

防止「換臉」騙案 需建立AI法規體系

人工智能（AI）技術快速普及，騙徒利用AI換臉和擬聲技術行騙更加難防。本港目前雖然暫未收到正式報案，但警方沒有絲毫懈怠，日前已委任4名警務督察作為「防騙刑警」，分享相關罪案趨勢和防騙策略。不過，隨着AI換臉技術愈趨成熟，已有測試發現有不少作品是人類憑肉眼無法識別，因此，當局必須及早未雨綢繆，建立AI法規體系規範，以確保其用於合法用途。

據本港警方分析，AI換臉技術可應用在網戀騙案、電郵騙案、釣魚騙案及其他科技騙案。現階段，AI技術和數據

並不完善，被偽冒人物的眼神、口形出現不協調，臉部邊緣線不自然，手指動作變得模糊和遲滯等，市民若有懷疑，只要叫對方在視像中做出用手指橫過臉部的動作，便可看出破綻，判定這可能是一個假影像。

然而，科技發展一日千里，騙徒又擅長利用受害人心理，光靠掌握上述「破綻」並不足恃。事實上，AI換臉技術在幾年前還屬於需要高端設備的尖端技術，但現在卻已在全球普及，只需要普通筆記本電腦或智能手機就可以。在2022年國家網絡安全宣傳周網絡安全博

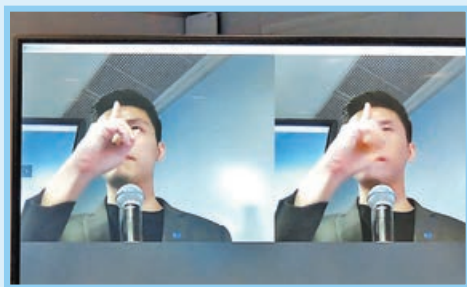
覽會上，職員現場演示只需數十秒便能合成連語音的換臉視頻，並指出大約30%經過AI換臉的照片和視頻，是人類僅憑肉眼無法識別的，帶來巨大安全隱患和法律問題。

雖然謹慎保護個人信息能在一定程度上避免自己成為受害人，但黑客和騙徒可以利用技術或騙術來控制受害者的電腦攝像頭，即時合成受害者面孔，讓他人上當。不久前，福建省便有科技公司老闆在10分鐘內被騙走430萬元人民幣，連有專業知識的科技人都上當，一般市民更加難防。而且最近也有不少

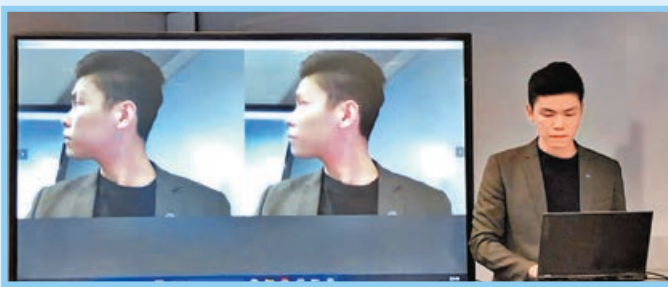
「楊冪」或「迪麗熱巴」等明星「直播帶貨」，亦是利用AI換臉和擬聲技術所為，讓人信以為真。

因此，如果沒有足夠的法律規範，只靠公眾自行識別只怕很快會力不從心。本港當務之急是立法確保個人隱私得到保護，防止未經授權的使用者將他人的臉部特徵用於換臉技術；同時需強制技術公司在推出換臉技術或軟件，以及所有使用者在生成任何AI換臉作品，必須明確標註相關信息。技術本身並沒有好壞，重要的是要有適合的法律和監管，來引導這項技術發展和使用。

預製「變臉」眼神口形不協調 要求做指定動作現破綻 AI偷聲盜面 警「一手」拆穿



■測試AI「變臉」可叫對方用手指橫過面前，如果右邊畫面出現模糊情況，便要小心。



■警方示範範AI「變臉」，當模擬頭像（右）打倒時會露出破綻，面部輪廓較為模糊。

網絡騙案防不勝防，有圖/有片有真相的日子恐成過去。AI人工智能「換臉」、「換聲」的「深偽技術」開始運用於詐騙，全球出現零星個案，香港今年亦收到兩宗涉及AI詐騙查詢。儘管因技術和成本等原因尚未成為詐騙主要類型，警方仍提醒市民應及早提高防範意識，建議遇上懷疑騙局時可叫對方在鏡頭前做指定動作來識破「真人假象」，同時提醒市民避免接聽陌生人的視像電話、保護好個人臉部、聲音等生物特徵信息，免被騙徒收集成數據用來「換臉」「換聲」造假行騙。

利用AI技術生成的deepfake（深度偽造技術），是透過人工智能作深度學習的方法，模擬特定對象的多角度面部特徵和聲音，製成高仿真的模擬影像，有海外個案顯示此技術已被騙徒利用來行騙（詳見另文）。

目前香港警方尚未接獲涉及AI詐騙案的舉報，但警方獲悉有兩宗涉及香港元素的個案查詢。今年5月一名日本男子在社交平台瀏覽到一名香港銀行CEO賬號，發現內有關於在香港投資的新聞報道片段，殊不知是騙徒以深偽技術製造新聞女主播推介投資項目及專訪CEO的報道。日漢信以為真，最終被騙購買1,570港元的點數卡，他其後致電涉事銀行尋找該名CEO，銀行指並無此人，男子和銀行都將事件通知日本警方，並得知騙徒是盜用了另一間銀行CEO的樣貌。

今年3月一名25歲香港男子在交友平台玩裸聊，被誘騙下載不知名手機程式，騙徒透過程式的視像功能盜取港男的樣貌

及手機電話簿，再以「深偽技術」將其頭像移花接木到色情影片，並向事主勒索1萬元。事主拒絕付款，但他只是通知警方，沒有正式報案，故香港警方暫未接到利用「深偽技術」實施詐騙的報案。

警委4督察組「防騙刑警」

警方網絡安全及科技罪案調查科首次委任4名警務督察作為「防騙刑警」，包括高級督察吳柏慧、高級督察陳智穎、高級督察張文瀚及督察梁珮筠，日前向本報等媒體講解和分析「深偽技術」騙局的趨勢。警方並演示利用AI「變臉」的手法，以數星期時間搜集及模擬到一名警司臉部資料，將其套用在另一人身上並作實時視像聊天，可是因數據不完善，畫面中被偽冒人物的眼神、口形出現不協調，臉部邊緣線不自然。

警方指，要特別留意手指在鏡頭擺動的動作，因數據不完整及電腦運算力不足，無法應對突然改變的畫面，令手指動

應對和預防AI詐騙貼士

- 在視像對話中要求對方在鏡頭前做指定動作。
- 向對方提問，測試對方身份真偽。
- 切勿輕易提供人臉、指紋、聲音等生物辨識信息。
- 若有「親友」在視頻或錄音中提出匯款要求，要特別警惕。
- 避免接聽陌生人的視像通話來電。
- 如懷疑文字或圖片被竄改，可試用搜尋器查找出處。
- 多從不同媒體查找資訊，以多角度查找真相。
- 在解讀「消息指」、「已Fact Check」等信息時應保持懷疑態度。
- 如懷疑是假資訊，應避免轉載並向有關機構查詢。
- 撥打防騙易18222熱線或使用防騙視伏器App，留意警方最新防騙消息。

資料來源：警務處

作變得模糊和遲滯，所以市民若有懷疑，只要叫對方在視像中做出用手指橫過臉部的動作，便可看出破綻，即可判定這可能是一個假影像。

警方指利用「深偽技術」作視像電話，其實都是騙取受害人信任度的一個行騙手段，整體套路與傳統手法大致相同。惟科技發展一日千里，市民必須時刻保持警惕，謹記「眼見不一定為實，有圖並不一定為真相。」

AI版尹光翻唱可亂真

AI科技日趨成熟和普及，由於「深偽技術」須收集大量被模擬對象的原始影像及語音數據，才能達至理想的偽造效果。故此騙徒絞盡腦汁打造幾可亂真的「犯案工具」犯案，一些經常曝光的公眾人物或明星首當其衝成為受害者，如在內地早前便有騙徒以AI變臉變聲的「深偽技術」，將直播間推銷員搖身變成「楊冪」、「楊穎」、「迪麗熱巴」等女星帶貨，推高銷量，有詐騙之嫌。

本港有「廟街歌王」之稱的男歌手尹光，近期亦被人以AI製造「翻唱」歌曲在YouTube頻道播放。尹光早前向傳媒表示，聽過由AI模仿自己聲音唱出林家謙、姜濤等的歌曲後，「覺得好笑，都唱得好似，不過與自己真人唱肯定有分別！」

至於在歐美等發達國家，近年涉及「深偽技術」的詐騙案不斷上升。今年5月，有網絡公司發布多國首季涉及「深偽技術」的詐騙案比例的統計數據顯示，與去年同期相比，美國已從0.2%上升到2.6%，加拿大則從0.1%飆升至4.6%。另在英國、德國、意大利等的「深偽技術」詐騙案所佔比例都超過了5%。

今年3月在加拿大，便有一對夫婦接獲騙徒利用AI模仿其兒子的聲音來電，被騙去2.1萬加元（約12萬港元）。據悉，騙徒是在電話上利用以AI合成其兒子的「聲線」致電該對夫婦，訛稱因駕車撞死一名美國外交官，現身處監獄，急需金錢支付律師費。數小時後，騙徒又再佯稱是其兒子的代表律師致電，聲稱開庭前需要2.1萬加元。



■警方加強向市民宣傳日新月異的詐騙手法及預防知識。