DEEPFAKE JAKO NOWA BROŃ W WALCE INFORMACYJNEJ

14.08.2018

Fałszywe wiadomości są obecnie nieodłącznym elementem środowiska informacyjnego. Miliardy danych udostępniane są w internecie poprzez serwisy społecznościowe, które w błyskawiczny sposób rozpowszechniają wszelkie informacje angażując przy tym odbiorców. Aby odróżnić to co fałszywe często polegamy na konkretnych dowodach, którymi są m.in. nagrania wideo. Uważamy, że to co widzimy i słyszymy musi być prawdziwe zwłaszcza jeżeli jest to przedstawiane przez innych uczestników środowiska informacyjnego.

Dzięki rewolucji technologicznej nawet filmy narażone są na przekłamanie. Wraz z zaawansowanymi metodami śledzenia twarzy i manipulacji wideo, nadchodzi nowa era dezinformacji.

Deep learning

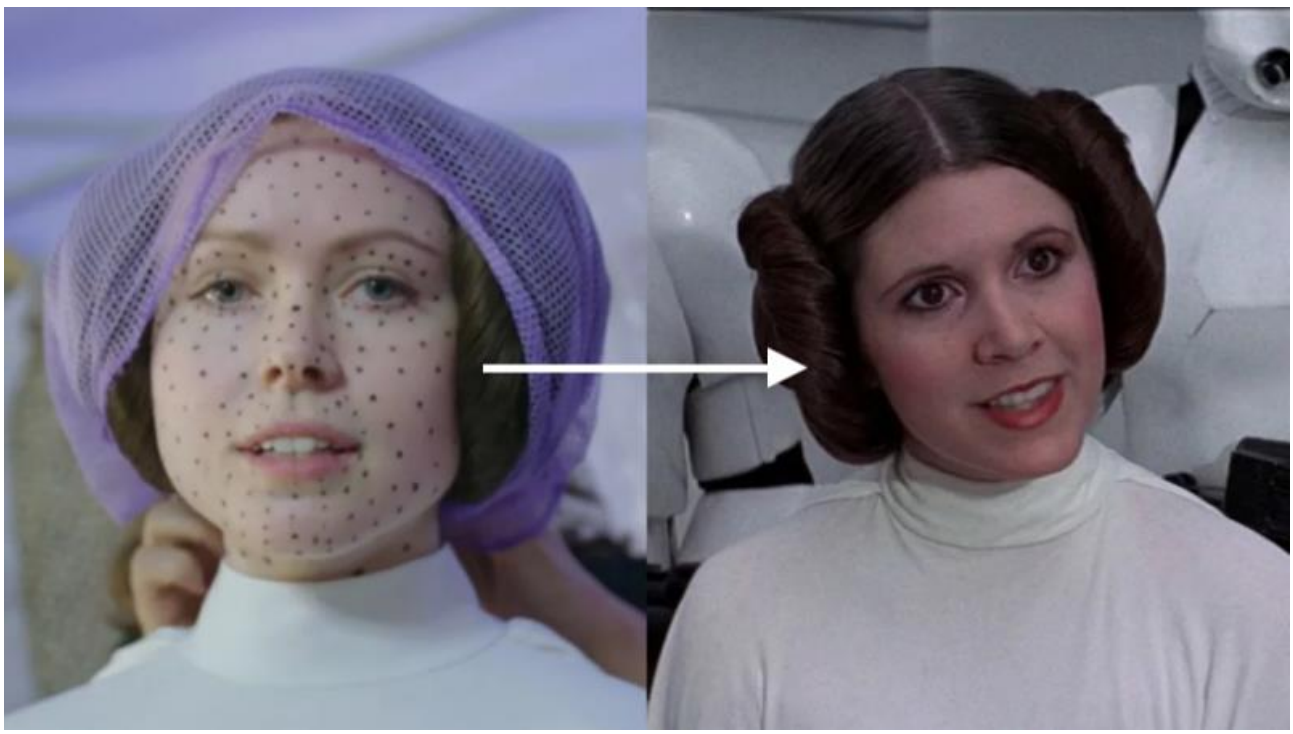
> DZIĘKI REWOLUCJI TECHNOLOGICZNEJ NAWET FILMY NARAŻONE SĄ NA PRZEKŁAMANIE. WRAZ Z ZAAWANSOWANYMI METODAMI ŚLEDZENIA TWARZY I MANIPULACJI WIDEO, NADCHODZI NOWA ERA

Deep learning to najnowsza sztuczna inteligencja. Jest on jednym z procesów uczenia maszynowego. Polega na stworzeniu jak największej liczby połączeń procesorów wykorzystujących do tego dostępne zbiory danych. Umożliwia to opracowanie tzw. sieci neuronowej (z ang. neural network). Wizualizując, taka sieć w dużym stopniu przypomina połączenia neuronów w ludzkim mózgu. W kontekście deep learningu jej celem jest **ulepszanie technik rozpoznawania głosu i mowy, przetwarzania naturalnego języka, wizji komputerowej i tworzenia prognoz.** Deep learning staje się jedną z najbardziej obiecujących technik w rozwoju nauk komputerowych, a także może mieć ogromny wpływ na naszą przyszłość.

Myśląc o konkretnej osobie wyobrażamy sobie jej twarz, specyficzne dla niej rysy, gesty i reakcje. Ludzka percepcja umożliwia nam rozpoznanie człowieka, jej płci, wieku, a także cech charakterystycznych dla danej osoby. Mamy również zdolność oceny, analizowania i odzwierciedlania wyrażanych przez innego człowieka emocji za pomocą neuronów lustrzanych. Jak się okazuje to samo jest teraz możliwe dzięki współczesnym algorytmom sztucznej inteligencji w tym deep learningu. W tej technologii to komputer gromadzi dane i przygotowuje podstawowe parametry. Rozpoczyna proces samodzielnego uczenia poprzez rozpoznawanie

wzorców. Ta technologia usprawniła działanie komputerów, a przede wszystkim zdolność rozumienia danych.

Rozpoznanie obrazu jest jednym z najistotniejszych elementów tej technologii. Tak samo jak człowiek potrafi zidentyfikować daną osobę. Zadaniem komputera jest wykrycie twarzy na obrazie, czy identyfikowanie jej z zestawem danych poprzez porównywanie i rozróżnianie. Proces analizy twarzy w obrazie kryje się pod pojęciem face mappingu. Głównym zadaniem tego procesu jest odnajdywanie kluczowych punktów na twarzy, które po połączeniu tworzą sieć, umożliwiając modyfikowanie jej ruchu.



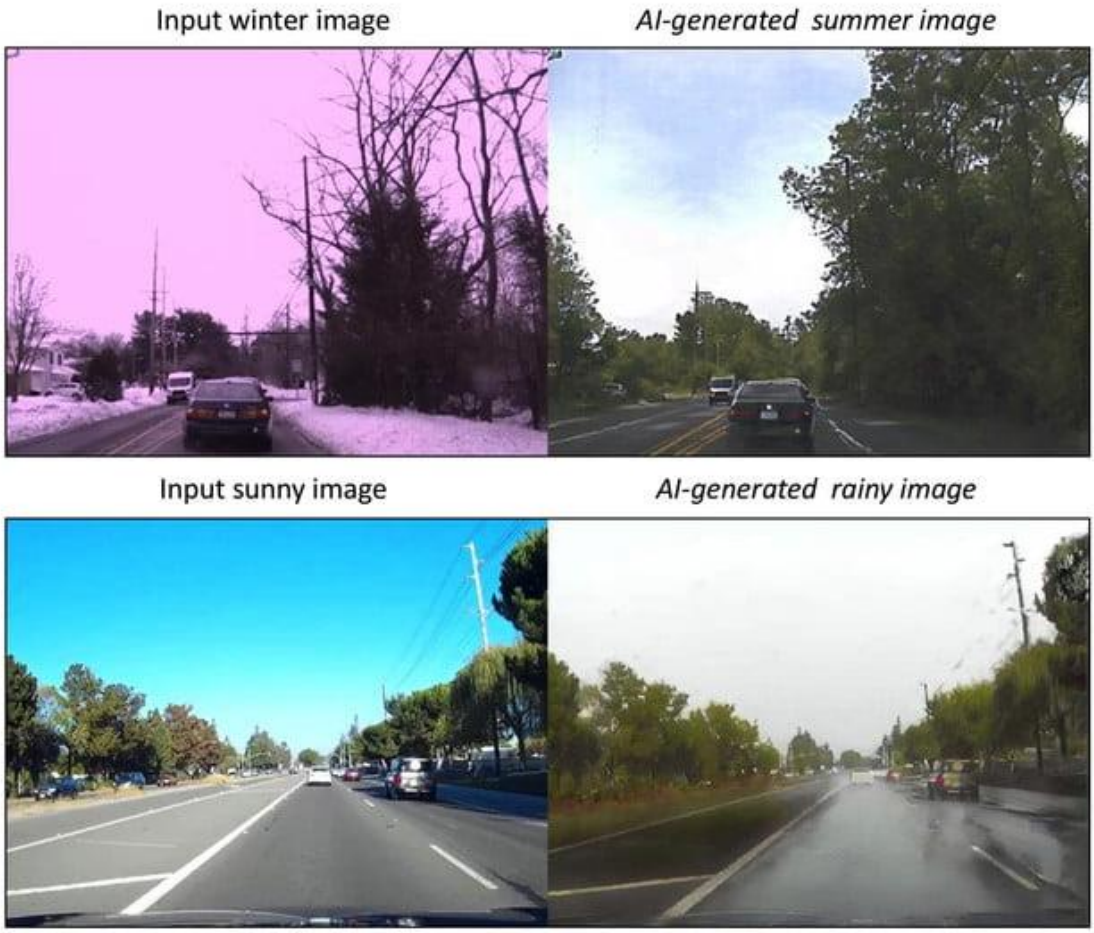
(Wykorzystanie technologii face mappingu w filmie Gwiezdne Wojny.
Źródło: https://hackernoon.com/exploring-deepfakes-20c9947c22d9)

Deepfake - nowa era walki informacyjnej

Deep learning wykorzystujący technologię face mappingu stał się szansą dla tych, których celem jest wpływanie na odbiorcę za pomocą fałszywej informacji.
W grudniu 2017 roku użytkownik o nazwie „DeepFake" opublikował na portalu Reddit filmy, na których pojawiły się sławne osoby. Przygotowany materiał jednak nie przedstawiał rzeczywistych filmów, lecz te wykonane za pomocą technologii deep learning, z którego wywodzi się deepfake. Polegają one na przygotowaniu z wykorzystaniem wszelkich dostępnych programów komputerowych bardzo realistycznych filmów, na których znajdują się osoby wypowiadające słowa, których nigdy nie użyły. Filmy są tworzone przez załadowanie złożonego zestawu instrukcji do komputera wraz z dużą ilością zdjęć i nagrań dźwiękowych. Następnie program

komputerowy uczy się kopiować wyrazy twarzy, mimikę, ruchy, głos i wzorce mowy. Wystarczająca liczba filmów i zapisów dźwiękowych danej osoby umożliwia systemowi stworzenie nagrania z tą osobą mówiącą cokolwiek tylko chcemy. Wachlarz możliwości jest szeroki, dostateczna ilość danych osoby A i osoby B sprawia, że możemy również wykonać wysokiej jakości face swap korzystając jedynie z odpowiedniego algorytmu.

Deep learning to obecnie bardzo szybko rozwijająca się technika. Przeprowadzone badania, oprócz wyżej opisanej modyfikacji głosu i obrazu umożliwiają także zmianę pory dnia i roku na filmie. Zmiana lata w zimę czy dnia w noc, jest możliwa poprzez wykorzystanie sieć neuronowej w celu uzyskania nienadzorowanego tłumaczenia obrazu na obraz. Oprócz przekształcenia twarzy, wypowiedzi możemy zaprezentować daną osobę w miejscu i scenerii, w której nigdy nie była. Przedstawienie danej sytuacji w innym czasie niż rzeczywisty nie będzie także stanowiło problemu.



(źródło: https://www.digitaltrends.com/cool-tech/nvidia-ai-winter-summer-car/)

Niestety ludzka pomysłowość nie ogranicza się do zastosowania technologii do osiągnięcia uczciwych celów.

Nowe metody umożliwiające adaptację na pewno znajdą swoje zastosowanie do wywoływania szerokiego spektrum szkód poprzez zdolność do produkowania podróbek. Dzięki połączeniom sieciowym systemów informacyjnych proces ten będzie się pogłębiać, zaburzając efekty procesu poznawczego człowieka. Zagrożenia, które niesie za sobą nowa era walki informacyjnej można podzielić ze względu na grupę odbiorców na dwie kategorie. Pierwsza grupa obejmuje osoby indywidualne i organizacje, a druga odnosi się do ogółu, czyli całego społeczeństwa.

Zagrożenia dla osób indywidualnych i organizacji

Wyzysk informacji jest stałym elementem walki informacyjnej. Nie zabraknie go również obecnie. Szczególnie, gdy pojawia się nowa możliwość uzyskania danych. Za pomocą głęboko sfałszowanej technologii kradzież tożsamości, czy wydobycie wartościowych informacji staje się łatwiejsza niż do tej pory. Obawiać się mogą wszyscy. Ofiary mogą być zmuszone do przekazania tajemnic handlowych, ważnych informacji o organizacji, dostarczenia pieniędzy, kompromitujących zdjęć czy filmów. Wszystko to, po to, aby zapobiec uwolnieniu się w sieci deepfake'a.

Technologia deepfake obecnie stosowana jest na masową skalę do tworzenia filmów pornograficznych. Coraz bardziej popularne staje się zamawianie takich filmów na forach. Przekazanie wystarczającej liczby nagrań i zdjęć, często skradzionych z Facebooka czy Instagrama umożliwiają wykonanie deepfake'ów. To wszystko podkreśla jak łatwo człowiek może stać się ofiarą technologii.

Oprócz zadawania bezpośredniej krzywdy psychicznej ofiarom, technologia deepfake znajdzie swoje zastosowanie w różnych innych wymiarach. Fałszywe filmy mogą być ukierunkowane na sabotaż. Wystarczy przygotować film, na którym ofiary niszczą własność bądź ją kradną, wypowiadają się w sposób godzący w instytucję. W rezultacie prowadzi to do utrudnienia prawidłowego działania instytucji firmy, jej dezorganizacji, a także może przynosić straty. Nawet jeśli ofierze uda się zdemaskować fałszywe nagranie to niemożliwe będzie cofnięcie wynikających z tego konsekwencji.

Wpływanie na społeczeństwo

Technologia deepfake nie ogranicza się jedynie do ataku na osoby indywidualne i organizacje. Może być skierowana przeciwko całemu społeczeństwu na wiele sposobów. Systematyczne wykorzystanie głębokich podróbek może wyrządzić długofalowe szkody dla całego państwa. Intencje wielu aktorów skupiać się będą na wykorzystaniu zdolności do fałszowania filmów, aby manipulować przekonaniami opinii publicznej. Powody mogą być różne. Dla jednych korzystna będzie nieuczciwa walka o idee, inni zrobią to z powodów państwowych. Znajdą się również Ci którzy potraktują takie działania jako intelektualny wandalizm. **Przytoczona strategia aktorów może doprowadzić do podważenia znaczenia demokratycznych rządów, instytucji państwowych, dyplomacji czy dziennikarstwa.**
Ukazanie osób ze środowiska polityki, urzędników, sędziów, dziennikarzy czy pracowników organizacji

wypowiadających się w sposób rasistowski, niezgodny z ideą demokratycznych rządów, ponadto przedstawienie takiej osoby wykonujące czynności nieetyczne może zachwiać ich autorytetem, a także wywołać niepokój wśród społeczeństwa. Można sobie wyobrazić jak łatwe stanie się przygotowanie wideo, na którym znajdą się przedstawiciele policji, agenci służb specjalnych czy żołnierze nadużywający swoich kompetencji. Zwłaszcza w środowisku gdzie już istnieje nieufność, prowokacyjne filmy znajdą swoją publiczność i będą trafiały do coraz szerszego grona odbiorców. Wiarygodność dziennikarstwa będzie stale poddawana ocenie.

(Deepfake z udziałem Baracka Obamy. Źródło: https://www.youtube.com/watch?v=cQ54GDm1eL0)

Deepfakes staną się idealną szansą dla tych, których celem jest manipulowanie wyborami. Ingerencja w proces decyzyjny człowieka w celu oddania głosu na danego kandydata w ostatnich latach staje się coraz bardziej intensywna. Nowa technologia sprawi, że proces decyzyjny może być sterowany poprzez fałszywe filmy przedstawiające kandydatów w taki sposób aby ofiara zmieniła swoje preferencje. Manipulacja za pomocą deepfake będzie wyjątkowo skuteczna biorąc pod uwagę walory filmowe, które poruszają wszystkie zmysły człowieka. Sprawia to, że nie możemy już dłużej ufać temu co widzimy i słyszymy w sieci Internet.

Obecnie generowanie takich filmików wykorzystywane jest głównie przeciwko osobom sławnym i do tworzenia humorystycznych nagrań. Wraz z upowszechnieniem się technologii, deepfake będą jednym z elementów kreowania środowiska informacyjnego. Już teraz opublikowane podróbki prezentujące Baracka Obame i Donalda

Trumpa są wyświetlane przez miliony użytkowników i wzbudzają ich aktywną reakcje. Różnorodne zaprzeczanie prawdy i tworzenie własnych wersji stanie się idealna szansą dla innych narodów, organizacji terrorystycznych czy prywatnych firm konkurujących na rynku.

—

Autor: Aleksandra Kopciuch

Fundacja Bezpieczna Cyberprzestrzeń

_____

Śledź na:
TT: @cybsecurity_org
Facebook: **@FundacjaBezpiecznaCyberprzestrzen**
@FundacjaBezpiecznaCyberprzestrzen