單靠軟件加固易被入侵洩私隱

人臉識別APP安全成疑

專家：硬件系統更可靠

人臉識別技術已愈來愈多地應用於日常生活，然而這項技術是否成熟到足以讓人信賴？背後的技術運作原理和發展現狀又當如何？香港中文大學工程學院信息工程學系教授劉永昌接受《大公報》訪問時詳細解析當下該技術存在的不足，他直言，純粹靠軟件而沒有運用硬件的安全單元（Secure Element）保護的人臉識別應用程式（APP），其安保能力令人擔憂，應當引起高度關注。

劉永昌研究團隊在近年的一項研究中，通過撰寫應用程式，以自動化分析方法，掃描了18,000多個流動應用程式，發現當中有373個的原碼包含了有安全漏洞的人臉識別應用模組。劉永昌表示，所有使用了這些含安全漏洞的人臉識別應用模組的應用程式，都更易受到黑客攻擊，需要採取設置硬件等其他方法加固，「純粹靠軟件加固的方法仍有相當風險，並非一勞永逸。」

掃一掃有片睇

▲劉永昌教授表示，人臉識別應用程式易受黑客攻擊，故建議目前使用人臉識別的商戶應盡量用硬件類系統。 大公報記者何嘉駿攝

大公報記者 苑向芹（文） 李斯達（資料） 融媒組（視頻）

人臉識別系統的載體分為硬件和軟件兩大類，硬件系統即擁有單獨的設備，例如市民過海關出入境時的人臉識別系統；一些手機本身亦自帶人臉識別系統。而軟件系統則通常指手機應用程式內的人臉識別系統，例如某些銀行應用程式要求用戶登記人臉識別時，會在APP內彈出人臉識別的畫面。

專家指出，軟件系統與硬件系統由於運作模式不同，安全系數亦不相同。據劉永昌教授介紹，一些軟件系統是將人臉識別數據上傳到雲端，而雲端是聯網的，意味着黑客只要一旦攻擊雲端，雲端上所有持有數據的用戶都會受害；而硬件的人臉識別系統由於有自己的獨有系統去儲存生物數據，則較大程度能避免這種問題。

專家檢測18系統 11個存漏洞

在軟件人臉識別系統研究方面，劉永昌教授帶領的中大團隊，在去年深入分析檢測了市場上18個人臉識別服務供應商提供的流動應用模組，發現其中11個存在安全漏洞。這些安全漏洞大致可分為四類：一、黑客可以藉干擾應用模組的操作，令在活體測試階段提供給用戶的指定動作過於單一、簡單，容易預判；二、人臉識別的參數設置可以被黑客更改令其設置不當，影響系統判斷的準確率；三、傳送到雲端的用戶生物數據易被黑客篡改；四、在通過實體測試且影完相之後，系統一般會有一個電子簽證來認證其真實性，有的黑客會模擬一個沒有電子簽證的版本送到雲端，並且設法令到之後雲端在驗證該用戶時，選用無電子簽證的版本去進行校對。

劉永昌教授表示，其中第一點提到的活體測試，是建立人臉識別數據賬戶的第一階段。在這個階段，軟件系統需要通過活體檢測技術（liveness detection）來判斷用家是否真人，包括指定用家做特定的動作，例如眨眼、張嘴、搖頭等。上述指定動作皆為隨機指令，以防不法分子預錄視頻蒙混過關。在通過真人驗證後，系統會要求用戶拍照，或者錄製短視頻，以獲取用戶的生物數據，再上載到雲端處理，建立人臉識別賬戶。

近兩年深度偽造（deepfake）技術興起引發關注，劉教授指出，從目前的技術來看，深度偽造技術自然可以應付大多數的活體測試，惟這項技術成本過高，黑客往往極少選擇。「如果你話呃一單有幾千萬元，咁係抵啦，但係一般唔會有呢種情況。」

通過篡改參數可冒充當事人

劉永昌教授說，現時許多黑客通常會選擇從第二類漏洞切入，通過篡改參數這種低成本的方式去攻擊人臉識別系統，且這種攻擊方式通常會涉及所在雲端內的所有用戶，影響力和破壞力較深度偽造更大。

劉永昌教授解釋，篡改參數則會直接影響人臉識別的準繩度。準繩度分為兩種情況：一是非當事人去做人臉識別，系統判定這位非當事人為當事人，又稱「假陽性」狀態；另一種情況是當事人自己去做人臉識別，但由於和當時登記時的樣貌狀態有些許不同，人臉識別就判定不是本人，又稱「假陰性」狀態。

而從技術操作層面來講，軟件工程師在設計參數時需要找到一個平衡點，如若調節不好，例如將「假陽性」的發生概率調至很小，就意味着「假陰性」的發生概率會變高，反之亦然。而調節參數對於黑客而言還是很容易篡改的，所以黑客將參數調到發生「假陰性」的概率極低的時候，就意味着誰都可以通過人臉識別冒充當事人了。

團隊以一張照片通過活體測試

中大研究團隊在這項研究中扮演黑客破壞人臉識別系統的參數，結果憑藉一張特朗普的照片成功通過用戶活體測試，而用戶真實身份實為學生本人。可見相關系統風險之高，令人咋舌。

至於現在逐漸流行的健身中心使用人臉識別一事，是否也有上述相關的系統風險，劉永昌教授表示團隊尚未專門研究，不過如果健身中心用的是與手機應用程式相關的人臉識別系統，則安全系數同樣較低。故他建議目前使用人臉識別的商戶都盡量用硬件類的人臉識別系統。

使用人臉識別技術 五大常用場景

❶ 門禁系統

通過人臉識別記錄上班、下班的考勤，或確保進入授權區域的人員具有相應的權限，以替代傳統工卡、指紋的打卡模式。一些人臉識別系統也逐漸應用於私人住宅、健身房、會員場所等。

❷ 安全認證、身份核實

在需要嚴格身份認證的應用場景下，人臉識別技術被運用在提供遠程服務的手機應用(APP)，比如金融服務、電子支付、電信服務中，甚至有些航空公司將人臉識別技術應用在登機檢查中。

❸ 監控攝像設備

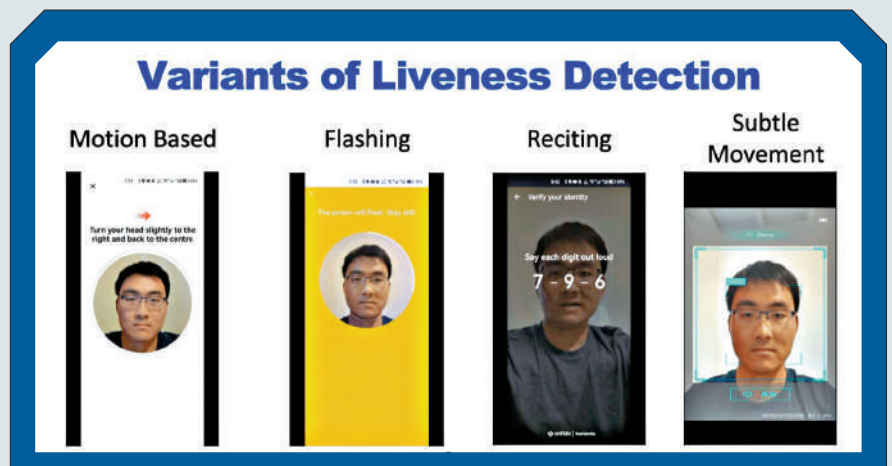
在一些公共區域的監控系統中，通過利用人臉識別技術，以識別進入特定區域的未授權人員。這類應用亦能幫助警方追捕嫌疑犯。

❹ 無人商店

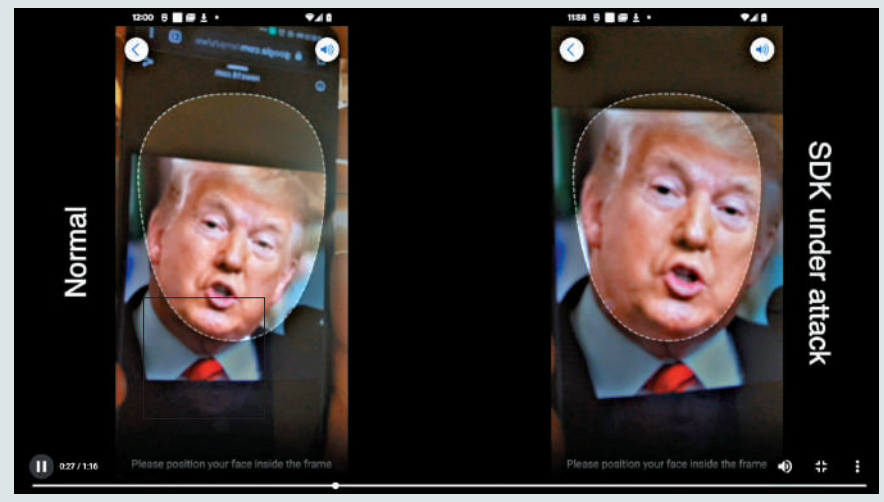
無人商店集上述多項應用於一體，既可以通過人臉識別賦予的嚴格身份認證功能保證商店貨物、購物環境的安全，還可以同時實現電子支付的功能。

❺ 消費者行爲分析

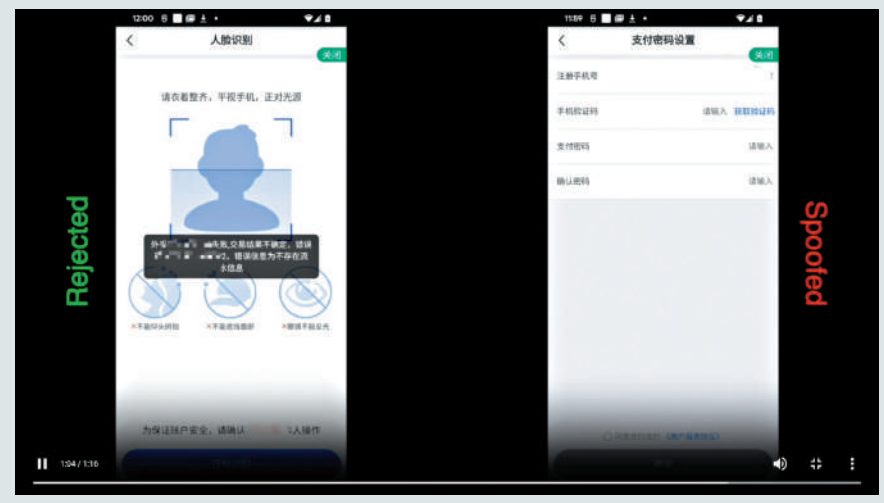
將人臉識別技術運用到產品和服務的應用中，比如駕駛座艙的設置，從而記錄用戶的產品或服務體驗、使用習慣和偏好設置。商家通過人臉識別系統獲取的多維度的數據，勾勒出數據主體的數據畫像、消費者偏好分布、熟客訪問率等，有助提升企業對用戶針對特定產品或服務體驗的認知，以進行大數據分析，從而達到調整門店布局、營銷策略、改進產品或服務的目的。



▲手機軟件應用程式在給用戶建立人臉識別數據之前，需要通過活體檢測技術來判斷用戶是否眞人，包括指定用戶做特定的動作，例如眨眼、搖頭、數字跟讀等。 受訪者供圖



▲▼中大研究團隊在一項人臉識別系統研究中，模擬黑客破壞系統的參數（見右圖，左圖為系統正常的對照組），結果團隊憑藉一張特朗普的照片成功通過用戶活體測試，而用戶眞實身份是一名學生。 受訪者供圖



技術待優化 方便安全難兼顧

仍須完善

人臉識別技術的發展和普及應用勢不可當，惟現階段技術仍有待完善，除了其安全性需要提升以外，該技術存在不便利、不公正等現象。這些弊端不但影響用家的體驗，亦令到這項技術在許多國家和地區都存在不同程度的法律爭議。

中大工程學院信息工程學系的劉永昌教授以身邊個案為例，指用戶在手機銀行APP驗證人臉識別時，系統會要求用戶做出眨眼、搖頭等動作，但經常因為網絡問題而驗證失敗，需要重複幾次相同的動作才能通過驗證。「啲接觸信號窒下窒下，搞咗成半個鐘都搞唔定。」因此，按照現在的技術，似乎網絡安全和便利有些衝突，「你想最簡單、方便，就最不安全；你想最安全，但有可能最不方便。」

有黑人被識別成「大猩猩」

除了不便利以外，人臉識別系統自帶的偏見性在愈來愈多的報道和研究中體現。據2019年美國NIST發布的一項研究報告顯示，在一些人臉識別算法中，亞裔和非裔美國人被誤認的可能性比白人高100倍。其中最荒謬的案例，則是一位黑人發現自己被谷歌的算法識別成「大猩猩」。此外，在篩選簡歷方面，這類有算法偏差的人臉識別系統被證明因為誤判而將更多的有色人種淘汰。

個人資料私隱專員鍾麗玲對大公報記者表示，誤判有色人種的人臉識別系統則與訓練該系統的數據庫有關，以美國該案例為例，其數據庫中獲得的白人數據更多，有色人種數據更少，而系統的學習自然是越多數據越能學習得準確。「因此人臉識別數據庫的準確性以及完整性都好緊要。」

大公報記者 苑向芹

話你知

硬件只作內部運算 避免加密金鑰被盜

現時在手機較常用在保護個人身份識別的硬件安全單元（Secure Element）的IC晶片，其內部就像是一部超小型的電腦，除了負責運算的微處理器及記憶體之外，並含有加速簽章及加解密運算的密碼運算副處理器。當用戶要進行簽章或加解密時，是將資料透過I/O界面送到IC晶片內部進行運算，而不必將加密金鑰讀出到外部進行運算，所以加密金鑰永遠不需外露，不會發生加密金鑰被盜取的狀況，因此可確保安全性，適合行動身份識別，保障個人私隱。

人臉識別違規投訴 今年飆逾倍

私隱爭議

生物認證技術，為人類帶來方便，但同時衍生私隱問題及爭議。個人資料私隱專員公署接獲的相關投訴，包括用於員工考勤打卡、屋苑的進出，部分公司接獲投訴後，雖然並無違規，但決定立即停用。

「世界幣」收集虹膜信息裁違例

私隱專員公署引述多宗個案，最轟動一宗投訴，虛擬貨幣Worldcoin（世界幣）的營運商，在香港設立六個營運點，以可以定期免費獲得虛擬貨幣「世界幣」，利誘市民交出面容掃描資料及虹膜影像，以製作虹膜編碼，多達8302人在自願提供相關生物認證資料，最終違反《私隱條例》，今年五月起停止採集資料。

另一宗投訴，涉及一間遊戲開發公司，使用人臉識別打卡機記錄員工考勤情況，經私隱專員公署介入後，有關公司讓員工可揀選使用人臉識別或拍卡系統記錄出勤情況，並向員工提供「收集個人資料聲明」以告知員工收集資料的目的。

此外，也有市民投訴一間物業管理公司，於屋苑的進出口採用人臉識別系統，私隱專員公署向有關物業管理公司發信，提醒有關公司關於《私隱條例》下，收集及使用面部圖像等生物辨識資料時的規定。

另外，有市民查詢部分銀行及儲值支付工具，透過手機應用程式進行人臉識別是否違例。公署今年截至七月底，合共接獲75宗人臉識別相關查詢，另有七宗相關投訴，不論查詢或投訴數字，也按年飆升逾倍，反映市民對於人臉識別等新科技的應用存有疑問，關注個人資料落入其他人的手中是否安全。

大公報記者 賴振雄