FOLIA 289

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 9(3) (2019)
ISSN 2657-8549
DOI 10.24917/26578549.9.3.9

Olga Wasiuta
ORCID ID 0000-0003-0481-1567
Uniwersytet Pedagogiczny w Krakowie

Sergiusz Wasiuta
ORCID ID 0000-0003-3402-963X
Uniwersytet Pedagogiczny w Krakowie

FakeApp jako nowe zagrożenie bezpieczeństwa politycznego i informacyjnego

Wprowadzenie

Wraz ze wzrostem liczby urządzeń mobilnych rośnie liczba aplikacji dostępnych dla ich użytkowników. Jednak, ponieważ cyberprzestępcy zawsze podążają tam, gdzie istnieje możliwość łatwego generowania zysków, skala ataków na urządzenia mobilne i ich użytkowników będzie stale rosnąć. Dlatego mamy do czynienia z coraz większą ilością zagrożeń mobilnych, w tym dotyczących złośliwego oprogramowania i fałszywych aplikacji, które często są bardzo popularne. Mogą one znaleźć się na witrynach internetowych, takich jak fora i pozornie niezależne tematycznie od samych aplikacji strony internetowe, chociaż niektóre pojawiają się również w oficjalnej aplikacji, na przykład Google Play. Są one dostępne do pobrania przez długi okres czasu, nie są wykrywane jako złośliwe oprogramowanie, dopóki nie zostaną uznawane za winne naruszenia praw autorskich. Rozprzestrzeniając fałszywe aplikacje, cyberprzestępcy często wykorzystują różne taktyki inżynierii społecznej, aby nakłonić użytkowników do pobrania fałszywek. Aplikacje są tym, co sprawia, że nasze smartfony są tak inteligentne.

Postęp w tej dziedzinie jest ogromny: w styczniu 2018 r. pojawił się program FakeApp – aplikacja komputerowa do bezpłatnego pobrania, która upraszcza produkcję fałszywych filmów, dzięki czemu technologia jest dostępna dla wszystkich: użytkownicy mogą sami produkować takie filmy w ciągu kilku godzin bez wiedzy programistycznej i na podstawie własnego materiału graficznego[32]. Ale chociaż termin ten przykuł uwagę świata w połączeniu z pornografią, pierwsze skomplikowane narzędzia do przechwytywania twarzy wykorzystywane do demonstracji technik zastosowanych przez FakeApp były początkowo stosowane do manipulowania postaciami politycznymi[33]. Choć Reddit ostatecznie zakazał wszelkich

32 *FakeApp*, https://www.malavida.com/en/soft/fakeapp/#gref [dostęp: 15.02.2019]

33 *Jordan Peele's simulated Obama PSA is a double-edged warning against fake news*, 18.04.2018, https://www.vox.com/2018/4/18/17252410/jordan-peele-obama-deepfake-buzzfeed; [dostęp: 15.02.2019]

fałszywych filmów generowanych przez deepfakes, mityczna „puszka Pandory" z fałszywą generacją rzeczywistości została otwarta.

Sztuczne podróbki

FakeApp za pomocą obliczeniowej karty graficznej jest w stanie stworzyć algorytm, który do dowolnego wideo wstawi twarz z przeanalizowanych zdjęć[34], pozwoli na zmianę twarzy, fryzury, płci, wieku i innych cech człowieka za pomocą smartphona. Ta aplikacja umożliwia użytkownikom łatwe manipulowanie wideoklipami, tworzenie i udostępnianie filmów wideo, w których zamieniono twarze. Aplikacja wykorzystuje sztuczną sieć neuronową i moc obliczeniową nowoczesnego procesora graficznego oraz trzy do czterech gigabajtów przestrzeni dyskowej do generowania fałszywego wideo[35]. Aby uzyskać szczegółowe informacje, program wymaga dużej ilości materiału wizualnego dotyczącej osoby, której twarz ma zostać wstawiona, aby dowiedzieć się, które aspekty obrazu należy wymienić, korzystając z wcześniej wspomnianego algorytmu głębokiego uczenia opartego na sekwencjach wideo i obrazach.

FakeApp może być określony jako **inteligentny program**, który wykorzystuje algorytmy sztucznej inteligencji, które najpierw „uczą się twarzy", by móc następnie przeprowadzić ich podmianę, czyli automatyczny Photoshop dla filmów. Do zastosowania tej metody potrzebne jest minimum 500 dobrej jakości zdjęć portretowych osoby, która ma być wprowadzona do filmu (bardzo dobre efekty można uzyskać mając 2000–3000 ujęć), na podstawie których aplikacja „uczy się" danej twarzy, a następnie samodzielnie ją podmienia. „Nowa" twarz zachowuje się tak jak oryginał[36]. Generowane przez internetową społeczność tą metodą montaże zostały nazwane „deepfakes" i na początku koncentrowały się na wstawianiu twarzy aktorek, piosenkarek i celebrytek w sceny z filmów przeznaczonych dla dorosłych[37]. Zostało to wykorzystane do stworzenia fałszywych, ale czasami bardzo przekonujących pornograficznych klipów kobiecych aktorek, takich jak Gal Gadot i innych. Nie brakowało także czysto humorystycznych krótkich filmów, na przykład takich, w których innym aktorom wstawiano twarz Nicolasa Cage'a. Nic dziwnego, że tego typu zmontowane krótkie produkcje zostały błyskawicznie rozpowszechnione przede wszystkim w portalach społecznościowych[38].

34 *FakeApp*…

35 M. Barni, L. Bondi, N. Bonettini, P. Bestagini, A. Costanzo, M. Maggini, B. Tondi, and S. Tubaro. *Aligned and nonaligned double jpeg detection using convolutional neural networks.* „Journal of Visual Communication and Image Representation" 2017, nr 49, p. 156.

36 R. Heartfield, G. Loukas, *Protection Against Semantic Social Engineering Attacks*. "Versatile Cybersecurity. Advances in Information Security", Edition: 72, Chapter: 4, Publisher: Springer, Cham, 2018, p. 99–140.

37 Ł. Kruczkowski, *FakeApp – czy powinniśmy obawiać się aplikacji, która z każdego może zrobić gwiazdę filmów dla dorosłych?,* 30.01.2018, https://www.onet.pl/?utm_source=technologie_viasg&utm_medium=nitro&utm_campaign=allonet_nitro_new&srcc=ucs&pid=554c238a-8523-51f1-8b35-dd5054acf3b9&sid=a6dee8f1-c258-4a9c-991e-af9040eb509b&utm_v=2 [dostęp: 19.02.2019]

38 D. Rivera et al., *Secure Communications and Protected Data for a Internet of Things Smart Toy Platform,* „IEEE Internet of Things Journal" 2019, p. 11.

Program FakeApp umożliwia zastępowanie w filmie twarzy jednej osoby twarzą innej, której zdjęcia wprowadzamy do programu. Program potrzebuje kilkaset takich fotografi, różnych ujęć prezentujących różne emocje. Po kilkugodzinnej pracy tworzy nowy film, w którym bohater – czy bohaterka – ma już nową twarz. Twarz, której mimika pochodzi od oryginalnej postaci i która wygląda na całkowicie autentyczną. Nie mamy tu zatem do czynienia z ordynarnym przymocowaniem głowy do tułowia. To raczej naciągnięcie nowej skóry na głowę[39].

Program korzysta z zasobów ogólnie dostępnych serwisów Google, które generują rezultaty o niesłychanej dotychczas jakości. Ponieważ produkcja taka wygląda znakomicie, fałszerze już od dawna nie ograniczają się do filmów z Obamą: gwiazdy Hollywood pojawiają się w filmach pornograficznych, w których nigdy nie zagrały. Fałszerze skopiowali twarze gwiazd z innych filmów w sposób nie do odróżnienia od oryginału i wstawili je do oryginalnego filmu. Na stronach internetowych znajdują się całe kolekcje takich klipów. Niektóre platformy, takie jak Reddit albo Twitter, z tego powodu zakazały już umieszczania takich treści[40].

Forum Deepfakes ma obecnie ponad 50 000 członków. Użytkownicy wysyłają prośby o filmy, dzielą się własnymi filmami i wymieniają zapisy celebrytów szkolących sztuczną inteligencję. Wyniki stają się bardziej wiarygodne każdego dnia. Nazwa „Deepfakes" stała się synonimem nowego rodzaju Fakens[41] (*Fakes Forge*)[42]. Oczywiście, to tylko kwestia czasu, zanim użytkownicy oprogramowania zamieszczą swoich znajomych, kolegów z klasy, pracy i znajomych z Facebooka w filmach pornograficznych zamiast gwiazd Hollywood.

Technologia, która stoi za tymi filmami, istnieje już od jakiegoś czasu, ale ogromną różnicą polega na tym, że dziś oprogramowanie takie jest dostępne wszędzie i jest łatwe w użyciu. Wystarczy pobrać program FakeApp i postępować zgodnie z instrukcją. FakeApp automatycznie generuje bardzo realistyczne transformacje twarzy na zdjęciach. Różne czasopisma komputerowe oferują je na swoich stronach. Na przykład Giga.de twierdzi, że dzięki tej aplikacji otrzymuje się możliwość wymiany twarzy w filmach. Redakcja podkreśla, że aplikacja jest przeznaczona wyłącznie do celów rozrywkowych: nikt nie powinien fałszować twarzy osób bez ich zgody i publikować efektów takiej pracy, ponieważ może to stanowić naruszenie dóbr osobistych i konsekwencji prawnych[43]. Dzięki takim aplikacjom rozpoczęła się nowa era memów, powstałych zgodnie z instrukcjami dotyczącymi FakeApp, ponieważ ich wyniki są niewiarygodnie realistyczne.

---

39 G. Lindenberg, *Głęboko fałszywa rzeczywistość. Jeśli nie wiadomo, co jest prawdą, to lepiej w nic nie wierzyć*, https://wiadomosci.onet.pl/tylko-w-onecie/deepfake-manipulacja-grozniejsza-niz-klasyczne-fake-newsy/c10cyzp [dostęp: 19.02.2019]

40 *FakeApp*…

41 T. Bezmalinovic, *Wenn Merkel plötzlich Trumps Gesicht trägt: die gefährliche Manipulation von Bildern und Videos*, 03.02.2018, https://www.aargauerzeitung.ch/leben/digital/wenn-merkel-ploetzlich-trumps-gesicht-traegt-die-gefaehrliche-manipulation-von-bildern-und-videos-132155720 [dostęp: 16.02.2019]

42 Fakes Forge – fejsbukowa inicjatywa kilku zapaleńców, graczy z krwi i kości, którzy postanowili raczyć świat najwyższej jakości fejkowymi grafikami.

43 P. Gensin, *Deepfakes: Auf dem Weg in eine alternative Realität?* 22.02.2018, http://faktenfinder.tagesschau.de/hintergrund/deep-fakes-101.html [dostęp: 16.02.2019]

Fala „zakazanych" scen z udziałem gwiazd kina, muzyki i celebrytek powstałych dzięki zastosowaniu zaawansowanej sztucznej inteligencji nie tylko pokazuje możliwości tej technologii, ale dowodzi, że każdy może z niej korzystać. W sieci coraz popularniejsza staje się aplikacja oparta na skrypcie, który powoli zbliża użytkowników do rzeczywistości, w której wszystko jest możliwe[44]. Sfabrykowanych materiałów z politykami nie rozpozna nikt, a wideo jako dowód sądowy przestanie mieć jakikolwiek sens.

Fałszerstwa pornograficzne

Niedawne postępy w sztucznej inteligencji wywołały nowe sposoby tworzenia fałszywych i zmanipulowanych filmów. Korzystając ze specjalnego oprogramowania, takiego jak Face2Face i Project Voco, naukowcy mogli zamienić zdjęcie śnieżnego krajobrazu na wiosnę, sfałszować mimikę twarzy i ruch warg, a nawet stworzyć oryginalną treść mówioną na podstawie głosów polityków. Istnieją przykłady, takie jak fałszywe nagranie prezydenta Obamy mówiącego o przepłacaniu pracowników, który wygląda i brzmi jak prawdziwa osoba[45].

Zdarzały się przypadki, w których młode dziewczyny popełniły samobójstwo z powodu opublikowania ich sfałszowanych obrazów i szantażu przy wykorzystaniu wykreowanych profili seksualnych. Wiele osób cechujących się szeroką obecnością w mediach społecznościowych lub tworzących i przesyłających wideo na YouTube, ułatwia gromadzenie danych, co stanowi zagrożenie dla nich i czyni je potencjalnym celem nękania, kampanii nienawiści i szantażu[46].

Odrębnym problemem pozostaje tworzenie i odbiór wirtualnej pornografii dziecięcej – albo z całkowicie wygenerowanymi komputerowo nastolatkami, z wygenerowanymi komputerowo twarzami na prawdziwych ciałach dorosłych albo nawet z prawdziwymi twarzami dorosłych ciał. Działania takie rodzą ważne pytania etyczne, a nowe przepisy będą konieczne, aby chronić ofiary i usunąć tę szarą strefę.

Programy sztucznej inteligencji

Najnowszym osiągnięciem twórców aplikacji jest program sztucznej inteligencji, który umożliwia poprawianie ruchów ust i mimiki aktorów w dubbingowanych filmach. Umożliwia on edycję wyrazu twarzy aktorów, aby dokładnie dopasować głosy dubbingowane, a także oszczędzić czas i zredukować koszty ponoszone przez przemysł filmowy. Może być również używany do korekty spojrzenia i pozycji

44 A. Dodge, L. House, E. Johnstone, *Using Fake Video Technology To Perpetrate Intimate Partner Abuse Domestic Violence Advisory Ridder*, Costa & Johnstone LLP1, https://withoutmyconsent.org/sites/default/files/blog_post/2018-04-25_deepfake_domestic_violence_advisory.pdf [dostęp: 20.02.2019].

45 P.A. Kopciak, *Fake Algorithms: Your face in my video. The influence of elaborate fake videos on our perception and socjety. History, theories and current developments in the media landscape, regarding aesthetics and socjety,* University of Applied Sciences St. Pölten Master course "Digital Mediatechnologies". Vienna, 2018, p. 8–9.

46 *What are deepfakes & why the future of porn is terrifying*, https://www.highsnobiety.com/p/ what-are-deepfakes-ai-porn/ [dostęp: 16.02.2019].

głowy w wideokonferencjach, a także umożliwia nowe możliwości postprodukcji wideo i efektów wizualnych. Technika została opracowana przez międzynarodowy zespół kierowany przez grupę z Instytutu Informatyki Maxa Plancka[47] i obejmującą naukowców z Uniwersytetu w Bath, Technicolor, TU Monachium i Uniwersytetu Stanforda. Program nazwany *Deep Video Portraits,* został zaprezentowany po raz pierwszy na konferencji SIGGRAPH 2018 w Vancouver 16 sierpnia 2018 roku[48].

W odróżnieniu od poprzednich metod, które koncentrują się wyłącznie na ruchach twarzy, program Deep Video może także animować całą twarz, w tym oczy, brwi i pozycję głowy w filmach, za pomocą elementów sterujących, znanych z animacji twarzyw w grafice komputerowej. Może także syntetyzować prawdopodobne statyczne tło wideo, jeśli głowa zostanie przesunięta.

Przedstawiciele Instytutu Informatyki Maxa Plancka podkreślają, że program działa przy zastosowaniu wychwytywania trójwymiarowego obrazu twarzy, aby w efekcie zarejestrować szczegółowe ruchy brwi, ust, nosa i pozycji głowy aktora dubbingującego w filmie. Następnie ruchy te są przenoszone elektronicznie na ruchy „docelowego" aktora, aby dokładnie zsynchronizować usta i ruchy twarzy z nowym dźwiękiem, uzyskując wysoki poziom realizmu[49]. Nowe możliwości programu da się stosować w innych aplikacjach, na przykład do zmiany w czasie rzeczywistym wyglądu osób w trakcie połączeń telekonferencyjnych, aby prezentowały się lepiej[50]. Oprogramowanie umożliwia także wiele nowych kreatywnych zastosowań w produkcji mediów wizualnych, ale autorzy zdają sobie również sprawę z możliwości niewłaściwego wykorzystania nowoczesnej technologii edycji wideo[51].

Oprócz tego w Dolinie Krzemowej[52] programiści pracują nad rekonstrukcją twarzy w wysokiej rozdzielczości, aby stworzyć trójwymiarowe awatary do wirtualnych światów. Ponadto naukowcy University of Erlangen-Nuremberg, wraz z partnerami Stanford University oraz Instytutu Informatyki Maxa Plancka opracowali technologię, która wykrywa mimikę i ruchy warg ludzkich i może być przeniesiona na obraz innego człowieka w czasie rzeczywistym[53]. W ten sposób można stworzyć wideo, w którym polityk swoim głosem, ruszając ustami w normalny dla siebie sposób, mówi rzeczy, których nigdy w rzeczywistości nie powiedział.

---

47 Instytut Informatyki im. Maxa Plancka (ang. Max Planck Institute for Computer Science, niem. Max-Planck-Institut für Informatik) to placówka naukowo-badawcza prowadząca badania z zakresu informatyki. Jej działalność poświęcona jest zarówno teoretycznym podstawom informatyki, jak również ich różnorodnym zastosowaniom. Instytut mieści się w Saarbrücken w Niemczech i należy do Towarzystwa Maxa Plancka – największej niemieckiej instytucji naukowej. Do najważniejszych zadań Instytutu należą: opracowywanie publikacji naukowych, tworzenie oprogramowania oraz kształcenie kolejnych pokoleń naukowców.

48 V. Just, *AI could make dodgy lip sync dubbing a thing of the past*, 17.08.2018, https://techxplore.com/news/2018-08-ai-dodgy-lip-sync-dubbing.html [dostęp: 15.02.2019].

49 Ibidem.

50 G.Lindenberg, *Głęboko fałszywa rzeczywistość*…

51 V. Just, *AI could make dodgy*...

52 Dolina Krzemowa to tereny stanu Kalifornia, które stanowią od lat 50. XX wieku centrum amerykańskiego przemysłu tzw. nowych technologii, głównie przemysłu komputerowego.

53 P. Gensin, *Deepfakes*…

Istnieją również programy sztucznej inteligencji, które umożliwiają samo edytowanie głosu. Program nie tworzy nowego głosu, działa tak jak edytor tekstu, w którym można dodawać i usuwać zdania i słowa. Musimy mieć nagrania oryginalnego głosu, którym program nauczy się mówić. Gdy program będzie potrafił posługiwać się czyimś głosem, wówczas wystarczy wpisać zdania, które mają zostać wypowiedziane danym głosem. Wygenerowane wypowiedzi są w zasadzie nie do odróżnienia od prawdziwych[54].

We wrześniu 2018 roku okazało się, że zespół informatyków z Wielkiej Brytanii oraz Indii stworzył nowy algorytm związany ze sztuczną inteligencją, który ma pomóc w rozpoznawaniu twarzy użytkowników nawet wtedy, kiedy zostanie ona częściowo zakryta[55].

Obecnie tworzenie fałszywego wizerunku przy użyciu aplikacji można uznać co najwyżej za naruszenie prywatności i danych, naruszenie praw autorskich, nękanie lub zniesławienie. Z uwagi na fakt, że większość szkód jest wyrządzana przez krążenie i dzielenie się materiałem multimedialnym, powstrzymywanie i zapobieganie temu procederowi, przy użyciu dzisiejszej technologii, jest prawie niemożliwe. Dokładne motywacje twórców i widzów są niejasne, trudne do weryfikacji pozostaje też, czy konsumenci mediów uczestniczą w tworzeniu popytu. W Europie prawo do prywatności rozwijane jest właśnie w odpowiedzi na zagrożenia płynące z internetu, czego przykładem jest RODO, w tym prawo do usunięcia z sieci niepochlebnych publikacji o danej osobie.

Ofiary FakeApp pozostają często zdegradowane i odhumanizowane, cierpią z powodu obrażeń psychicznych, straty reputacji, są ofiarami alternatywnej narracji, czemu nie mogą się sprzeciwić. Te nowe zastosowania technologii wywołają dyskusje i wszyscy – prawodawcy, badacze, widzowie – będą musieli współpracować, aby zapobiec nieetycznemu i krzywdzącemu wykorzystaniu zaawansowania technologicznego. W rzeczywistości „fake newsów" znacznie większe obawy budzi jednak możliwość tworzenia takich materiałów z udziałem ważnych osób świata polityki, biznesu czy sportu.

„Połączeniu twarzy Donalda Trumpa wklejonej w przemówienie Angeli Merkel trudno odmówić walorów humorystycznych, lecz nietrudno domyślić się, co ktoś pozbawiony poczucia humoru i zdeterminowany do osiągnięcia politycznego celu, mógłby potencjalnie zrobić, wykorzystując tę technologię"[56]. Jeden podstawiony gest, grymas, wypowiedziane zdanie, mogą w jednej chwili zmienić nastawienie opinii publicznej, a przy dzisiejszym tempie rozprzestrzeniania się fałszywych informacji w sieci – także i wpłynąć na relacje międzynarodowe.

---

54 G. Lindenberg, *Głęboko fałszywa rzeczywistość*…

55 A. Stopka, *Sztuczna inteligencja. Wielka nadzieja czy wielkie zagrożenie?* 13.09.2017, https://pl.aleteia.org/2017/09/13/sztuczna-inteligencja-wielka-nadzieja-czy-wielkie-zagrozenie/ [dostęp: 16.02.2019].

56 Ł. Kruczkowski, *FakeApp – czy powinniśmy obawiać się aplikacji, która z każdego może zrobić gwiazdę filmów dla dorosłych?* 30.01.2018, https://technologie.onet.pl/elektronika/fakeapp-czy-powinnismy-obawiac-sie-aplikacji-ktora-z-kazdego-moze-zrobic-gwiazde/jgk04vd [dostęp: 19.02.2019].

W chwili obecnej aplikacja FakeApp dostępna jest w wersji dla systemu operacyjnego Windows. Po jej pobraniu i zainstalowaniu potrzebne są także dostępne za darmo narzędzia deweloperskie, takie jak CUDA[57] firmy NVIDIA[58] i Visual C++ Microsoftu oraz FFmpeg[59].

Po zainstalowaniu oprogramowania następuje proces uczenia przez oprogramowanie twarzy, która ma zostać zastąpiona oraz tej należącej do przyszłej ofiary. Wymagane jest przygotowanie odpowiedniej liczby ujęć, przeprowadzenie ich dopasowania i „treningu" sztucznej inteligencji – to właśnie w tym momencie oprogramowanie uczy się detali wyglądu i mimiki charakterystycznych dla obu twarzy. Kolejny element to wyodrębnienie z filmu poszczególnych klatek i poddanie ich w aplikacji konwersji, po której film trzeba złożyć na nowo.

Sztuczna inteligencja potrafi m.in.: tworzyć trójwymiarowe modele twarzy ze zwykłych zdjęć, tworzyć oryginalne obrazy w odpowiedzi na żądanie (narysuj wulkan, ptaka, uliczkę), ocenić wartość estetyczną obrazu i go zmodyfikować, aby ją podnieść (oceny SI porównywano z tymi, wystawionymi przez ludzi), samodzielnie zmieniać źródło oświetlenia i cienie na zdjęciu, tworzyć podkład dźwiękowy na podstawie obrazu niemego filmu, zmieniać detale wyglądu osoby („pozbawienie włosów" Donalda Trumpa) podczas transmisji na żywo, sprawiać by znane osoby na twitterowych portretach uśmiechały się (*Smile Vector*)[60].

Najgroźniejszą konsekwencją rozpowszechnienia deepfake'ów stworzonych przy użyciu omawianego oprogramowania może stać się załamanie zaufania do całego systemu politycznego: jeśli nie wiadomo, co jest prawdą, to na wszelki wypadek lepiej w nic nie wierzyć – w żadne wypowiedzi, obietnice ani zaprzeczenia. Nie będzie powodu, żeby uznawać system demokratyczny za lepszy od innych, bo nie będzie wiary w realność tego, co o nim będzie można się dowiedzieć i jakich faktów obywatel będzie mógł być pewien[61].

Nietrudno sobie wyobrazić sytuację, w której z tej samej technologii korzysta ktoś, kto chce osiągnąć określony polityczny czy ekonomiczny cel albo którego dążeniem jest sprowokowanie agresji wymierzonej przeciwko konkretnej osobie lub grupie społecznej, wykorzystanie go do wywoływania politycznych napięć. Jedyną obroną przed wprowadzeniem w błąd jest zwiększanie świadomości odbiorców. Deepfake będące efektem FakeApp z każdym rokiem stają się coraz większym problemem, głównie dlatego, że algorytmy odpowiedzialne za tworzenie materiałów,

57 CUDA (ang. *Compute Unified Device Architecture*) – opracowana przez firmę Nvidia uniwersalna architektura procesorów wielordzeniowych umożliwiająca wykorzystanie ich mocy obliczeniowej do rozwiązywania ogólnych problemów numerycznych w sposób wydajniejszy niż w tradycyjnych, sekwencyjnych procesorach ogólnego zastosowania.

58 Nvidia Corporation – amerykańskie przedsiębiorstwo komputerowe będące jednym z największych na świecie producentów procesorów graficznych i innych układów scalonych przeznaczonych na rynek komputerowy. Założona została w 1993 roku. Główna siedziba firmy mieści się w Santa Clara, w stanie Kalifornia, w Stanach Zjednoczonych.

59 FFmpeg jest kompletnym pakietem elementów umożliwiających nagrywanie, konwertowanie i streaming audio i wideo. Warto dodać, że ten zbiór narzędzi umożliwia konwersję pomiędzy różnymi formatami wideo i jest całkowicie wolny i rozpowszechniany na licencji GPL.

60 P. A. Kopciak, *Fake Algorithms...,* p. 11.

61 G. Lindenberg, *Głęboko fałszywa rzeczywistość*...

w których zmieniona jest twarz bohaterów, stają się coraz bardziej kreatywne. Pojawiają się coraz lepsze narzędzia do ich wykrywania, ale jednocześnie sama podmiana twarzy działa coraz lepiej i znacznie trudniej jest dostrzec jakieś uchybienia, które wśród przeciętnych użytkowników wzbudziłyby jakiekolwiek podejrzenia.

Podsumowanie

W ciągu ostatnich dziesięcioleci popularyzacja smartfonów i rozwój sieci społecznościowych spowodowały powstanie wielu obrazów i filmów cyfrowych. Codziennie prawie dwa miliardy zdjęć pojawia się w internecie. Takie olbrzymie wykorzystanie cyfrowych obrazów nastąpiło w rezultacie pojawienia się nowych technologii. Dzisiaj powszechnie uznaje się niebezpieczeństwo fałszywych wiadomości, a rozprzestrzenianie się sfałszowanych wideo budzi coraz więcej obaw tym bardziej w kontekście, w którym ponad 100 milionów godzin treści wideo oglądanych jest każdego dnia na portalach społecznościowych, a cyfrowe wykrywanie fałszowania wideo nadal pozostaje trudnym zadaniem.

W ostatnich latach technologia przetwarzania obrazu (aparaty cyfrowe, telefony komórkowe itp.) stała się wszechobecna, umożliwiając ludziom na całym świecie otrzymywanie natychmiastowych zdjęć i filmów. Odzwierciedleniem tego wzrostu liczby obrazów cyfrowych jest zdolność nawet stosunkowo niewykwalifikowanych użytkowników do manipulowania i zniekształcania przekazu mediów wizualnych. Podczas gdy wiele manipulacji jest wykonywanych dla zabawy lub dla wartości artystycznej, inne służą celom takim, jak propaganda lub tworzenie kampanii dezinformacyjnych. Ta manipulacja multimediami wizualnymi jest możliwa dzięki szerokiej dostępności zaawansowanych aplikacji do edycji obrazu i wideo, a także zautomatyzowanych algorytmów manipulacji, które umożliwiają edycję w sposób bardzo trudny do wykrycia wizualnie lub za pomocą aktualnej analizy obrazu i narzędzi do analizy wizualnej mediów.

Liderzy państw demokratycznych doceniają obecnie wagę problemu, jaki niesie ze sobą możliwość tworzenia treści, w których generowane komputerowo obrazy znanych postaci życia publicznego wypowiadają bulwersujące twierdzenia i są nie do odróżnienia od prawdziwych osób. Materiały wideo tego rodzaju są potencjalnym zagrożeniem dla bezpieczeństwa wewnętrznego każdego państwa, a także mogą stać się narzędziem wpływu na wyniki wyborów. Kolejny sfabrykowany wideo skandal może zagrozić bezpieczeństwu narodowemu lub wpłynąć na opinię publiczną, co stanowi pole działania dla oszustów chcących ingerować np. w nastroje polityczne w społeczeństwie, a także staje się nową bronią w wojnie informacyjnej. Technologia ta będzie naturalnym narzędziem wykorzystywanym przez państwa celem manipulowania opinią publiczną i przeprowadzania kampanii dezinformujących, a także podkopywania wiary w obecnie istniejące instytucje. Z wyłaniającymi się i przerażająco zaawansowanymi metodami śledzenia twarzy i wideo manipulacji, nadchodzi zatem nowa era dezinformacji.

W czasach, w których publiczne zaufanie do mediów i polityki jest już zagrożone, możliwość, że wszystko, co oglądamy w internecie, może być przekonującą formą oszustwa wymyśloną przez jakąś osobę posiadającą nowoczesny komputer

osobisty, może jeszcze bardziej zagrozić wiarze w demokrację. Reasumując można metaforycznie stwierdzić, że niewykluczone, iż już jest za późno, żeby wepchnąć dżina z powrotem do butelki.

Bibliografia

Bailey J., *The deepest fake: how new tech will test our belief in what we see,* 04.05.2018, https://www.smh.com.au/technology/the-deepest-fake-how-new-tech-will-test-our-belief-in-what-we-see-20180423-p4zb4w.html [dostęp: 16.02.2019]

Barni M., Bondi L., Bonettini N., Bestagini P., Costanzo A., Maggini M., Tondi B., Tubaro S., *Aligned and nonaligned double jpeg detection using convolutional neural networks.* „Journal of Visual Communication and Image Representation" 2017, nr 49.

Bezmalinovic T., *Wenn Merkel plötzlich Trumps Gesicht trägt: die gefährliche Manipulation von Bildern und Videos*, 03.02.2018, https://www.aargauerzeitung.ch/leben/digital/wenn-merkel-ploetzlich-trumps-gesicht-traegt-die-gefaehrliche-manipulation-von-bildern-und-videos-132155720 [dostęp: 16.02.2019]

Chiny: Serwisy informacyjne poprowadzą prezenterzy wygenerowani komputerowo, 9.11.2018, https://www.cdaction.pl/news-55063/chiny-serwisy-informacyjne-poprowadza-prezenterzy-wygenerowani-komputerowo-wideo.html [dostęp: 20.02.2019]

Creating Breakthrough Technologies And Capabilitiesfor National Security, https://www.darpa.mil/ [dostęp: 16.02.2019]

Cyganek A., *Pomysłowość Chińczyków nie zna granic. Stworzyli prezentera za pośrednictwem DeepFake.* 09.11.2018, https://www.instalki.pl/aktualnosci/internet/33377-pomyslowosc-chinczykow-nie-zna-granic-stworzyli-prezentera-za-posrednictwem-deepfake.html; [dostęp: 20.02.2019]

Dodge A., House L., Johnstone E., *Using Fake Video Technology To Perpetrate Intimate Partner Abuse Domestic Violence Advisory Ridder*, Costa & Johnstone LLP1, https://withoutmyconsent.org/sites/default/files/blog_post/2018-04-25_deepfake_domestic_violence_advisory.pdf [dostęp: 20.02.2019]

Fake News: Read All About It, ed.The New York Times Editorial Staff. The Rosen Publishing Group, Inc, 2018, p. 34–35; *A Reddit User Starts 'Deepfake'*. 27.10.2017, https://www.eyerys.com/articles/timeline/reddit-user-starts-deepfake?page=8 [dostęp: 16.02.2019]

FakeApp, https://www.malavida.com/en/soft/fakeapp/#gref [dostęp: 15.02.2019]

Gensin P., Deepfakes: Auf dem Weg in eine alternative Realität? 22.02.2018, http://faktenfinder.tagesschau.de/hintergrund/deep-fakes-101.html [dostęp 16.02.2019]

Giles M., *Five emerging cyber-threats to worry about in 2019*. January 4, 2019, https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/ [dostęp: 15.02.2019]

Heartfield R., Loukas G., *Protection Against Semantic Social Engineering Attacks*, *Protection Against Semantic Social Engineering Attacks*. "Versatile Cybersecurity. Advances in Information Security", Edition: 72, Chapter: 4, Publisher: Springer, Cham, 2018, p. 99–140.

Jordan Peele's simulated Obama PSA is a double-edged warning against fake news, 18.04. 2018, https://www.vox.com/2018/4/18/17252410/jordan-peele-obama-deepfake-buzzfeed; [dostęp: 15.02.2019]

Just V., *AI could make dodgy lip sync dubbing a thing of the past,* 17.08.2018, https://techxplore.com/news/2018-08-ai-dodgy-lip-sync-dubbing.html [dostęp: 15.02.2019]

Kopciak P.A., *Fake Algorithms: Your face in my video. The influence of elaborate fake videos on our perception and socjety.* History, theories and current developments in the media landscape, regarding aesthetics and socjety. University of Applied Sciences St. Pölten Master course "Digital Mediatechnologies". Vienna, 2018.

Kruczkowski Ł., *FakeApp – czy powinniśmy obawiać się aplikacji, która z każdego może zrobić gwiazdę filmów dla dorosłych?* 30.01.2018, https://www.onet.pl/?utm_source=technologie_viasg&utm_medium=nitro&utm_campaign=allonet_nitro_new&srcc=ucs&pid=-554c238a-8523-51f1-8b35-dd5054acf3b9&sid=a6dee8f1-c258-4a9c-991e-af9040eb509b&utm_v=2 [dostęp: 19.02.2019]

Lindenberg G., *Głęboko fałszywa rzeczywistość. Jeśli nie wiadomo, co jest prawdą, to lepiej w nic nie wierzyć*, https://wiadomosci.onet.pl/tylko-w-onecie/deepfake-manipulacja-grozniejsza-niz-klasyczne-fake-newsy/c10cyzp [dostęp: 19.02.2019]

Rivera D. et al., *Secure Communications and Protected Data for a Internet of Things Smart Toy Platform,* „IEEE Internet of Things Journal" 2019.

Stopka A., *Sztuczna inteligencja. Wielka nadzieja czy wielkie zagrożenie*? 13.09.2017, https://pl.aleteia.org/2017/09/13/sztuczna-inteligencja-wielka-nadzieja-czy-wielkie-zagrozenie/ [dostęp: 16.02.2019]

Suwajanakorn S., Seitz S.M., Kemelmacher-Shlizerman I., *Synthesizing Obama: Learning Lip Sync from Audio.* ACM Transactions on Graphics (SIGGRAPH) 36, 4, July 2017, 95:1ś13. https://doi.org/10.1145/3072959.3073640. [dostęp: 15.02.2019]

Tomaszkiewicz M., *Chińczycy stworzyli sztucznego prezentera wiadomości,* 09.11.2018, https://www.antyradio.pl/Technologia/Duperele/Chinczycy-stworzyli-sztucznego-prezentera-wiadomosci-27057 [dostęp: 20.02.2019]

What are deepfakes & why the future of porn is terrifying. https://www.highsnobiety.com/p/what-are-deepfakes-ai-porn/ [dostęp: 16.02.2019]

Fakeapp as a new threat to political and information security

Abstract

With the development of technology, new possibilities of creating human faces have appeared, which can be used to carry out personal attacks on target people. FakeApp is a smart program that uses artificial intelligence algorithms that first "learn faces" so that they can then perform a substitution, which is an automatic Photoshop for movies. The FakeApp program allows you to replace one person's face with the face of another person whose photo is entered into the program. FakeApp reduces the task of transforming faces in a movie into a one-button process by automatically splitting, transforming and combining video frames.

Słowa kluczowe: FakeApp, program Deep Video, edytowanie głosu, sztuczna inteligencja

Key words: FakeApp, Deep Video, voice editing, artificial intelligence

Olga Wasiuta
profesor zwyczajny, doktor habilitowany, Dyrektor Instytutu Nauk o Bezpieczeństwie, Kierownik Katedry Bezpieczeństwa Narodowego Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie. Zajmuje się problematyką bezpieczeństwa regionalnego i europejskiego oraz wojną hybrydową. Jest autorką lub współautorką m.in. takich monografii jak: *Wojna hybrydowa Rosji przeciwko Ukrainie* (Kraków 2017), *Państwo Islamskie ISIS. Nowa twarz ekstremizmu* (Warszawa 2018); współredaktor monografii wieloautorskich poświęconych bezpieczeństwu: *Współczesne wyzwania bezpieczeństwa europejskiego* (Kraków

2016), *Współczesne problemy bezpieczeństwa państwa* (Stalowa Wola 2017), *Wyzwania bezpieczeństwa międzynarodowego* (Stalowa Wola 2017); *Vademecum bezpieczeństwa* (2018); jest również autorką licznych artykułów naukowych. Jest członkiem Polskiego Towarzystwa Geopolitycznego; członkiem Komitetu Redakcyjnego oraz przewodniczącą Rady Programowej czasopisma „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate"; zastępca redaktora naczelnego czasopisma naukowego „Socjologia prawa" (Ukraina, Kijów). E-mail: olga.wasiuta@up.krakow.pl

Sergiusz Wasiuta
profesor zwyczajny, doktor habilitowany Instytutu Politologii Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie. Jest autorem ponad 250 prac naukowych w wydawnictwach krajowych i zagranicznych na temat historii stosunków polsko-ukraińskich na przełomie XX–XXI; zajmuje się politycznym i społeczno-ekonomicznym rozwojem Ukrainy w okresie niepodległości; w kręgu zainteresowań naukowych znajdują się również badania nad walka informacyjną, problemy bezpieczeństwa społeczno-informacyjnego i energetycznego w kontekście zagrożeń hybrydowych i cywilizacyjnych; przyczyny i skutki kryzysu ekologicznego oraz jego wpływ na bezpieczeństwo międzynarodowe. Jest autorem lub współautorem licznych publikacji naukowych, w tym ponad 10 monografii: *Wojna hybrydowa Rosji przeciwko Ukrainie* (Kraków 2017), *Państwo Islamskie ISIS. Nowa twarz ekstremizmu* (Warszawa 2018); *Екологічна політика*: *національні та глобальні реалії*. У 4-х томах. (Чернівці 2003–2004) i in.; jest autorem licznych artykułów naukowych. Dziś jest zastępcą redaktora naczelnego i współredaktorem kwartalnika „Przegląd Geopolityczny" (Geopolitical Review) (Polska, Kraków); zastępcą redaktora naczelnego czasopisma „Ekologiczne prawo Ukrainy" (Ukraina, Kijów); ekspertem Centrum Europy Wschodniej Uniwersytetu Marii Curie-Skłodowskiej w Lublinie w zakresie problematyki historycznej, politycznej, ekonomicznej, społecznej i kulturowej państw Europy Wschodniej. E-mail: sergusz.wasiuta@up.krakow.pl.