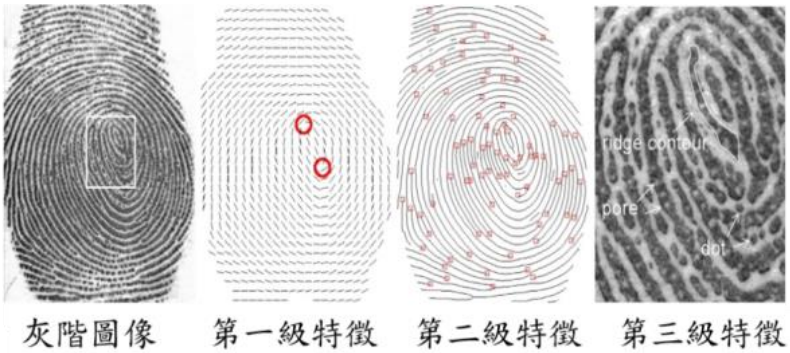
傳統的指紋圖像可分為滾動按壓、平面按壓及潛在指紋等三類(如圖三)，通常在用戶配合時，使用指紋掃描感測器採樣獲得的滾動及平面指紋圖像品質很好，辨識系統使用前述圖像較易於提取特徵值進而匹配比對。相對的，潛在指紋存在於個人無意間接觸或使用的物體表面上，必須運用各種手段將其採起，困難度相對較高及圖像品質相對較低，所以較適用於執法取證相關特殊的應用。

圖三 三種類型的指紋圖像

資料來源：作者繪製。

指紋特徵通常分為三級，第一級特徵採用了指紋的宏觀細節，以指紋紋理的走向可區分為左旋、右旋、拱型、尖拱型、螺旋及雙螺旋等類型的紋理走向。另外，由脊線走向形成的特殊點(稱為奇異點)亦屬於第一級特徵，其中包含某一脊線方向終止處的「核心點」及三條脊線匯集處的「三角點」。前述特徵的辨識度不高，僅能對指紋進行粗略區分，必須獲得進一步的特徵才可滿足身分認證所需的獨特性。第二級特徵是指更精細的指紋特徵，也稱為「細節點」特徵。主要應用指紋脊線的分岔點和終結點，是一種具方向性的點，細節點的方向即可代表局部脊線的方向。在一張指紋圖像中通常包含 50 個以上的細節點，資料量不大故易於儲存，再加上細節點特徵穩定以及辨識度極高，是目前指紋識別系統技術中最主流應用的特徵。指紋的第三級特徵則是比第二級特徵更為精細，需要在高數位解析度的圖像中才可以獲得，而所謂的第三級特徵指的是手指表皮的毛孔、脊線輪廓和點等特徵，由於穩定度欠佳，且資料量大不利儲存，在自動指紋辨識系統中較少使用，較適合應用在執法單位鑑識科學方面(如圖四)。

圖四 指紋的三級特徵



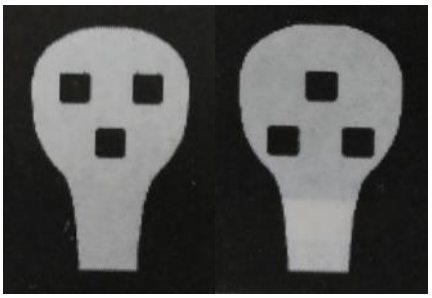
資料來源：A. Jain, A. Kumar, “Biometric recognition: an overview,” in: E. Mordini, D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context, vol. 11, Springer, Netherlands, 2012, p87.

(二)人臉辨識

自古以來人臉辨識在人類社會中是最平常及最自然的工作，成年人之間的人際互動、青少年崇拜偶像明星或嬰幼兒只認得父母而害怕陌生人等，都是人類自然辨識人

臉的範例。人臉圖像認知是人類與生俱來的能力，人類的視覺系統對人臉具有天生的識別基因。根據研究成果[6]表示，嬰兒對類似於人臉的模板圖像有相當高的興趣，尤其是對上重下輕圖案的關注度遠大於上輕下重的模板圖像(如圖五)，說明了人類的視覺系統天生對人臉圖案具有強烈的識別敏感度。人臉辨識看似容易，但是應用在計算機的領域中，人臉的非線性結構對特徵識別模式卻成為了複雜的問題。

圖五 上重下輕(左)及上輕下重(右)的臉部模板圖像



資料來源：作者繪製。

早期的臉部辨識系統是運用幾何特徵方法，將五官設定為預定地標，測量五官之間對應點和線的組合，進而構建人臉的幾何形狀圖以作為識別分類器的簡單方法，受限於當時計算機能力，辨識精準度不佳。在 1991 年美國麻省理工學院的 M. Turk 和 A. Pentland 提出以整體臉部外觀的主成分分析(Principle Component Analysis, PCA)之「特徵臉」方法[7]，此方法為第一個以大規模人臉數據的統計及訓練為基礎的特徵提取方法，使人臉辨識進入數據統計時代。後續有學者針對特徵臉缺乏人臉具體細節的缺點陸續提出改進研究，如 Wiskott 等人提出的「彈性圖匹配」方法是利用臉部模型識別的研究，透過檢測臉部的若干基準點(例如眼角、鼻尖、嘴角和下巴)並構建 2D 或 3D 臉部模型的屬性圖，其中包含了臉部關鍵特徵點及多方向局部特徵的組合。對於任意輸入的人臉圖像，先對預先定義的臉部關鍵特徵點定位後，再提取多方向局部特徵，最後得到輸入圖像的屬性圖，進而與已知人臉屬性圖進行相似度匹配完成辨識。此方法的優點是既保留了臉部的全面結構特徵，也對人臉的關鍵局部特徵進行建模，改善了特徵臉缺乏具體細節的缺點。

受惠於計算機的運算能力持續提升，使生物辨識模式進入了大數據時代，在 2001 年 Viola 和 Jones 提出利用自適應提升(Adaptive Boost)和類哈爾特徵(Haar-like Features)的人臉檢測演算法[8]，構建了數目達到 20 萬以上的高冗餘特徵集，並將幾萬張已標註

[6] F. Simion, V. M. Cassia, C. Turati, "The original of face perception: specific versus non-specific mechanisms," Infant Child Develop, 10, 2001, pp.59-65.

[7] Turk M., Pentland A., "Face recognition using eigenfaces," IEEE Computer Society Conference on. IEEE, 1991, pp. 586-591.

[8] P. Viola, M. jones., "Robust real-time face detection," International Journal of Computer Vision, 57(2), 2004, pp.137-154.

的人臉及非人臉圖片(訓練用)透過前述演算法，對這些冗餘特徵進行選擇及合併，從大規模的數據中自動學習分類資訊，其成果將臉部識別準確度提升一個數量級，數據量增加了 10 倍以上，此項研究成果被視為臉部識別的一項代表性里程碑。雖然演算法的進步有助於提高人臉辨識的精確度，但在 2D/3D、紅外線或視頻攝影機的數位攝影科技技術的大幅精進，同樣也使人臉辨識系統進展良多。由於半導體技術的改進，圖像感測器的偵測速率、空間解析度和品質已顯著提高，同時感測器也變得更小、更便宜，可將它們嵌入許多個人電子設備，如穿戴裝置(如 Google 眼鏡)、平板電腦和行動電話中，用以拍攝高品質的臉部圖像，進而使得臉部辨識的應用範圍更加廣泛。

大部分的生物特徵辨識技術在實際生活應用中需要部署專用的感測器，而人臉辨識唯一需要的感測器設備僅是攝影機，無論是在公共(私人)場所的監視器或是筆記型電腦、智慧型手機及其他行動裝置上配備的攝影鏡頭都可適用。使得人臉辨識不受時間及空間的限制，只要完成臉部拍攝就可以由識別系統進一步完成身分認證，其便利性同時大幅提升了臉部辨識技術的可用性，也是任何其他生物特徵辨識技術所無法相提並論的。

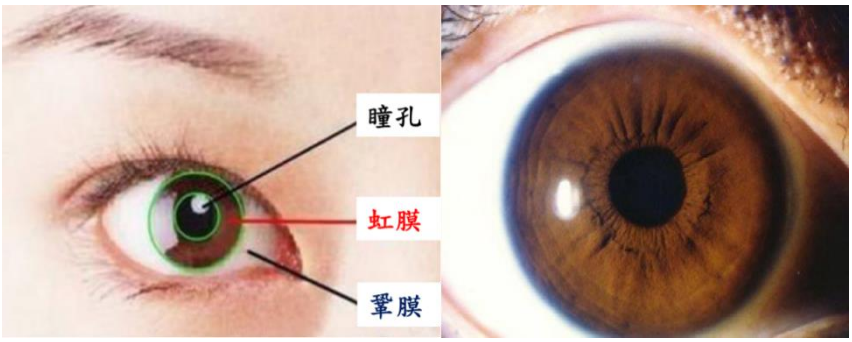
人臉辨識區分靜態與動態，傳統的靜態人臉辨識需要受測者站至定位並面向指定鏡頭拍攝靜態照片後實施辨識，且無法同時辨識非特定多數人群；而所謂的動態影像人臉辨識技術指的是即使被拍攝的對象在移動且並未意識到鏡頭，也能即時進行人臉辨識。運用動態辨識技術，就能快速解析監控系統影片，檢測可疑人物，進而預防特定事件的發生。以軍事行動應用為例，將動態影像人臉辨識系統部署在重要設施出入口，人員進出不需要刻意站在鏡頭前，在自然行走過程中就能完成辨識，可於短時間內分辨敵、我(友)軍及平民，可用性及便利性更是大幅提升。目前在動態影像人臉辨識技術中，主要導入兩項核心技術為「多重比對人臉偵測法」以及「深度學習(Deep Learning)」。運用多重比對技術可改善在不同角度或遭遮擋時人臉影像比對的精準度，而導入深度學習可強化系統對臉部方向變化、距離鏡頭太遠(低解析度)的人臉影像辨識能力，相較於傳統電腦視覺的特徵抽取(Feature Extraction)，使用多重比對及深度學習的人臉辨識系統，可以達到更好的效果。

(三)虹膜辨識

虹膜是介於眼角膜之後、水晶體之前，鞏膜與瞳孔之間的「環狀可視薄膜」，它具有紋理、血管和斑點等多項細微特徵(如圖六)。從眼睛的外觀上來看，鞏膜為眼球外圍的白色部分，約佔眼睛結構面積的 30%，眼睛中心的瞳孔面積僅約佔 5%，虹膜即佔了眼睛結構面積的 65%，而且虹膜中含有色素，不同人種具有不同的顏色，且內含豐富的紋理資訊，是人體中最獨特的結構之一，可用於個人識別。虹膜的形成是由遺傳基因決定，人類至週歲左右虹膜就已經發育到穩定狀態，並可維持數十年不會有

太大的變化，除了極少數的異常病變或受外力影響，才可能造成虹膜外觀的改變。虹膜辨識是利用人眼圖像中虹膜區域的環狀物、皺紋、斑點及冠狀物等特徵，建立特徵模板，之後透過匹配或比較這些特徵參數以完成身分識別。每個人的虹膜都是獨一無二的，而且即時虹膜掃描不太可能提供假樣本，因此虹膜作為身分認證技術是相當可靠及穩定的。

圖六 虹膜示意圖



資料來源：作者繪製。

在 1985 年眼科學家 Leonard Florin 和 Aran Safir 提出了拍攝虹膜圖像、特徵提取和自動匹配的研究構想，取得虹膜辨識系統的第一項專利。在 1993 年 John Daugman 研發了第一個實際運作的虹膜辨識系統，該系統結合了虹膜相機及虹膜特徵提取演算法(IrisCode)，以壓縮二進制碼的形式來表示虹膜圖像特徵，現有的商規虹膜辨識系統產品大多以 Daugman 的演算法為基礎，已成功地應用於大規模人口的身分認證，例如阿拉伯聯合大公國、荷蘭、美國和加拿大等國家在出入境管制方面部署了虹膜辨識系統，英國則使用了虹膜辨識的移民系統以及美國軍方在阿富汗和伊拉克進行的軍事行動，也廣泛使用了虹膜辨識。

由虹膜相機拍攝受測者的眼睛圖像後，接著就要將影響識別的干擾因素去除，即是找到虹膜與瞳孔的邊界(虹膜內圓定位)以及虹膜與鞏膜的邊界(虹膜外圓定位)，主要目的是將眼睛圖像中的虹膜區域定位出來，以進一步提取虹膜特徵。由於眼睛圖像中部分虹膜區域常被上下眼瞼、睫毛所遮蓋，所以在虹膜定位前必須將前述影響因素去除，進而提升定位的精確度。目前虹膜定位演算法主要有 John Daugman 提出的「微積分圓形邊緣探測器法」，利用微積分演算子搜索圓形邊界進一步定位出虹膜的內外邊界，準確性及穩健性較高，但是搜索計算所需時間較長。值得注意的是，虹膜區域面積的大小直接受到瞳孔變化的影響，而瞳孔變化又與人類生理需求及環境光照變化息息相關，當瞳孔極度收縮時直徑可小於 1mm，在極度放大時瞳孔直徑可達 9mm，大小差異範圍相當大，會造成特徵提取及匹配精確度的影響。

虹膜辨識技術發展在早期受限於圖像採集設備體積龐大且價格昂貴的窒礙因素，

還需要受測者高度合作將頭部保持在相對穩定的位置，同時直視相機，才不會由於離軸採樣、部分閉合的眼瞼或睫毛，以及過度擴張或收縮的瞳孔等因素無法拍攝高品質且清晰的虹膜圖像。另外再加上暗色的虹膜在可見光下無法明確分辨紋理細節，受光源影響會導致圖像亮度不均及紋理失真，而需採用近紅外光光源以避免前述影響。所以，虹膜圖像的獲得相對於指紋及臉部圖像較為不易，直接箝制了虹膜辨識技術的發展。時至今日，虹膜辨識技術同樣地受惠於半導體技術及光學感測元件技術的開發與成長，使虹膜相機已變的更方便攜帶、體積小、價格實惠及容易使用。以韓國三星公司在 2017 年 3 月推出的 Galaxy S8 智慧型手機為例，該型手機同時採用了指紋、臉部及虹膜辨識等三種生物特徵辨識模式作為手機解鎖工具，其中虹膜辨識即是運用近紅外線相機(700~900nm 紅外線 LED 及影像感測鏡頭)結合相機控制技術，當用戶觀看螢幕時，手機上的紅外線 LED 燈便會閃爍，再由近紅外線相機拍攝虹膜圖像，進而提取特徵紋理以辨識用戶身分。由此可知，虹膜辨識技術已有巨大突破，未來虹膜辨識可朝向在可見光、遠處和移動的條件下獲得受測者的虹膜紋理，並進行識別技術之研究，其應用前景可期。

美軍生物辨識發展概況

美軍開始運用生物辨識技術起源於 1999 年美國國會的一份生物辨識技術可行性研究報告，該報告中指出生物辨識技術是一種新興科技，對於國防部至關重要，必須加以標準化與集中化管理。2000 年，美國聯邦公法(Public Law 106-246)明定由美國陸軍部長代表美國國防部(DoD)執行各項生物辨識計畫指導與協調工作，美國陸軍在當年隨即於資訊部門下設立了生物辨識管理辦公室(Biometrics Management Office, BMO)。

美軍初始發展生物辨識技術階段，主要研究方向為國防部人員出入營區的實體安全及網路作業安全應用，較偏向基礎技術研究。為了能更有效的支援作戰任務，於 2006 年改名為生物辨識特遣部隊(Biometrics Task Force, BTF)，並改隸屬於作戰訓練部門管制，BTF 職掌為負責制定國防部生物特徵辨識技術的戰略方向，協同其他政府部門共同制定生物辨識標準與政策，管理生物特徵資料庫系統與支援戰場上各項生物辨識設備操作與維護。

2010 年 BTF 生物辨識特遣部隊擴編更名為生物辨識身分管理局(Biometrics Identity Management Agency, BIMA)，2013 年 BIMA 整合了原先隸屬陸軍內部的鑑識(Forensic)單位，整併為國防鑑識與生物辨識管理局(Defense Forensics and Biometrics Agency, DFBA)，由憲兵司令直接管轄。美軍近年生物辨識組織發展進程如圖七。DFBA 為現行美軍統籌生物辨識業務的最高執行機關，編制約 250 人，共包括策略整合部門

(Strategic Integration Division)、作戰部門(Biometrics Operations Division)及專案部門(Programs Division)等三個部門，組織架構如圖八。

圖七 美軍生物辨識組職發展進程

資料來源：作者繪製。

圖八 美軍國防鑑識與生物辨識管理局(DFBA)組職架構

資料來源：作者繪製。

DFBA 依照國防部政策、願景、聯戰訓練目標及軍種需求，制定美軍生物辨識策略架構，需求規劃、能量籌建、工程研發、標準制定及教育訓練，並負責維管生物特徵資料庫系統，執行生物特徵的儲存、比對、分析與分享等作業，提供執法單位、情報部門、國際盟友及作戰部隊運用。其主要職掌如下：

一、負責代表國防部執行各項生物辨識計畫、專案。

二、負責指導並執行生物特徵的採集、儲存、比對、分析與分享作業。

三、確保國防生物辨識技術的裝備、系統與服務，符合國防部的標準架構與相容性規範。

四、負責通用、專業與跨部門單位之間的需求研議、架構與標準之發展。

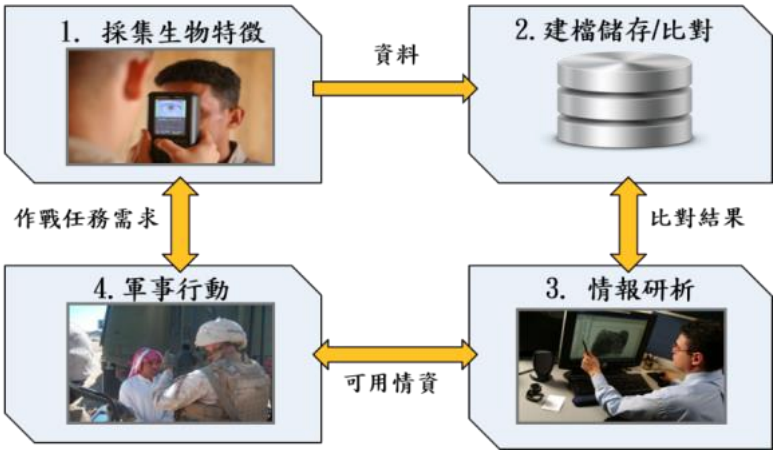
五、建置生物辨識技術能量，以滿足作戰部隊與指揮官之作戰需求。

六、監督與維護國防部授權之生物辨識資料庫，負責匯集各個來源之生物辨識資料，並加以儲存、比對與分享。

美軍生物辨識作業流程(如圖九)透過前線作戰部隊採集各種生物特徵，傳輸至資

料庫加以建檔與比對，比對結果交由情報部門研析或提供作戰部隊指揮官運用，最終以滿足支援作戰任務需求為主要目標。

圖九 美軍生物辨識作業流程圖



資料來源：作者繪製。

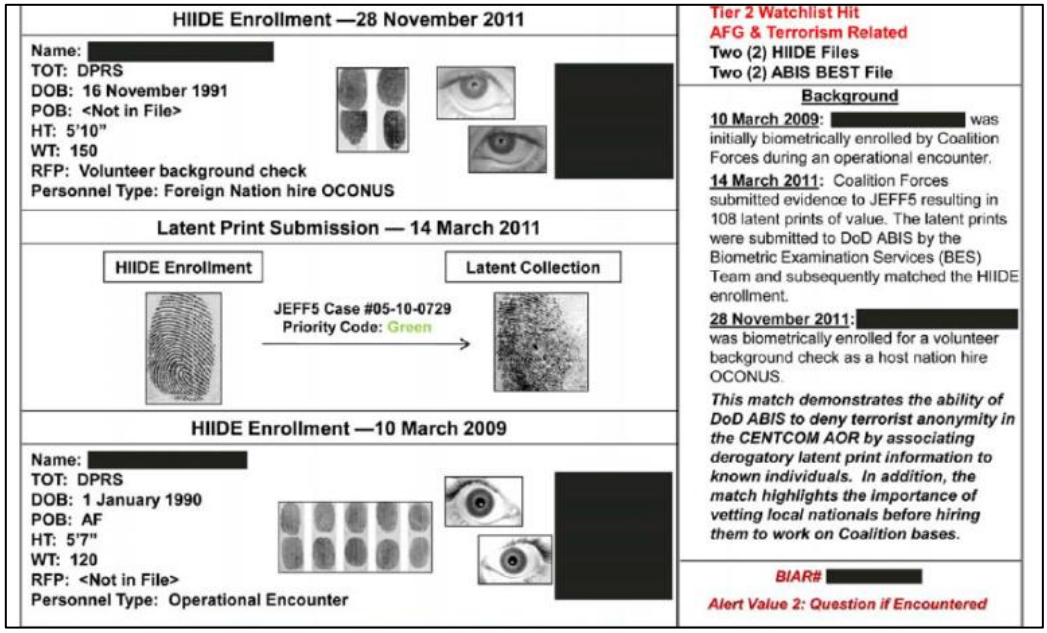
美軍為了能有效遂行生物特徵的儲存、比對、分析與分享等核心作業，於 2004 年建置自動化生物辨識比對鑑識系統(Automated Biometrics Identification System, ABIS)。ABIS 系統採集的生物特徵包括指紋、人臉、虹膜等；蒐集的對象包括列入觀察名單者、敵國軍事人員、犯罪者、被拘留者、申請進入美軍海外設施人員。ABIS 系統是參考美國 FBI 聯邦調查局的 IAFIS(Integrated Automated Fingerprint Identification System, IAFIS)自動化指紋比對系統所設計，可透過 ABIS 系統直接進入 FBI 的 IAFIS 系統進行交叉比對。美國 FBI 聯邦調查局的 IAFIS 資料庫自 1999 年開始使用，蒐集了曾遭逮捕或犯罪者的指紋和犯罪歷史資料庫，是美國司法部用以追蹤和比對犯罪紀錄最大型的資料庫，儲存超過 6 千 6 百萬筆以上的紀錄，透過這個交叉比對的功能，美軍可對在戰場所拘留的不明人士，進行犯罪紀錄的查詢，有效支援反恐任務。

美軍 ABIS 系統初始建置時可容納 1 千萬筆資料，每日可處理資料量為 1 萬 5 千筆。2014 年 ABIS 升級至 1.2 版，提升容量至 1 千 8 百萬筆資料，每日資料處理量也提升至 3 萬筆。ABIS 系統可顯示人員的基本資料，註冊的指紋、人臉、虹膜等生物特徵，以及比對結果。ABIS 系統畫面範例如圖十，畫面左側顯示了個人資訊及其指紋、人臉、虹膜等生物特徵；畫面右側顯示了比對結果，注意右上角為紅色告警字樣，顯示該員被列為 2 級觀察名單(Tier 2 Watchlist Hit)，與恐怖活動有所關聯。

目前美國政府各部門管理的生物特徵資料庫，除了美國 FBI 聯邦調查局的 IAFIS 系統資料庫與國防部的 ABIS 資料庫，還有國土安全部(Department of Homeland Security, DHS)的 IDENT 自動生物辨識系統。國土安全部的 IDENT 資料庫儲存了各種簽證、旅客、偷渡客、非法移民、合法居民、難民…等資料，也可直接進入 FBI 的 IAFIS

系統搜尋旅客或移民的犯罪記錄。目前美國 FBI 聯邦調查局、國土安全部及國防部已共同規劃未來整合為共享的作業環境(如圖十一)，預期將可大幅提升作業效能。

圖十 美軍 ABIS 系統畫面範例



資料來源：U.S. Government Accountability Office, "Defense Biometrics: Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics," GAO-12-442, 2012.

圖十一 美國聯邦調查局、國土安全部及國防部共享作業環境

資料來源：作者繪製。

美軍應用生物辨識技術之案例

一、裝備介紹

美軍將生物辨識技術視作一種戰場能力，對於區域衝突以及全球反恐戰爭產生重大的影響，亦對未來無論是在和平時期的突發事件、人道主義行動或大規模軍事行動，皆賦予生物辨識技術重要之定位。美軍近年來持續在各種軍事任務中運用生物辨識技術，並結合相關情報功能提供部隊對威脅進行準確分析的能力，進而更有效地反制威脅，同時最大限度地減少對周邊平民的影響。以美軍在伊拉克和阿富汗的兩個主要戰場為例，生物辨識技術提供了在戰場上積極尋找敵方人員的關鍵助力，同時也協助部隊即時區隔無辜者與意圖傷人者，以避免無辜平民遭受戰火波及。

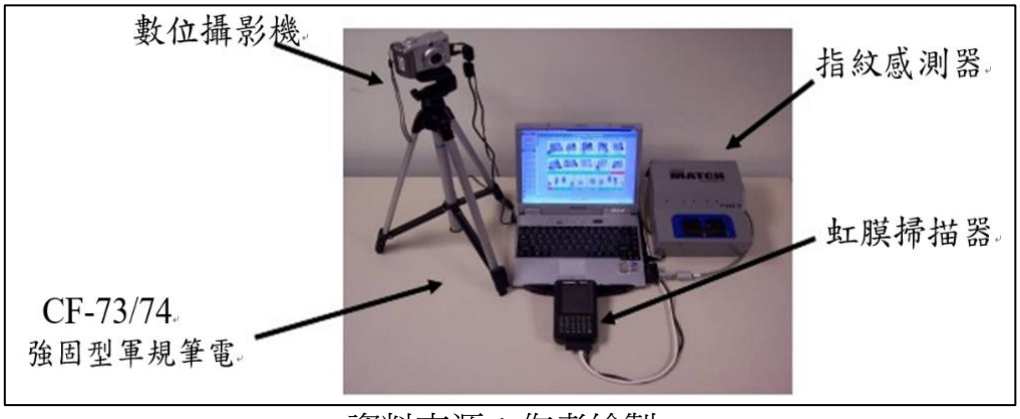
美軍於 2004 年底在伊拉克費盧杰市執行第二次叛亂份子掃蕩運動，海軍陸戰隊利用生物辨識技術在戰鬥中積極識別被捕的叛亂份子，以及在作戰行動之後返回城市的平民，生物辨識技術成為當時行動最重要的助力；美空軍將生物辨識技術作為基地安全的核心；美陸軍在各方面混用生物辨識裝置和資料庫，用來阻止敵戰鬥人員跨越國際邊界、進行人犯拘留和訊問行動；美海軍則是在對葉門海盜和馬克蘭海岸執行海上攔截行動任務中，運用生物辨識技術實施即時身分管理。

美軍在戰場所使用的生物辨識裝置，依不同作戰環境及需求，可概分為固定式及手持式，以下針對地面作戰和支援行動中，美軍所使用生物辨識裝置做一介紹：

(一)生物辨識自動化工具(Biometric Automated Toolset, BAT)

美國駐科索沃部隊因為缺乏辨識當地僱用人員的能力，而使有問題的當地雇員在解僱後，可以去另一個不同的營地應徵而重新被僱用，產生潛在的危安風險。為能夠有效辨識有問題的人員，所以美軍於 2001 年在科索沃建置了生物特徵識別自動化工具(如圖十二)，而後在伊拉克及阿富汗的大多數美國基地都使用 BAT 作為生物辨識工具。BAT 可運用其周邊裝置掃描指紋、虹膜及拍攝臉部圖像，亦可下載其他生物辨識裝置收集的資訊，儲存至強固型軍規電腦中的查詢和搜索資料庫(內含 120 萬筆以上資料及最新觀察列表)，並可將最新觀察列表上傳至行動裝置。

圖十二 生物辨識自動化工具諸元示意圖

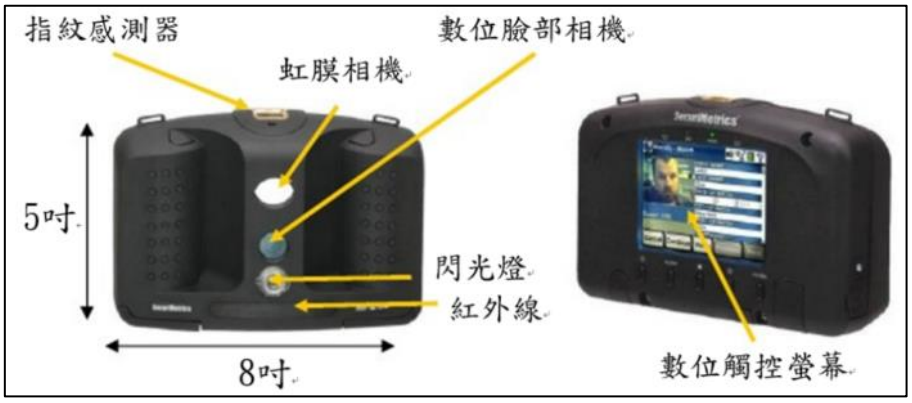


資料來源：作者繪製。

(二)手持式身分檢測設備(Handheld Interagency Identity Detection Equipment, HIIDE)

美軍為提供作戰部隊一個不受場地限制、便於攜帶的生物辨識特徵收集和識別平台而開發了 HIIDE(如圖十三)，並在 2006 年 10 月開始部署到陸軍部隊使用，而後廣泛用於伊拉克及阿富汗的作戰任務中。HIIDE 是一套手持式戰術裝置，可採集受測者的指紋、虹膜及臉部圖像與內建生物辨識資料庫進行匹配，是生物辨識自動化工具運用的延伸，可透過乙太網路連線(Ethernet)或連接 USB 隨身碟將其創建的新資料檔案轉存至 BAT 系統中，亦可從此系統下載最新觀察列表。

圖十三 手持式身分檢測設備諸元示意圖



資料來源：作者繪製。

圖十四 安全電子註冊套件諸元示意圖

資料來源：作者繪製。

(三)安全電子註冊套件(Secure Electronic Enrollment Kit, SEEK)

在軍事行動中，時間至關重要，尤其對特種作戰部隊而言。美國國防部希望在特種部隊人員抵達任務現場時，可以迅速檢索必要的資訊，並採取適切之行動，而安全電子註冊套件可提供特種部隊士兵迅速收集、比對和儲存生物特徵資料的設備。SEEK 是一款手持式生物辨識裝置(如圖十四)，可快速收集受測者指紋、臉部和虹膜圖像並與其內建生物辨識資料庫進行匹配，與 HIIDE 不同的是，SEEK 可以透過 3G 無線網

路(Wireless)或連接 USB，將所收集的生物特徵數據傳送到網路資料庫予以儲存。在 2011 年 5 月 1 日狙殺奧薩姆賓拉登行動中，美國特種作戰部隊突擊隊即是使用 SEEK 的臉部辨識功能，確認擊斃目標的身分為賓拉登並在幾秒鐘內將圖像回傳五角大廈。

以下針對前述生物辨識裝置功能及其運用範疇整理如表一，可看出美軍主要還是運用生物辨識裝置的指紋、虹膜及臉部辨識三大識別模式。而隨著科技進步，計算機及感測器之效能持續提升，而其組成元件體積卻更加縮小，未來或可結合智慧型穿戴裝置，使生物辨識裝置更有利於作戰任務之運用。

表一 美軍地面作戰和支援行動使用生物辨識裝置功能及用途比較表

裝備名稱	功能摘要	運用範圍
生物辨識自動化工具(BAT)	一、 指紋/虹膜辨識。 二、 可輸出臉部圖像識別證。 三、 固定式工作站。 四、 乙太網路連線。 五、 內建可擴充資料庫。 六、 具最新觀察列表。	一、 美軍於 2001 年在科索沃戰爭開始使用。 二、 基地進出防護。 三、 羈押人員身分查核。 七、 人口管理。 四、 簡易爆炸裝置採證。 五、 當地僱傭人員審查。
手持式身分檢測設備(HIIDE)	一、 指紋/臉部/虹膜辨識模式。 二、 手持式裝置。 三、 乙太網路連線。 四、 可連接 BAT 更新資料庫及觀察列表。	一、 美陸軍於 2006 年 10 月開始使用。 二、 支援特種部隊戰術行動。 三、 檢查哨人員查核。 四、 機動巡邏任務。 五、 支援道路排雷小組巡檢。
安全電子註冊套件(SEEK)	一、 指紋/臉部/虹膜辨識模式。 二、 手持式裝置。 三、 乙太網路/3G 無線網路連線。 四、 可連接網路資料庫(FBI 及軍方) 。	一、 美軍特種部隊於 2010 年開始使用。 二、 支援特種部隊戰術行動。 三、 檢查哨人員查核。 四、 機動巡邏任務。 五、 支援道路排雷小組偵檢。

資料來源：作者繪製。

二、支援攻勢作戰

美軍在攻勢作戰中使用生物辨識技術的主要用途在於識別特定的敵人及其支援人員，以有效遂行戰鬥行動，其應用從指定目標的作戰，如斬首行動、俘虜作戰，到全面管控作戰區域內人員的行動皆可適用。應用生物辨識技術可幫助美軍將有限的作戰資源集中，以發揮最大效能，同時可避免不必要的負面後果。舉例來說，美軍一旦錯殺或俘虜錯誤的對象，不僅浪費軍隊作戰資源，而且也會使當地民眾與軍隊更加疏遠，這種疏離感可能會導致許多負面反應，造成當地人員情報匱乏及遭受暴力報復的

惡性循環。

(一)建立具有生物辨識能力的檢查站

美軍在作戰區建立檢查站(Checkpoints, CPs)作為支援持續作戰或未來作戰的重要工具，在 CPs 內配置一套生物辨識特徵收集系統，其中內含最新的生物特徵觀察列表(敵特定目標)，使其具有分辨敵人或尋找敵人之能力，甚至可繪製出當地的人口分布狀況。使用生物學功能的戰場情報準備分析，可有助於找到 CPs 在整個作戰區的最佳位置，在時間和作戰情況允許狀況下，可以登記通過該地區的所有人員的身分或至少如役齡男性的身分，並將重要的資訊提供情報作業使用。美軍在執行特定目標的俘虜/獵殺行動時，會將特定地點(通常是一個小鎮或村莊)予以隔離進而實施搜索，此時會將 CPs 的戰術位置納入作戰規劃，管制可能試圖以步行或乘車逃離目標區域的「遺漏者」或其同夥。而此類任務指派給配備生物辨識能力的 CPs，則可以確保特定目標不至於逃跑，發揮其最大管制效能，尤其在生物辨識裝置無法全面配發給整個任務部隊時，這種規劃方式將特別有用。

具有生物辨識能力的 CPs 可有效控制威脅份子的移動，精準提供具威脅對象或組織的資訊，進一步支援未來攻勢作戰。舉例來說，美軍會沿著主要道路到過境點建立一系列具生物特徵能力的 CPs，經過長時間的部署，迫使叛亂份子或特定目標轉移，或集中到另一個地區，並使用生物辨識系統對該區域內的所有人口完成認證及登記，此時美軍作戰部隊可更有效、精準的與目標交戰，獲得較大勝利公算。

(二)生物辨識運用於人口管理

控制或管理當地人口的行動，並切斷叛亂份子與當地支持叛亂行動民眾的連繫，對於後續作戰而言是相當重要的。美軍先前在越戰中採取的策略是將當地民眾遷移到受美軍軍隊保護的村莊，藉以隔離叛亂份子，雖然這項策略是有效的，但花費昂貴而且導致被迫撤離家園民眾的嚴重不滿。爰此，美軍在伊拉克戰爭中，透過運用屏障、檢查站和全面登記當地居民的個人資料(包含註冊生物辨識特徵)等手段，將城鎮或村落人群內的叛亂份子隔離出來。

美軍於 2004 年底執行費盧杰市第二次叛亂份子掃蕩運動後，即有效地運用這項戰術。先將平民暫時撤離安置，並在戰鬥行動中成功地消滅了當地的叛亂份子，在允許民眾回到費盧杰市之前，美軍針對所有役齡男性都實施生物辨識特徵註冊、登錄並發給身分證，而後在城市周邊設置一系列的屏障，僅開放幾個由兵力警戒的檢查站提供民眾進出。一般民眾在進出城市時，可使用這些身分證件和生物辨識特徵資訊來驗證身分，美軍在巡邏城市時亦可實施隨機抽查，這些作為可以防止叛亂份子重新滲入城市，並有效地終結叛亂份子利用費盧杰市作為對巴格達和安巴爾省進行攻擊跳板的企圖。

三、支援守勢作戰

生物辨識技術在支援守勢作戰之應用更加廣泛，從提供基地防護及進出控制的安全性、支援人員審查、檢測內部威脅及部隊戰力的保護皆然，以下分別說明。

(一)生物辨識運用於基地防護

對於任何軍隊而言，基地整體安全防護和人員進出管控是非常重要的，尤其是當部隊位處在可能遭受攻擊或其他威脅的環境中時。美軍在伊拉克的作戰基地使用一套生物辨識進出管制系統(Biometrics Identification System for Access, BISA)(如圖十五)，BISA 是特別為軍隊部署基地開發的一套生物辨識進出控制系統，用以作為「非美國人員」進出美軍基地的生物特徵審查、篩選及登記管制工具，BISA 也可以印製出一個具生物辨識功能的進出識別證，可提供給需要定期進出基地的人員快速查驗通關。

圖十五 在伊拉克使用的 BISA 基地進出管制系統

資料來源：William C. Buhrow, “Biometrics in Support of Military Operations : lessons from the battlefield,” CRC Press, 2015, p.48.

為了達到最佳效果，生物辨識進出管制系統必須與前線作戰部隊使用的生物辨識系統相互交換資料庫模板，如此在戰場採集的生物特徵數據即可用於支援進出管制系統。同理，進出管制系統獲得的生物特徵數據亦應同步提供作戰部隊，以協助他們識別在戰場遭遇到的不明人員身分；另外進出管制系統能夠與戰場部隊同步使用最新的「生物辨識觀察列表」也是非常重要的，因為這種進出管制必須提供最快及最可靠的方式，以便立即辨識和篩選出對軍隊和設施構成最大威脅的人員。

(二)生物辨識支援人員審查

美軍在伊拉克和阿富汗的作戰初次面臨到恐怖組織的威脅，所以將生物辨識技術納入人員聘用資格審查程序的一部分，俾確保部隊不會僱用、培訓、支付薪資給參與或支持叛亂或恐怖組織的人員，充分運用生物辨識技術保護作戰部隊及資源免於遭受敵破壞。美軍在進行持續作戰時，需要大量後勤、運輸和基礎服務方面的外部支援，

而需求會隨著作戰期程持續增加，這類支援不僅來自於美國及其盟國，也經常需向作戰地區的廠商或民眾採購以獲得資源或服務。如果在反叛亂作戰中，叛亂份子的成員和支持者可能就是同樣區域的人民，顯然這種對外部依賴的因素就是一項顯著的安全風險。

在每一次軍事行動中美軍都訂有全面的部隊保護計畫，其中包含審查與作戰部隊接觸的外國人員的程序，以了解在這批外國承包商或其他支援人員之中誰是朋友或敵人，但囿於阿富汗官方提供的資料庫或可靠的個人資訊很少，部隊在偏遠地區要確認一個人的真實身分是困難的。因此，美軍使用生物辨識技術的人員審查程序，就可以知道不明受測者的指紋或 DNA 是否曾經在 IED 爆炸攻擊現場或相關的材料上採獲，或者在擄獲的敵方文件或設備上發現，確認將要僱用的人員是否在當地有犯罪記錄，進而成功地將這個人與他「隱藏的過去」連繫起來。

(三)生物辨識有助檢測內部威脅

2011 到 2012 年，美國及聯盟盟友遭受他們信任並聘用的阿富汗人襲擊事件大幅增加。在許多案例中，大多數是屬於臨時起意的襲擊事件，而肇因為阿富汗人對一些輕微或不滿的個人問題感到惱怒(如古蘭經褻瀆事件)；少數的襲擊卻是當地國民為支持叛軍而採取的行動。因此，美軍使用生物辨識技術作為全面性檢測內部威脅的作業模式，以因應前述第二種類型的威脅，其中包括運用生物辨識初步審查與美軍部隊定期接觸的外國軍事人員，並由反情報人員使用各種技術手段持續監控可疑對象。

以美海軍陸戰隊在阿富汗訓練安全部隊為例，美軍使用生物辨識技術篩選當地受訓成員，將這些採集到的生物辨識特徵集與觀察列表名單人員匹配，以利檢測內部潛在威脅並即時採取適當行動，亦可納入生物辨識特徵資料庫作為未來作戰任務運用(如圖十六)。

綜上，茲將美軍作戰應用生物辨識技術綜整如表二。

圖十六 美軍使用手持式身分檢測設備採集阿富汗當地受訓學員生物辨識特徵

資料來源：Marine Corps Lessons Learned newsletter, Vol.9/Issue7, January 2013, p.7.

表二 生物辨識技術支援美軍作戰之應用

作戰類型	運用區分
攻勢作戰	一、建立作戰區檢查站(CPs) (一)斬首/俘虜行動。 (二)過濾作戰區敵特定目標。 (三)繪製作戰地區的人口分布狀況。 (四)限制威脅份子的移動。 二、運用於人口管理 (一)辨識作戰區具威脅人員身分。 (二)建立作戰區平民身分資料庫。 (三)阻絕叛亂份子滲透。
守勢作戰	一、基地安全防護 (一)外部工作人員身分申請及登記。 (二)人員進出基地安全檢查及管制。 (三)建立資料庫模板提供第一線作戰部隊運用。 二、支援人員審查 (一)聘用人員資格審查。 (二)後勤支援安全確認。 三、檢測內部威脅 (一)過濾內部潛伏叛亂份子。 (二)檢測外籍軍事訓練人員。

資料來源：作者繪製。

國軍應用芻議

縱觀美軍生物辨識技術在軍事應用的發展進程，歷經 10 餘年生物辨識有關組織的調整及擴編，結合美國政府各部門生物辨識技術研發及運用成果，使生物辨識技術進一步成為支援戰場各項作戰任務不可或缺之利器。而美軍在戰場所使用的生物辨識裝置，主要是來自商用市場採購之商規現貨或由國防部合約商提供的軍規產品，均非美軍自主研發的方案，此項策略之優點在於使用商用現貨可迅速籌獲並納入作戰任務運用。

依據我國國防部在 106 年 3 月 16 日發布「四年期國防總檢討」中提出「防衛固守、重層嚇阻」的最新軍事戰略指導，以「防衛固守」作為國軍戰略防禦主軸，而「重層嚇阻」從被動守勢轉為積極防禦。依前述戰略指導及策略，國軍可朝守勢作戰及資安防護面向發展生物辨識技術及相關應用，並參考美軍直接採用商用產品技術之策略，以減少自力研發時程，有效強化並提升軍事安全。以下茲針對我國軍可應用面向列舉幾點建議：

一、資訊系統認證

國軍現行的智慧型加解密隨身碟即已採用指紋辨識功能，部分營區機敏處所(如資

訊機房、專案辦公室)亦可見採用指紋辨識裝置確認進出人員身分。另國軍辦公室自動化系統亦已結合智慧卡 PIN 碼進行認證授權，未來僅需增加感測裝置(如指紋感測器)，即可使用生物特徵作為主要認證機制，除具有更佳便利性與安全性的優勢，用戶登入電腦後之使用歷程更具不可否認性，可作為資安事件稽核之利器。

二、機敏處所管制

考量建置成本，生物辨識系統適合設置在安全等級要求較高之處所，如各軍總部、機房、機敏辦公室、作戰中心、作戰指揮所等機敏處所，可作為人員管控或警監安全應用，落實嚴進嚴出之管制作為，大幅提高機敏處所門禁管制的安全性。

三、營區安全維護

隨著高解析度攝影機、紅外線攝影機、夜視鏡頭、熱顯像等各種不同硬體感測器技術性能的持續提升，透過前端監視系統拍攝到高品質的數位影像，再結合後端生物辨識技術，即可達到主動式的智慧監控功能。此功能對於腹地較大或衛哨人力不足之營區更為適用，例如在營區內重要處所，透過人臉辨識功能發現非屬單位人員，系統即可主動告警，爭取主動應急的時間，消弭因人員不足而可能產生的安全罅隙。

四、人員安全調查

保防部門針對合作廠商或新聘人員的安全背景調查作業，可考慮結合未來內政部推動換發的國民晶片身分證功能，透過系統交叉比對人員安全背景，可快速獲得相關資訊，有效預防及降低可能發生的人員危安因素。

五、醫務病歷管理

可透過國軍醫療體系建置生物特徵系統資料庫，平時整合國軍人員體檢、體測與醫療紀錄，落實個人健康管理；戰時可建置行動式身分辨識裝置，透過指紋、臉部、虹膜…或其他生物特徵，以快速有效辨識傷者身分、血型、病史…等紀錄，提升戰場救護效能。

結論

根據 Acuity Market Intelligence 機構的研究[9]，全球具備生物辨識能力的行動裝置(包含智慧型手機、穿戴式裝置與平板電腦)將從 2017 年的 19 億台成長至 2022 年的 55 億台，並預測到了 2019 年，智慧型手機將高達 100%具備生物辨識技術，預料生物辨識技術成長與應用範疇將更加普及與多元，也將更融入在人們日常生活周遭。而生物辨識技術蓬勃發展之主要原因即在於可作為身分認證的可靠工具，不論是智慧型手機或平板電腦上的商用處理器，都可在幾分之一秒內以非常高的精確度完成指紋、人臉

[9] 〈2022 年行動生物辨識市場規模可達 506 億美元〉，http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=13784，2017/9/30。

或虹膜辨識，提供使用者極佳的安全性及便利性，並有助應付日益增長的資訊安全威脅和金融詐騙。

生物辨識技術目前仍然面臨許多挑戰，例如系統資料庫的安全性、生物特徵可偽造性及隨時間老化問題亦待克服，用戶對於提交具隱私性之個人生物特徵接受度，以及建置系統投資成本較高等問題，亟待持續的研發改進現有技術，以開闢新的生物特徵識別應用範疇。本文概述了現有生物辨識技術架構、運作方式、分類及性能評估指標，並以生物辨識技術軍事應用為主軸，介紹美軍生物辨識技術之發展現況與實務應用，另提出國軍可參考運用之方向，期可供國軍未來發展相關技術與政策之參考。

參考文獻

一、 邱建華、馮敬、郭偉、周淑娟，《生物特徵識別》(北京：清華大學出版社，2016 年)。

二、 Department of Defense Directive(DoDD) 8521.01E DoD Biometrics, 2017.

三、 U.S. Government Accountability Office, “DOD Biometrics and Forensics: GAO-17-580 Progress Made in Establishing Long-term Deployable Capabilities, but Further Actions Are Needed,” GAO-17-580, 2017.

四、 U.S. Government Accountability Office, “Defense Biometrics:Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics,” GAO-12-442, 2012.

五、 Steve Mansfield-Devine, “Biometrics at War: The US Military's Need for Identification and Authentication,” Biometric Technology Today, no.5, 2012.

六、 Identity Dominance:The U.S. Military’s Biometric War in Afghanistan, https://publicintelligence.net/identity-dominance/.

參考文獻

李建鵬中校，中正理工學院電機系 87 年班、國防管理學院國管指參班 101 年班，曾任電子官、修護組長、通參官、科長、資參官、電戰官，現任國防大學國防管理學院國管中心中校教官。

周兆龍中校，中正理工學院資訊系 87 年班、國防大學理工學院電子工程研究所 93 年班碩士、國防大學理工學院國防科學研究所博士，曾任電腦硬體工程官、程式設計官、資訊參謀官、後勤參謀官，現任國防大學理工學院資工系助理教授。