真人？假人？　從眼睛辨別真偽

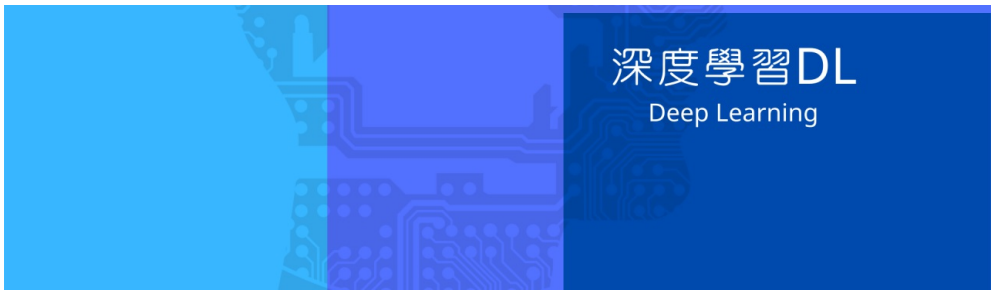
記者 蘇芳威 報導　　2021/04/18

科技迅速的進步和創新性突破，使辨別真假內容變得更加困難，當眼見不再為憑，我們應該相信甚麼？隨著人工智能（Artificial Intelligence，AI）技術的進步，有心人士能夠透過深偽（Deepfake）技術，將任何一個人的臉隨意換成另一個人的臉，並製作出一般人難以判別的假照片、假影片。這項技術能夠製造出大量的假人，甚至有網站每次刷新，便會生成一張不存在這個世界上的人的照片，如何分辨照片中、影片中的「人」是真是假，是項重要的議題。

深偽技術是什麼？

深偽是使用AI跟人體圖像合成的技術，將現有的圖片或影片，疊加在目標的圖片或影片上，製作出看起來以假亂真的造假圖片或影片，這種利用AI製作出來的假影片或假照片，一般人無法用肉眼輕易辨別出來。而深偽技術除了影像之外，也能製作出造假音檔。

要製作深偽影片，需要使用機器學習（Machine Learning，ML）中深度學習（Deep Learning，DL）的基礎——生成對抗網路（Generative Adversarial Network，GAN）。此項技術要使兩個AI同時工作，第一個AI稱為生成網路（Generative Network），負責掃描「被複製的本體」以及「對象」的照片，即時產生新的假影像；第二個AI稱為鑑別網路（Discriminating Network），負責審核第一個AI所產生影像的失誤率。若發現產生的影像「太假」，鑑別網路會告訴生成網路再重新製作另一個新影像，生成網路收到此訊息後會調整影像的細節，使影像通過鑑別網路的失誤率審核。兩個AI彼此相互對抗，以此不斷調整運算的細節及參數，直到生成網路產出的新影像通過鑑別網路所有的審核，最終產出深偽圖片或影片。



人工智慧涵蓋之技術示意圖。（圖片來源／蘇芳威重製）資料來源：HCAI

深偽技術　影視產業的雙面刃

深偽技術的出現對人類來說，是一個福音也是一個災難，若將深偽技術用於正當用途，它能讓過世的演員在電影中復活，讓年老的演員在電影中回春。2015年上映的電影《玩命關頭7》中的主角保羅沃克（Paul Walker），在電影拍攝完成前意外辭世，《玩命關頭7》的劇組便運用深偽技術讓保羅沃克在電影中「復活」。2019年上映的電影《愛爾蘭人》讓76歲的主角勞勃狄尼洛（Robert De Niro）透過深偽技術回春。從20幾歲的青年到60幾歲的老人，都由勞勃狄尼洛親自飾演。


意外過世的演員保羅沃克在《玩命關頭7》電影中出現。（圖片來源／Pinterest）

然而深偽技術卻大多被應用於成人影片上，根據荷蘭深偽檢測技術公司的報告指出，2019年識別出使用深偽技術的影片共有14678個，其中96%是成人影片，有心人士將女明星的臉換到成人影星的身體上，以滿足個人私慾。未經他人同意，便隨意利用他人的面容製作不雅影片在網路上散布，無疑讓受害女星的形象受到莫大傷害。據科技媒體MOTHERBOARD TECH BY VICE報導，2017年時電影《神力女超人》中女主角蓋兒加朵（Gal Gadot）的臉被有心人士利用，將她的臉置換到成人影片主角的臉，製作出假影片，同時該名有心人士也利用深偽技術製作出其他知名女星，如史嘉蕾喬韓森（Scarlett Johansson）、泰勒斯（Taylor Swift）、奧布瑞普拉扎（Aubrey Plaza）等的假影片。時至今日，隨著深偽技術的發展漸趨成熟，讓受害的知名女星、網紅也越來越多。由此可見深偽技術確實是把影視產業的雙面刃，用於正當用途可以創造許多奇蹟，造福閱聽人

的影視享受，但若用於不良用途，除了受害者的名譽被損害外，也破壞閱聽人對網路世界的信任。

主角有無靈魂　靈魂之窗判斷

因為深偽技術的進步，假影片越加的氾濫，如何判定影片內人物是有靈魂的真人抑或是無靈魂的假人？紐約州立大學水牛城分校（University at Buffalo）的研究人員胡署（Shu Hu）、李岳尊（Yuezun Li）、呂思偉（Siwei Lyu）於2021年發佈的一份研究指出，透過人類的靈魂之窗來辨認照片或影片中的人是真是假，其原理是運用演算法，透過眼角膜的反射來判定人像的真偽。這項演算法的準確率高達94%。

研究團隊提出基於生物與物理的GAN合成面孔檢測方法，該方法使用了兩隻合成眼睛之間，眼角膜鏡面高光（Specular highlight）的不一致。眼角膜鏡面高光，是捕捉眼角膜表面上的環境光或是反射物體的圖像。當被攝對象的眼睛直視相機，且周圍環境中的光源或反射距離被攝對象相對較遠時，兩隻眼睛會看到相同的場景，並且它們對應的角膜鏡面高光會顯示出來。研究團隊利用演算法，可以自動從兩眼比較眼角膜鏡面高光的相似性。

此項判定技術還有些限制性，該演算法僅比較像素差異，而不考慮幾何形狀和場景的不一致。當光源距離拍攝對象非常近或兩隻眼睛都看不到的外圍光源時，演算法可能會產生失誤，且該演算法不適用於不存在鏡面反射圖案的影像。

假影片氾濫　培養媒體識讀力

近年來，許多人利用深偽技術製作出一系列的假影片、假照片發佈到網路上，也就是說深偽技術有助長假資訊氾濫的可能性，而這也掀起了一場「造假」陣營與「打假」陣營的頂尖對決：造假陣營會盡可能地將深偽技術生成的圖像、影像以及聲音做到毫無破綻；而打假陣營也會竭盡所能的從看似毫無破綻的圖像、影像以及聲音找到破解方法。

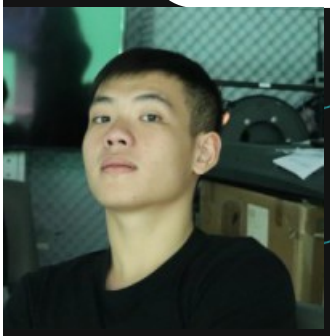
參與這樣的頂尖對決，對普羅大眾來說太過困難了，然而身處在假資訊氾濫的世代，如何分辨假資訊，培養媒體識讀力，是這個世代的人們都該面對的課題。

對於如何培養媒體識讀力，國際圖書館協會聯盟（International Federation of Library Associations and Institutions，IFLA）於2018年製作了一張圖表，教導一般民眾使用八個步驟辨別假新聞，分別為「考慮資訊來源」、「查核作者」、「檢查發佈日期」、「消除偏見」、「詳細閱讀」、「資訊來源」、「這是個笑話嗎？」、「向專家請教」。提高自身的媒體識讀力，在看見各種假資訊時，不再輕易受騙上當，甚至在看見深偽技術所製造出來的假照片、假影片時，用自己的眼睛判斷影片內的人是真人還是假人。

八個步驟辨別假新聞。（圖片來源／蘇芳威重製）資料來源：IFLA

關鍵字：深偽、AI、機器學習、GAN、演算法

縮圖來源：Pinterest



記者 蘇芳威

編輯 劉智誠