

認識 Deepfake 技術及其應用與風險

俗稱「AI 換臉」的 Deepfake 技術又稱為「深偽技術」，它是深度學習 (deep learning) 與偽造 (fake) 的混成字，意指一類利用深度學習技術進行逼真的人像影像合成的技術。Deepfake 技術之所以引起全世界如此重視的原因，在於它的相關軟體可以讓一般人輕鬆地取得，並且運作於一般的個人電腦或行動裝置上，因此各種相關的善意或惡意的應用方式層出不窮，迫使這個世界必須嚴肅看待 Deepfake 技術帶來的巨大衝擊。

一、什麼是 Deepfake 技術

說到 Deepfake 的「換臉」能耐，除了幾乎天衣無縫的效果，它還能夠做到各種角度和表情的換臉，並套用在照片、影片、甚至是即時的視訊聊天當中，它是如何做到的呢？

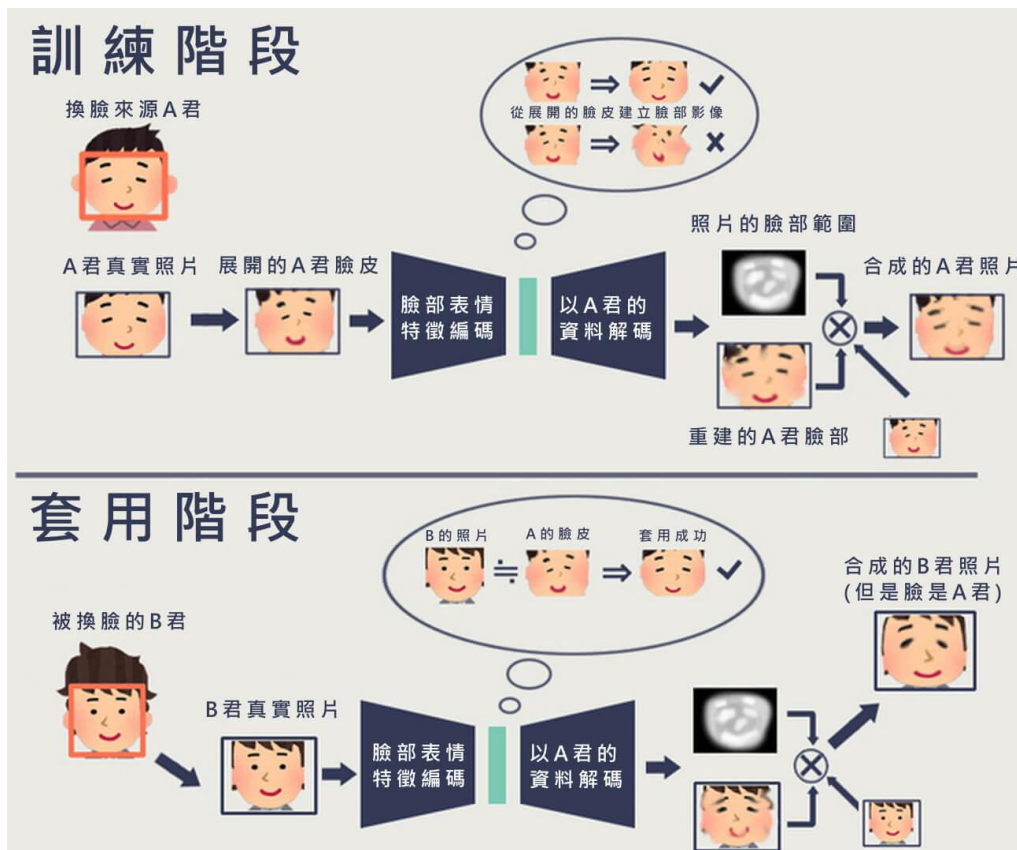


圖 1: Deepfake 技術基本流程 (譯自 Github 開源專案 [faceswap-GAN](#))

我們想使用 Deepfake 軟體將 A 君的臉移花接木到 B 君的照片上，首先要盡可能地提供 Deepfake 大量的 A 君真實照片或影片，讓軟體捕捉 A 君各種拍攝角度和神情的臉部影像。如圖 1 所示，使用了 Deepfake 技術的軟體在訓練階段，會把 A 君的真實照片

擷取臉部影像以後，展開為攤平的臉皮影像，接著對臉上的表情或特徵進行編碼，以便日後進行影像的重建與合成。在這個過程中，軟體 AI 會以機器學習技術不斷地嘗試基於擷取到的臉皮影像與編碼資料，試圖重建 A 君在各個角度下的臉部影像，並且和原來的真實照片比較，調整到最佳效果，這個過程就像是 AI 在「反覆練習與精進修圖技能」。

完成訓練階段之後，此時 AI 已經非常擅長描繪 A 君各種表情之下的臉部影像了，之後在套用階段，對於要被換臉的 B 君，同樣地從真實照片中擷取他的臉部表情與特徵並加以編碼，此時將這些編碼資料與 A 君的訓練資料加以匹配，以 A 君的資料進行解碼，於是就在 B 君的照片上畫出 A 君相同角度與表情的臉部影像，我們便獲得了品質優良的換臉照片。

Deepfake 技術不只能針對照片或影片進行換臉，如果運行在 GPU 規格稍微高一點的電腦上，也可以對即時視訊進行換臉，如圖 2 所示，這同樣也是一般人可以自由取得的軟體，再搭配使用語音模仿軟體，你完全可以在網路上冒充另外一個人，並與人進行視訊聊天。

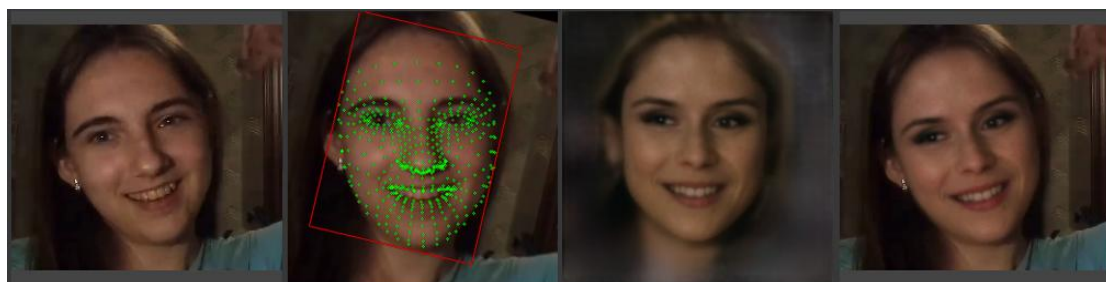


圖 2: 在即時視訊中進行 Deepfake 換臉（取自 Github 開源專案 [DeepFaceLive](#)）

Deepfake 這個字裡雖然有個 fake，但此技術並非沒有正面的用途，例如影視產業會用它來替換中途退出的演員，在藝術層面也能讓名人或古人做出一些趣味演出。無論如何，我們都必須認知到，網路世界已經徹底地進入了「眼見不為憑」的時代。

二、Deepfake 技術的善意與惡意應用

（一）Deepfake 技術的善意應用

1. **趣味演出**：在不侵害他人肖像權和智財權的前提下，將某些照片或影片換臉是很有趣的，甚至可以轉換影中人的性別，目前在各大 app 商店都可以下載到此類型的應用軟體。
2. **影視產業上的應用**：在戲劇或電影當中，當某些演員因為傷故而無法繼續演出

的時候，利用 Deepfake 技術可以讓他人頂替原本的演員完成演出，例如在電影《玩命關頭 7》的拍攝期間，男主角保羅沃克（Paul Walker）不幸意外離世，之後利用 Deepfake 技術由他的親弟弟頂替他完成電影演出。除此之外，當劇中角色必須橫跨年齡的時候，例如由年輕演到老，除了特殊化妝以外，Deepfake 技術也是一個可行的選項，例如勞勃狄尼洛（Robert Anthony De Niro）在《愛爾蘭人》中以此演出年輕的模樣。特別一提的是，由於影視產業對畫質的要求較高，在取得換臉對象的「臉皮」時，經常是特別製作角色的高精細度 3D 模型，而非從照片素材拼湊，然後以 Deepfake 技術去控制 3D 模型的表情再合成到影視作品中。

（二）Deepfake 技術的惡意應用

1. **復仇式色情：**社會上常見朋友或網友之間起爭執，憤而將對方的不雅影像公諸於世的報復手段，而 Deepfake 技術讓這種報復方式更加的氾濫。私密影像本是親密關係人之間才能取得的，然而 Deepfake 技術可以任意將他人的面貌換臉到其他的不雅影像上，進而達到羞辱他人的效果。將 Deepfake 技術應用於此可能會同時觸犯多項法律，包括侵害了肖像權、著作權、妨害名譽、散布猥褻物品罪，以及不實性影像罪等等，如果影像內容涉及未成年人，還會觸犯《兒童及少年性剝削防制條例》，後果非常的嚴重，切勿以身試法！
2. **冒充親友及網路交友詐騙：**現代人經常在網路上分享生活照片或影片，並且輕易地留下個資，由於 Deepfake 能夠讓人輕易地在網路上冒充他人進行視訊聊天，因此這些「分享族」就成了歹徒們冒充的對象。有時候是冒充孩子向親友詐財，有時候冒充公司主管欺騙員工盜用公款，有時候是冒充富商或名人鼓吹高風險投資，有時候是冒充網路上的帥哥美女進行交友詐騙，尤其是網紅或名人容易在網路上留下高解析度的特寫影音，更是歹徒們容易取得 Deepfake 訓練素材的對象。
3. **假訊息與假新聞：**除了騙財之外，規模更大、影響更鉅的是國際層級的 Deepfake 造假行為，試圖影響國際輿論或國內選舉。例如在俄烏戰爭期間，有烏克蘭總統呼籲軍民向俄羅斯投降的 Deepfake 影片，又如美國總統選舉期間，網路上有一些 Deepfake 製造的合照宣稱某些族群支持特定的候選人。我們身處在這個大 Deepfake 時代，要懂得對網路上所見的一切抱持懷疑態度並加以查證。

三、避開 Deepfake 相關的陷阱

如何避開網路上的 Deepfake 相關陷阱可以分成兩方面來談，其一是不被 Deepfake 生成物所騙，其二是避免讓自己成為 Deepfake 影片的主角。首先我們要認識 Deepfake 影片的常見破綻，盡可能地辨識眼前所見是否為 Deepfake 產物。

（一）Deepfake 影片的常見破綻

這裡列出一些常見的 Deepfake 影片破綻，你在網路上看到的影片或即時視訊如果有以下現象，可以高度懷疑它已經過 Deepfake 技術變造，但是影片如果沒有這些破綻，也不能保證就一定不是 Deepfake 產物。

1. **臉部影像模糊或打光怪異：**如果用來訓練 Deepfake 軟體的照片或影像素材的臉部解析度並不高，即使成功地合成在他人臉上，也是模糊的，有此情況幾乎可以確定該影片經過變造。
2. **臉部邊緣或側臉有破碎或不自然接縫：**由於網路上的生活照片大多是採取正面或稍微側臉的拍攝角度，因此以網路照片為素材為基礎的 Deepfake 影片，容易在完全側面時產生破綻。
3. **有細長形物體，例如手指、筆、筷子在臉前變成透明：**因為 Deepfake 軟體在合成影像的時候，乃是將臉部影像覆寫在他人的臉上，因此如果原本的臉部前有一些細長的物體在，可能被覆蓋而呈現半透明狀態。
4. **兩眼無神或非往頭部方向聚焦：**眼睛是原本素材照片的一部分，無法隨著影片中人的行為而改變方向，這是非常關鍵的破綻。
5. **聲音和口形對不上：**在即時視訊中使用 Deepfake 軟體造假的時候，可能因為裝置的 GPU 運算能力跟不上，而造成畫面的延遲。



圖 3：側面與臉前物體的 Deepfake 破綻（取自法務部[識詐宣傳](#)影片）

如果在網路上與人透過視訊聊天，可要求對方讓你看側臉，或是拿個細長物體在臉

前揮舞，以檢驗對方的面貌並非 Deepfake 變造。但是以上的破綻並非是絕對的，如果訓練素材品質足夠優良，例如擷取自網紅的特寫照片或影片，製作 Deepfake 影片時的軟硬體足夠先進，可能不會出現上述的破綻。例如圖 4 的即時視訊，便幾乎沒有以上的破綻。



圖 4: 使用 DeepFaceLive 軟體進行即時視訊（取自 [Geek on X](#) 影片）

在尋找 Deepfake 影片的破綻之外，如果視訊的對象是親友或家人，建議可以在事前約定「通關密語」，對方如果能夠正確回答，才能夠確信眼前人並非他人以 Deepfake 技術假冒的，又或者可另以其他方式聯繫求證，例如打一通普通電話，確定接起電話的人就是眼前的這個人。

（二）避免自己的資料被人作為 Deepfake 素材

要避免自己變成他人 Deepfake 影片中的主角，最重要的就是避免流出自己的臉部照片和聲音，所以透過網路分享日常的時候，請切記慎選分享對象，避免對陌生網友公開。除此之外，為了竊得大眾的個資和影音素材，歹徒會發布一些特殊的「打工機會」，例如網路面試或是一些錄製有聲書的工作，也請提高警覺，才能有效防範遭到濫用或詐騙，守護自身隱私與安全，避免成為受害者。

四、參考資料

1. ETtoday 新聞雲. (2022, March 17). 烏克蘭總統喊話「國民快投降」瘋傳！澤倫斯基 67 秒演說竟是 AI 換臉. ETtoday 新聞雲. <https://www.ettoday.net/news/20220317/2210494.htm>
2. Geek. (2024, April 23). DeepFaceLive [Tweet]. X (formerly Twitter).

- <https://x.com/geekbb/status/1782724379237081498>
3. Iperov. (n.d.) . DeepFaceLive [Computer software]. GitHub.
<https://github.com/iperov/DeepFaceLive>
 4. Shao, A. (n.d.) . faceswap-GAN [Computer software]. GitHub.
<https://github.com/shaoanlu/faceswap-GAN>
 5. Yahoo 新聞. (2024, January 5) . 騙徒 Deepfake 變女性面孔誘受害人投資虛擬貨幣涉 3400 萬 31 人落網. Yahoo 新聞. <https://reurl.cc/4N7vVv>
 6. 中華民國法務部. (2023, September 28) . 【識詐宣導】詐騙集團如何使用深偽技術 (Deepfake) 變臉 ? 調查官教您破解騙術 [Video]. YouTube.
https://youtu.be/pfyQC_Rk5Ao
 7. 公益資安平台. (n.d.) . AI 深偽技術：現實中的詐騙危機. 公益資安平台.
<https://www.npo.org.tw/npo165/OnePage.aspx?mid=2&id=22>
 8. 台灣事實查核中心. (2024, August 29) . 【謠言風向球】從迷因到助選 AI 生成影像攪動 2024 美國大選 . 台灣事實查核中心 . https://tfc-taiwan.org.tw/migration_article_105124_10963/
 9. 泛科學. (2022, January 25) . 濫用 Deepfake 製作換臉影片，有哪些法律責任？ 泛科學. <https://pansci.asia/archives/341284>
 10. 泛科學. (2022, January 24) . Deepfake 不一定是問題，不知道才是大問題！關於 Deepfake，你需要知道的是...？ 泛科學. <https://pansci.asia/archives/342421>