

【這是誰的臉？】延伸學習文章

- 教學對象：國小五至六年級
- 主題：網路識讀（深偽技術）

延伸閱讀：認識深偽技術，學會保護自己

你有用過手機的變臉濾鏡嗎？看著鏡頭前的自己一下子變老、一下子變成卡通人物，真的非常有趣！這些效果，其實都和一種叫做「深偽技術」（Deepfake）的技術有關。

深偽技術是利用 AI 來學習一個人的臉部特徵、表情動作，甚至連說話的聲音都能模仿。當 AI 學得夠多之後，就可以把這些特徵套用到影片或照片中，做出一段「看起來很像本人」的影像，讓旁人一時之間很難分辨真假。若能正向使用深偽技術，可以為社會帶來了許多有趣的可能。但是，這項技術如果被拿去做壞事，就會變成大麻煩！

🔍 深偽技術的正反面應用對照表：

💖 正向應用	⚠️ 負面風險
電影特效能讓演員變老、變年輕，或修正拍攝瑕疵。	製造虛假或不恰當影片，使他人受到誤會或名譽傷害。
讓歷史課本的人物「動起來」親自演戲，帶領學生重回現場。	資訊真假難辨，若未經查證可能誤導對事實的認知。
幫助失去聲音的患者，利用過去語音資料合成相近音色重新溝通。	詐騙集團假冒親友影像或聲音進行視訊借錢、求救。
提供有趣的變臉濾鏡增加生活娛樂。	個人正面照片、語音檔案可能被當作 AI 學習模仿的材料，被拿去冒用身分。

網路小偵探：識破假像的安全防禦術

面對這些真假難辨的影片，我們必須學習識破偽造的線索：

1. 找尋露餡的地方：觀看影片時，仔細觀察臉部與背景交界處（例如頭髮邊緣）是否有不自然的模糊或光影跳動，並觀察表情、眨眼是否顯得僵硬。可以參考公視 P# 新聞實驗室影片《10 分鐘用 AI 生成假影片 連專家都被騙倒 如何識別？》（網址：<https://www.youtube.com/watch?v=J56oMYQ2Heg>）的 05:28 至 05:56 秒處。影片實際展示了臉部配件不對稱、陰影怪異，以及手指在臉前揮動會產生模糊殘影或消失等技術漏洞。

2. 執行「二重驗證」：接到親友的求救或借錢電話時，不能因為有看到對方的臉或聽到聲音就深信不疑。掛斷電話後，不要撥打對方剛才提供的「新號碼」或點開他傳來的連結，而要改用其他聯繫的管道（例如家裡的電話）重新打給本人進行確認。
3. 約定「防詐密語」：和家人討論一個只有彼此知道的「防詐密語」，例如可以詢問「我們第一次出國是去哪裡？」或是「爸爸最喜歡吃食物是什麼？」如果對方支支吾吾或答錯，就能立刻識破這位「假親友」的真面目。

最後，我們要從源頭保護好自己，平時就應謹慎管理社群媒體的隱私設定，不隨意公開高品質的正面照片、自拍影片或長段語音檔案，因為這些資料都可能成為 AI 進行學習模仿的材料。最重要的一點是養成「存疑與舉報」的習慣，若發現自己或同學成為深偽內容的受害者，請立即儲存檔案保存證據，並勇敢向師長、學校求助，或撥打 110 報案，千萬不要因為恐懼而選擇隱瞞。

參考資料：

公視 P# 新聞實驗室（2024）。10 分鐘用 AI 生成假影片 連專家都被騙倒 如何識別？

<https://www.youtube.com/watch?v=J56oMYQ2Heg>

不知道才是大問題！關於 Deepfake，你需要知道的是……？<https://pansci.asia/archives/342421>

深偽偵測—在深偽內容（Deepfake）氾濫的時代，眼見仍為憑嗎？

https://www.sinica.edu.tw/news_content/557/2445