【2021 全國科學探究競賽-這樣教我就懂】

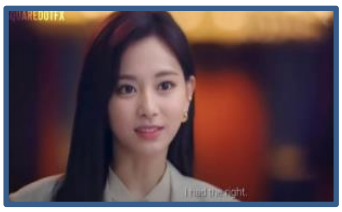
社會組 科學文章表單

文章題目：Deepfake 最深的深淵

文章內容：（限 500 字~1,500 字）

什麼？!臺灣女孩周子瑜出演韓國偶像劇女二，精湛演技讓人不不轉睛。

近期網路流傳一段周子瑜出演韓國某電視劇的影片，造成了粉絲間不小的轟動，劇中的子瑜與大咖演員同台飆戲卻絲毫不怯場，演技相當自然，任誰也沒想到這竟是網友利用合成技術 Deepfake，將子瑜的臉移至劇中女二姜漢娜的臉上，沒想到竟毫無違和，後也陸續出現子瑜出演古裝劇等其他戲劇的影片，網友震驚之餘，也紛紛期望這是真的，而 Deepfake 的議題也重新受到注意。(下圖為網友做的影片擷取片段，老實說並看不出來有任何違和感。)



Deepfake 問世 4 年，為何讓 AI 變網路犯罪工具？

Deepfake 一詞於 2017 年問世，隨著技術精進，讓 deepfake 門檻降低，只需要仿造對象的人物影音素材，就能製造出假影片。也延伸出一些可怕的犯罪問題，許多明星藝人被當作色情片的素材，影片的細緻度幾乎可以以假亂真，也造成了很大的風波，除了對當事者是種傷害之外，對於視聽者而言更是非常不利的假訊息，這些影片除了被用於色情產業，也有可能被當成政治操作或是製造假新聞帶輿論風向的利用工具。

Deepfake 的簡介

Deepfake，中文譯作「深假」或「深偽」，是一種透過人工智慧（AI）中的 deep learning（深度學習）技術所創造出的 fake（偽造）訊息。Deepfake 技術可以用於影像及聲音，只需要仿造對象的人物影音素材，就能製造出唯妙唯肖的假影片。

Deepfake 是怎麼製作的？

Deepfake 的生成有兩種方法。一個叫做自動編碼器（AutoEncoder），另一個叫做生成對

抗網路（Generative Adversarial Network, GAN），兩者都是 AI 深度學習的應用方式。

Deepfake 生成機制 1: 自動編碼器（AutoEncoder）

就是先將大量的人臉 A 以及人臉 B 的圖片匯入，使機器進行深度學習比對，到最後機器就能分辨異同，只要故意輸入錯誤的編碼，就能完美的將 A 的身體接上 B 的頭。

Deepfake 生成機制 2：生成對抗網路（GAN）

簡而言之就是用兩組模型不斷進行對抗，一個給錯的一個抓錯，如此一來兩者都能進步，生成更精準的圖片。

資訊爆炸時代如何自保？

現在 AI 技術日益精進，像 Deepfake 的 AI 絕對不會是唯一，Deepfake 的災情四起，尤其是現在社群媒體發達，像是公開的社群帳號很可能就會成為有心人士想要詐騙勒索的途徑之一，歹徒可能會竊取公開的照片及影片做成不雅的影片試圖散播，此時切勿落入歹徒陷阱，因謹慎思考後尋求社會資源的幫助。

參考資料

1.數位時代/**Deepfake 大解密！「換臉」技術更簡單，到底怎麼辦到的？/**
https://www.bnext.com.tw/article/57308/deepfake-autoencoder-gan
2.數位時代/ Deepfake 問世 3 年，為何讓 AI 變頭號網路犯罪公敵？/
https://www.bnext.com.tw/article/57260/deepfake-ai-deep-learning
3.數位時代
https://www.chinatimes.com/fashion/20201115001429-263903?chdtv