

Deepfake

Łukasz Migniewicz

Zdroje

Zdroj A

Deepfake je fenomén, ktorý je čoraz častejšie prítomný na internete a ktorý sa dá použiť na celom svete.[...] Samotný termín pochádza z dvoch anglických slov: „deep“ (hlboký ako pri hlbokom učení umelej inteligencie) a „fake“ (vymyslený). Ide o spracovanie zvuku a obrazu zamerané na vytváranie falošných videí pomocou pokročilej technológie umelej inteligencie. Hlavným cieľom tejto technológie je vytvárať zvukové a obrazové záznamy, ktoré nemožno odlíšiť od skutočných, vrátane pravdivých výrokov, prejavov a činov. Deepfake nevytvára nové filmy, ale vychádza z materiálu, ktorý už existuje online a ktorý potom prepracúva. Počítač sleduje tvár, identifikuje v nej desiatky kľúčových záchytných bodov a spojí ich do siete, ktorá umožňuje ich úpravu v pohybe. [...] Bolo vytvorené video, v ktorom bývalý americký prezident Barack Obama nazýva svojho nástupcu Donalda Trumpa „sviniarom“.[...]

„Deepfake na internete – čo to je?“[Deepfake w Internecie – čo to je?], 18. júna 2020 [prístup 10. decembra 2020]. K dispozícii na stránke Puffa.pl:
<http://www.puffa.pl/2020/06/18/deepfake-w-internecie-co-to-jest/>.

Zdroj B

V posledných rokoch sa technológia [...] stala všadeprítomnou a umožňuje ľuďom na celom svete okamžite prijímať fotografie a filmy. To sa prejavuje [...] v schopnosti aj relatívne nekvalifikovaných používateľov manipulovať a deformovať posolstvo vizuálnych médií. Hoci sa manipulácia videí vo veľkej miere využíva na zábavné alebo umelecké ciele, môže slúžiť aj na šírenie propagandy alebo vytváranie dezinformačných kampaní. Táto multimediálna manipulácia je možná vďaka širokej dostupnosti pokročilých aplikácií, ktoré upravujú zvuk a obraz, ako aj vďaka automatizovaným manipulačným algoritmom, ktoré uľahčujú úpravu spôsobom,

ktorý je vizuálne veľmi ťažko rozoznatelný. [...] Takéto videá predstavujú potenciálnu hrozbu pre vnútornú bezpečnosť každého štátu a taktiež sa môžu stať nástrojom, ktorý ovplyvní výsledky volieb. Vyfabrikované video môže ohroziť národnú bezpečnosť a ovplyvniť verejnú mienku, čo je oblasť, ktorú využívajú podvodníci, ktorí chcú zasahovať napríklad do politických názorov spoločnosti; stáva sa zbraňou v informačnej vojne.

Uvedená technológia bude prirodzeným nástrojom, ktorý budú štáty využívať na manipuláciu verejnej mienky a realizáciu dezinformačných kampaní, ako aj na podkopávanie dôvery v existujúce inštitúcie. S novými a veľmi pokročilými metódami sledovania tváre a manipulácie s videom preto prichádza nová éra dezinformácií.

V čase, keď je dôvera verejnosti v médiá a politiku už aj tak krehká, môže obava, že všetko, čo sledujeme online, môže byť presvedčivou formou podvodu vymysleného niekým s výkonným počítačom, ešte viac podkopať demokraciu [...]

Olga Wasiuta a Sergiusz Wasiuta, „FakeApp ako nová hrozba politickej a informačnej bezpečnosti“ [FakeApp jako nowe zagrożenie bezpieczeństwa politycznego i informacyjnego], *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate*, 2019, č. 9(3), s. 136 [prístup 10. decembra 2020]. Dostupné na *Studia de Securitate*: <https://studiadesecuritate.up.krakow.pl/wp-content/uploads/sites/43/2019/10/9-1.pdf>.

Zdroj C

Pomocou umelo vytvoreného hlasu generálneho riaditeľa veľkej spoločnosti zavolali zločinci riaditeľovi jednej z jej dcérskych spoločností a požiadali ho o prevod peňazí. Takto sa im podarilo vylákať 243 000 dolárov. [...] Podľa odborníka zločinci použili softvér na generovanie napodobeniny hlasu. [...] mohli upravovať aj úryvky autentických nahrávok hlasu generálneho riaditeľa. Využitie tejto technológie bolo prezentované napríklad na minuloročnej konferencii Black Hat, kde vedci dokázali, že už existujúce nástroje umožňujú rekonštruovať hlas kohokoľvek s cieľom prelomiť bezpečnostné opatrenia na identifikáciu hlasu, ktoré používajú napríklad banky. Tvrdia, že kvalita zvuku nemusí byť dokonalá, aby takéto bezpečnostné opatrenia prekonala. Dokázali tiež, že takýto podvod dokážu spáchať do desiatich minút.

„Zreplikovali hlas šéfa spoločnosti. Podvodne sa obohatili o 243 000 dolárov“ [Odtworzyli głos szefa firmy. Wyłudzili 243 tys. dolarów], 6. septembra 2019 [prístup 10. decembra 2020]. K dispozícii na stránke Konkret24: <https://konkret24.tvn24.pl/tech,116/odtworzyli-glos-szefa-firmy-wyludzili-243-tys-dolarow,967072.html>.

Zdroj D

Pristátie Apolla II na Mesiaci 20. júla 1969 znamenalo prelom v dejinách vesmíru. Čo keby sa to však nepodarilo? Nový projekt MIT ukazuje silu deepfake [...] „Osud rozhodol, že muži, ktorí išli na Mesiac, aby ho v pokoji preskúmali, zostanú na Mesiaci odpočívať v pokoji,“ hovorí prezident Nixon vo falošnom filme, pričom má na mysli astronautov Neila Armstronga, Buzza Aldrina a Michaela Collinsa [...]. Odborníkom z MIT trvalo približne pol roka, kým pripravili presvedčivú sedemminútovú nahrávku kombinujúcu zábery NASA s falošným Nixonovým prejavom. Na zabezpečenie toho, aby hlas a pohyby prezidenta napodobňovali jeho skutočné pohyby, boli použité technológie hlbokého učenia umelej inteligencie. Toto video je prvým videom vytvoreným v rámci projektu „In Event of Moon Disaster“, ktorého cieľom je ukázať ľuďom, aký nebezpečný môže byť vplyv manipulovaných videozáznamov. [...]

Klaudia Stawska, „Je pristátie na Mesiaci lož? Stačí si vypočúť slová prezidenta Spojených štátov“ [Ładowanie na Księżycu to kłamstwo? Wystarczy posłuchać prezydenta USA], 21. júla 2020 [prístup 10. decembra 2020]. Dostupné na Tech.wp.pl: <https://tech.wp.pl/ladowanie-na-ksiezycu-to-klamstwo-wystarczy-posluchac-prezydenta-usa-6534416849188481a>

[...] Cieľom projektu „In Event of Moon Disaster“ však bolo vytvoriť alternatívny priebeh udalostí. Na tento účel vedci použili nielen pôvodnú nahrávku s Nixonom, ale aj archívny materiál, ktorý zachytáva tieto minulé udalosti. Potom nastúpila umelá inteligencia, aby fikcia vyzerala reálne. Výsledok deepfake je skutočným skvostom. Diváka síce poteší, ale zároveň ho vydesí a ukáže, aké pokročilé sú už algoritmy deepfake. Inžinieri z MIT sa netaja tým, že cieľom projektu je upozorniť na to, akým smerom sa môže táto technológia vyvíjať a akú nepredstaviteľnú spúšť môže spôsobiť v internetových médiách. Pokiaľ ide o historikov, tí sa najviac obávajú, že na YouTube môžu byť zverejnené falošné videá o kľúčových historických a súčasných udalostiach, ktoré môžu manipulovať verejnú mienku a následne vyvolať sociálne nepokoje.

„Sfalšovaná katastrofa misie Apollo 11 – pozrite si tento úžasný DeepFake“ [Sfałszowana katastrofa misji Apollo 11. Zobaczcie ten niesamowity DeepFake], 22. júla 2020 [prístup 10. decembra 2020]. K dispozícii na stránke Geekweek.pl: <https://www.geekweek.pl/news/2020-07-22/sfałszowana-katastrofa-misji-apollo-11-zobaczcie-ten-niesamowity-deepfake-film/>.

Zdroj E

Technológia deepfake má pozitívny potenciál pre vzdelávanie. Vďaka interaktivite by mohla priniesť revolúciu do našich hodín dejepisu. Mohla by zachovať príbehy a pomôcť upútať pozornosť. Napríklad v roku 2018 Múzeum a vzdelávacie centrum holokaustu v Illinois vytvorilo hologramové rozhovory. Návštevníci sa tak mohli porozprávať a komunikovať s ľuďmi, ktorí prežili holokaust. Mohli klásť otázky a vypočuť si ich príbehy. S rozvojom technológie deepfake by sa tento druh virtuálnej histórie mohol stať dosiahnuteľným v oveľa väčšom rozsahu.

[...] Technológia deepfake môže plniť úlohu CGI [computer generated imagery - počítačom generované obrazy] a obnoviť podobu nedostupných hercov z minulosti. Takže postava nemusí umrieť spolu s hercom. Napríklad rekonštrukcia zosnulého Petra Cushinga v snímke Star Wars Story: Rogue One (2017), ktorý zomrel v roku 1994. [...] Technológia AI by nám mohla pomôcť vytvoriť virtuálne múzeá. [...] Technológia deepfake by nám dokonca mohla umožniť oživiť mŕtvych umelcov. Napríklad Salvadora Dalího v Múzeu Salvadora Dalího na Floride.

„Áno, existujú pozitívne príklady deepfake“ [prístup 10. decembra 2020]. K dispozícii na stránke ThinkAutomation: <https://www.thinkautomation.com/bots-and-ai/yes-positive-deepfake-examples-exist>.