MKD revue, ročník 11 (2024), číslo 1, ISSN: 1339-777X

Deepfake

Evolúcia, hrozby a možné využitie

Martin HANDLOVSKÝ, Zdenka ŠMEHYLOVÁ

Abstrakt

Technológia deepfake, založená na pokročilých metódach hlbokého učenia a umelej inteligencie, umožňuje generovať realistické falošné multimediálne obsahy, ako sú videá, fotografie a zvukové nahrávky. Tento článok poskytuje podrobnú analýzu vývoja a aplikácií deepfake technológie od jej prvého výskytu v roku 2017 až po súčasnosť. Skúma jej využitie v rôznych odvetviach vrátane zábavného a filmového priemyslu, vzdelávania a virtuálnych asistentov. Zároveň sa venuje vážnym bezpečnostným a etickým hrozbám, ktoré s touto technológiou súvisia, ako je manipulácia verejnej mienky, šírenie dezinformácií a kybernetické podvody. Článok tiež navrhuje opatrenia na prevenciu negatívnych dôsledkov deepfake technológie. Cieľom tohto článku je poskytnúť čitateľom komplexný prehľad o technológii deepfake, jej potenciálnych prínosoch a rizikách, a zároveň ponúknuť praktické odporúčania na zmiernenie negatívnych dopadov tejto revolučnej technológie.

Kľúčové slová

deepfake, deepfake technológia, hlbobé strojové učenie, hrozby deepfaku, prevencia proti deepfaku,

Abstract

Deepfake technology, based on advanced deep learning and artificial intelligence methods, enables the generation of realistic fake multimedia content such as videos, photos and audio recordings. This article provides a detailed analysis of the development and applications of deepfake technology from its first appearance in 2017 to the present. It examines its use in various industries including entertainment and film, education, and virtual assistants. It also addresses the serious security and ethical threats associated with this technology, such as the manipulation of public opinion, the spread of misinformation, and cyber fraud. The article also suggests measures to prevent the negative consequences of deepfake technology. This article aims to provide readers with a comprehensive overview of deepfake technology, its potential benefits and risks, while offering practical recommendations to mitigate the negative impacts of this revolutionary technology.

Keywords

deepfake, deepfake technology, deep machine learning, deepfake threats, deepfake prevention,

Úvod

Technológia deepfake predstavuje prelomový vývoj v oblasti umelej inteligencie a hlbokého strojového učenia, ktorá umožňuje vytvárať falošné, avšak veľmi realistické multimediálne obsahy. Základ tejto technológie spočíva v použití hlbokých neurónových sietí, ktoré umožňujú nahrádzať tváre a hlasy v existujúcich videách, fotografiách či zvukových nahrávkach, čím vznikajú obsahy, ktoré sú takmer nerozlíšiteľné od skutočných. Prvé deepfake videá sa objavili na internete už v roku 2017, pričom ich popularita rýchlo stúpala, najmä na platforme Reddit. Dnes je táto technológia natoľko vyvinutá, že jej aplikácie zasahujú do rôznych odvetví, vrátane zábavného priemyslu, vzdelávania a dokonca aj virtuálnych asistentov.

Aj keď deepfake technológia prináša nové možnosti a otvára dvere k inováciám, súčasne prináša aj vážne bezpečnostné a etické hrozby. Manipulácia verejnej mienky, šírenie dezinformácií a vytváranie kompromitujúcich materiálov, sú len niektoré z negatívnych dôsledkov, ktoré môžu vyplynúť z nesprávneho použitia tejto technológie. Okrem toho môže deepfake ohroziť aj bankové systémy a autentifikačné procesy, čo zvyšuje potrebu efektívnych opatrení na ochranu proti zneužitiu.

Cieľom tohto článku je poskytnúť komplexný prehľad o vývoji, aplikáciách a hrozbách deepfake technológie. Bude sa zaoberať analýzou jej evolúcie, využitím v rôznych oblastiach, potenciálnymi rizikami a možnými preventívnymi opatreniami, ktoré môžu pomôcť zmierniť negatívne dopady tejto technológie na spoločnosť.

Deepfake

Deepfake predstavuje jednu z techník umelej inteligencie. Táto technika umožňuje vytvárať falošné videá, obrazy, či dokonca aj samotné zvukové nahrávky. V súčasnosti je táto technológia natoľko vyvinutá, že jej diela sú takmer nerozlíšiteľné od skutočných (Wooldridge 2021).

Táto technológia, využíva hlboké neurónové siete na generovanie realistických falošných obsahov, často nahradzujúc tváre alebo hlasy ľudí vo videách, v nahrávkach alebo na

fotografiách. Napriek tomu, že deepfake môže byť použitý na zábavné účely, ako sú napríklad komediálne videá, má zároveň aj potenciál na tiež predstavovať vážne bezpečnostné a etické hrozby. Napríklad môže byť použitý na manipuláciu s verejným mienením, šírenie dezinformácií alebo dokonca na vytvorenie hanlivého materiálu s falošnými tvárami (Somers 2020).

Evolúcia deepfaku

Prvé deepfakes v online prostredí sa začali objavovať v roku 2017. V tom čase sa primárne deepfake obsah sústredil na platforme Reddit. Veľmi rýchlo si získali popularitu. Táto technológia umožňovala ľuďom vytvárať videá, v ktorých celebrity hovoria alebo robia veci, ktoré by inak nikdy neurobili. Takisto sa začala vo veľkej miere využívať aj pri kontaktovaní celebrít. Pomocou hlasovej nahrávky, ktorá znela ako vybraná verejne známa osoba, dokázal ktokoľvek kontaktovať inú verejne známu osobu (Somers 2020).

Technológia deepfaku sa neustále vyvíja a zdokonaľuje, pričom súčasné deepfakes sú takmer nerozlíšiteľné od skutočných videí. Vývoj deepfaku je úzko spojený s pokrokmi v oblasti hlbokého učenia a umelej inteligencie, pričom nové algoritmy a väčšie množstvo dát prispievajú k vytváraniu stále realistickejších falošných obsahov (Heikkilä, 2024).

Popularita deepfaku každým rokom enormne stúpa v období od roku 2019 do roku 2020 vzrástol počet obsahu vytvoreného pomocou umelej inteligencie až o 84%. V období od roku 2022 do roku 2023 to bolo dokonca až o 100% (Miškerík, 2023).

Avšak netreba zabúdať na to, že deepfake má aj svoju lepšiu stránku. Vďaka tejto technológií dokázala holywoodska produkcia aspoň pomocou obrazu oživiť zosnulého herca, Paula Walkera. Konkrétne sa tak stalo vo filme Rýchlo a zbesilo 7, kedy produkcia našla podobného herca a pomocou umelej inteligencií ho dokázali premeniť na Paula Walkera (Vnuk 2021).

Využitie deepfaku v rôznych oblastiach

Technológia deepfaku ponúka ma široký portfólio využitia. Najviac populárne je pri vytváraní zábavného kontentu. Avšak jej neustálym zlepšovaním sa začína využívať aj napríklad v oblasti vzdelávania, vo filomovom priemysle, ale aj v prostredí, ktoré využíva virtuálnych hovorcov.

Zábavný Priemysel

V zábavnom priemysle sa deepfake používa na vytváranie humorných videí a paródií. Tvorcovia obsahu často využívajú túto technológiu na zmenu tvárí v komediálnych situáciách, čo umožňuje divákom vidieť známe osobnosti v nečakaných a zábavných kontextoch. Napríklad deepfake videá, kde sú tváre hercov zmenené na tváre iných známych osobností, sú populárne na sociálnych sieťach, či dokonca na streamovacích platformách ako je napríklad YouTube (Galloway 2022).

Filmový Priemysel

Vo filmovom priemysle deepfake prináša revolúciu v oblasti vizuálnych efektov. Umožňuje starnutie, omladzovanie, či dokonca oživenie hercov, čo je užitočné pri vytváraní flashbackov alebo futuristických scén. Deepfake tiež pomáha prekonávať jazykové bariéry tým, že synchronizuje ústa hercov s preloženými dialógmi, čo môže zlepšiť divácky zážitok v rôznych jazykoch (Bhargav, 2023).

Virtuálni Hovorcovia

Deepfake technológia sa využíva aj na vytváranie realistických virtuálnych hovorcov. Títo hovorcovia môžu slúžiť ako avatary v prostredí virtuálnej asistencie alebo zákazníckeho servisu, čím zlepšujú interakciu s používateľmi a poskytujú personalizovanejšie a efektívnejšie služby (Westerlund 2019).

Satirické Paródie

Satira a paródie často využívajú deepfake na kritiku politikov, celebrít a iných verejne známych osobností. Tieto videá zvyčajne zosmiešňujú danú osobu tým, že ju umiestnia do absurdných alebo komických situácií. Satirické paródie majú potenciál upozorňovať na spoločenské a politické problémy a podporovať diskusiu prostredníctvom humoru (Agence France-Presse 2023).

Vzdelávanie

V oblasti vzdelávania sa deepfake využíva na simuláciu historických udalostí alebo oživenie historických osobností. Táto technológia umožňuje študentom zažiť dejiny interaktívnym a vizuálne atraktívnym spôsobom, čo môže zlepšiť ich porozumenie a zapojenie do vzdelávacieho procesu (Brdička 2023).

Dezinformácie a Kybernetické Podvody

Deepfake však nesie so sebou aj riziká, najmä v oblasti dezinformácií a kybernetických podvodov. Šírenie falošných správ, podvodov a propagandy prostredníctvom deepfake videí môže mať vážne dôsledky pre spoločnosť. Môže poškodzovať reputáciu ľudí a inštitúcií a ovplyvňovať verejnú mienku, čo zvyšuje potrebu efektívnych opatrení na detekciu a prevenciu deepfake obsahov (Boston Institute of Analytics 2024).

Hrozby

Samozrejme, každá nová technológia so sebou prináša určité hrozby. Zjednodušene môžeme povedať, že technológia deepfake môže byť v najväčšom množstve využívaná na vytváranie falošného obsahu, určeného na imitovanie určitého dôležitého ľudského autentifikačného znaku. Hlavne čo sa týka bankového sektora, ten používa zložitejšie autentifikačné metriky,

ktoré sa ale s pomocou použitia technológie deepfake budú dať oklamať, a tak vytvoria značne zraniteľné miesto (Deloitte. 2024).

Okrem samotného oklamania autentifikačného procesu môže byť technológia deepfake taktiež využitá na oklamanie či už zákazníkov rôznych firiem, alebo rôzneho personálu zastávajúceho rôzne strategické pozície v rámci podniku. Takýto typ podvodu môže vyústiť v značné finančné straty, prípadne inú formu ohrozenia strategickej pozície podniku na trhu (KMPG 2023).

S tým taktiež súvisí aj falšovanie rôznych dôležitých dokumentov, napríklad občianskych preukazov , či súdnych rozhodnutí, alebo iných dôležitých vládnych dokumentov. Takéto falšovanie vládnych dokumentov môže byť ďalej využité napríklad na vytvorenie falošnej identity, či zámerné očiernenie alebo zhoršenie reputácie určitej osoby (Deloitte 2024).

So zhoršením reputácie určitej osoby súvisí aj možnosť zhoršenia verejnej mienky, ak sa jedná o známu osobnosť, či už politika alebo celebrity výrazne investovanej do verejného života. Deepfake technológia totiž može byť použitá vyslovene na vytvorenie falošného kompromitujúceho materiálu, ktorý má slúžiť na poškodenie určitej osoby. Poškodenie takejto osoby môže mať výrazné následky nielen pre osobu samotnú, ale aj pre každého, kto by sa danou osobou rozhodol uzavrieť nejakú formu obojstrannej spolupráce. Škody môžu teda byť v tomto prípade dvojnásobné (Deloitte 2024).

Deepfake technológia môže byť taktiež využitá na podporu kyberšikany, konkrétne môže byť využitá na vytvorenie falošného kompromitujúceho materiálu, ktorý bude slúžiť ako dôkaz osôb dopúšťajúcich sa trestného činu kyberšikany.. Keďže dostupnosť týchto nástrojov nie je problémom, môžeme očakávať, že miera podobných incidentov výrazne narastie. Zraniteľnou sa môže stať hlavne mladšia generácia, ktorá má výrazne vyššiu mieru digitálnej gramotnosti ako staršia generácia. (Departement of Homeland security, [s. a.].).

Deepfake technológia môže byť taktiež, okrem doteraz spomenutých, na vytváranie a šírenie veľmi presvedčivých dezinformácií, kde môžu akúkoľvek strategickú osobu prinútiť k vyjadreniu akéhokoľvek kontroverzného názoru, čo môže viesť k poškodeniu samotnej osoby

či organizácie, či už finančne alebo nefinančne. Takéto dezinformácie samozrejme nemusia byť obmedzené len na poškodenie podniku, môžu okrem nich poškodiť aj neziskové organizácie či štáty, a ohroziť tak rôzne geopolitické vzťahy. S tým súvisí aj to, že deepfake technológia značne ohrozuje mieru dôveryhodnosti informácií, ktoré sú v online priestore publikované (Deloitte 2024).

Špecifickou formou využitia deepfake technológie je takzvaná deepfake pornografia. Do tejto kategórie spadá pornografia vygenerovaná umelou inteligenciou. Tento typ pornografie je považovaný za majoritnou kategóriou medzi videomateriálom vygenerovaným umelou inteligenciou. Tento typ deepfake videí má ale značne negatívnu povesť, hlavne kvôli tomu, lebo istú časť tohto videomateriálu tvorí aj takzvaná „non-concensual“ pornografia, teda pornografia vytvorená bez vedomia, a teda aj vysloveného súhlasu, jednej či viacerých osôb nachádzajúcich sa v takomto videu. (ajg.com) Podľa americkej Homeland Security bolo v rámci výskumu realizovaného v októbri 2020 nájdených až sto tisíc umelo vygenerovaných obrázkov z kategórie pornografického materiálu, pričom bol vytvorený bez súhlasu osoby nachádzajúcej sa na videu či fotografii. Niektoré štatistiky hovoria o tom, že až 95% deepfake videí generovaných melou inteligenciou bolo práve takejto povahy, teda pornografický materiál vytvorený bez súhlasu osoby nachádzajúcej sa v danom obrazovom materiáli (Departement of Homeland security, [s. a.].).

Prevencia

Okrem spomenutých skutočností je však potrebné si taktiež priznať, že voči každému negatívnemu vplyvu modernej technológie je možné sa do určitej miery brániť. Existujú totiž určité spôsoby prevencie voči negatívnym vplyvom deepfake technológie.

Jedným zo spôsobov, ako môžeme zamedziť negatívnym vplyvom deepfake technológie, ak sa jedná o určtitú organizáciu, je vzdelávanie pracovníkov našej organizácie o aktuálnom stave deepfake technológie, o tom, čo všetko táto technológia dokáže, a akými spôsobmi sa voči môžeme brániť voči jej negatívnym aspektom, ktoré môžu byť zneužité na určitú kriminálnu aktivitu (Sjouwerman 2024).

Rekreační používatelia nachádzajúci sa na internete môžu taktiež implementovať určité riešenia, aby zamedzili prípadnému zneužitiu ich identity deepfake technológiou. Medzi prvými by mala byť zaradená značná miera diskrétnosti pri zverejňovaní fotografií , prípadne videí, na internet, hlavne ak sa na nich nachádzajú určité citlivé informácie. Okrem toho by sme však mali mať nastavené čo najsúkromnejšie nastavenia na sociálnych sieťach, aby sme zamedzili príliš verejnému prístupu k našim fotografiám, či videám. V rámci prijímania video alebo foto obsahu zverejňovaného na internete by sme tiež mali pristupovať opatrne, a ideálne sa naučiť používať systémy reverzného vyhľadávania obrazu na overovanie foto a video obsahu, ktorý bol vytvorený alebo aj zverejňovaný pochybnými zdrojmi. (Farley 2024). Implementácia multifaktorovej autentifikácie by mala byť samozrejmosťou aj v každodennom živote, takisto aj s nastavením dostatočne silného hesla na všetky účty, do ktorých sa na internete prihlasujeme(Deloitte 2023) . Treba však okrem spomenutých skutočností aj mať naštudované pravidlá platformy, kde daný obsah zverejňujeme, keďže platforma môže mať tieto záležitosti nastavené na úplne zdieľanie zverejňovaného obsahu hocijakej tretej strane. (Farley 2024).

Okrem samotného poznania danej technológie môžeme jej negatívnym vplyvom zamedziť pomocou implementácie dodatočných bezpečnostných opatrení, príkladom môže byť implementácia dvojstupňového overovania, napríklad overovanie telefonických hovorov pomocou overenej emailovej adresy. Ďalším príkladom môže byť napríklad implementovanie overenia finančných transakcií manipulujúcich s väčším finančným kapitálom ďalším strategickým zamestnancom daného podniku či organizácie, čo je proces, ktorý dokáže firme ušetriť niekedy nespočítateľný obnos peňazí. Ideálna je fyzická prítomnosť oboch zamestnancov na jednom mieste, aby sa zamedzilo prípadnému využitiu deepfake technológie na vytvorenie falošného audio alebo video záznamu danej osoby (Sjouwerman 2024).

Deepfake technológia má taktiež určité bariéry, ktoré môžeme v čase písania tohto článku využiť na objavenie možnej manipulácie s video materiálom, teda ich môžeme odlíšiť od originálneho obrazového materiálu pomocou určitých znakov. Jedným z takýchto znakov je absencia žmurkania u osoby na ktorú je tento obrazový materiál zameraný, je to jeden z častých

nedostatkov pri vytváraní deepfake videí. S tým taktiež súvisí zreteľne neprirodzený pohyb očí, ktorý deepfake technológia má stále problém replikovať (FORTINET 2024).

Taktiež neprirodzené výrazy tváre sú dostatočne spoľahlivý indikátor toho, že s obrazovým materiálom pravdepodobne niekto manipuloval. Okrem týchto faktorov má deepfake technológia problém prirodzene replikovať prirodzenosť vlasov, nastavenia pozície tela či výrazy tváre logicky konzistentné s tým, čo osoba vo videu práve hovorí. Taktiež pohyb pier nemusí presne sedieť s tým, čo osoba práve hovorí. Taktiež aj na pozadí sa môže vyskytnúť určitá forma neprirodzenosti, napríklad v absencii pohybu určitého živého objektu, či nesprávne sediace farby pozadia .

Okrem spomenutých spôsobov však existujú ešte ďalšie spôsoby, ktorými sa môžeme brániť voči negatívnym vplyvom deepfake technológie. Platformy, na ktorých je možné zdieľať takýto obsah, by mali mať ideálne nastavené dostatočne silné pravidlá na to, aby sa zneužitiu obrazového materiálu publikovaného na platforme. Viaceré platformy sa už teraz snažia podniknúť rôzne kroky k tomu, aby zamedzili šíreniu deepfake obrazového materiálu na ich platforme. Sociálna sieť Facebook najala personál určený k vybudovaniu deepfake detektora. Iné platformy už teraz do určitej miery blokujú deepfake obsah tak, aby sa na ich platforme nemohol publikovať vôbec (FORTINET 2024).

Účinnejším spôsobom blokovania takéhoto obsahu je implementovanie určitej formy legislatívy na štátnej úrovni, ktorá by takýto vytváranie takéhoto obsahu postavila do roviny kriminálnej činnosti. Európska únia môže slúžiť ako príklad, stojí totiž za legislatívou, ktorá vyžaduje, aby všetok deepfake obsah bol jasne označený (Federal office for information security [s. a.].).

Taktiež je potrebné, aby boli vytvorené organizácie, či už ziskového alebo neziskového charakteru, ktorých hlavným zámerom by boli návrh, implementácia a neustále vylepšovanie nástroja určeného na detekciu deepfake obsahu. Viaceré takéto nástroje už existujú, napríklad firma Deeptrace ponúka program fungujúci na spôsob antivírusového programu ktorý ho označí ako škodlivý obsah, prípadne Reality Defender od firmy AI Foundation sa snaží zachytiť takýto obsah predtým než napácha akúkoľvek škodu (FORTINET 2024).

Príklady využitia technológie deepfake

Deepfake technológia umožňuje rôzne formy vylepšenia rôznych oblastí. Ako dva zaujímavé príklady môžeme spomenúť vytváranie vodoznakov v audio súboroch, a využitie umelej inteligencie vo fotopletysmografii.

Firma Google má k dispozícii viacero modelov založených na umelej inteligencii, medzi inými aj nástroj Lyria, určený na generovanie umelo vytvorenej hudby rôznych žánrov, či ž inštrumentálnej alebo s vokálmi. Do tohto nástroja sa Google rozhodol implementovať aj nástroj na vytváranie vodoznakov v umelo vytvorených audio súboroch, taktiež založený na umelej inteligencii. Okrem toho, že tento vodoznak nie je detekovateľný ľudským uchom, tak nestráca na kvalite ani v prípade dodatočnej kompresie, či pridania dodatočného zvuku. Tento nástroj je vysoko odolný voči klasickým formám úpravy ako strih či zmena veľkosti. V dnešnej dobe, keď je na vzostupe umelo vytváraný obsah, je dôležité vytvárať aj technológie určené na detegovanie a „pevne vryté“ označovanie umelo vytváraného obsahu (Porter, 2023).

Deepfake technológia je taktiež využívaná aj vo fotoplethysmografii, optická technika používaná na detegovanie zmeny objemu krvi. Aplikovaním deepfake technológie v tejto disciplíne sa podarilo vedcom vytvoriť unikátny nástroj, ktorý neinvazívnym spôsobom dokáže merať objem krvi v tele a zároveň aj tep srdca, a podľa výskumov sú neporovnateľne presnejšie v meraní daných veličín ako bežné konvenčné metódy merania (Sepehr, 2024).

Záver

Deepfake technológia je výrazným posunom do budúcnosti. Prináša nám nové možnosti využitia v rôznych oblastiach, a vďaka tomu bude výskum v oblastiach, kde sa táto technológia využije, napredovať značnou rýchlosťou, ak sa teda táto technológia implementuje správne.

Avšak, každá moderná technológia so sebou prináša určité negatívne aspekty, prípadne možnosti na vylepšenie morálne otáznych aktivít. V tomto príspevku sme si ukázali, kde by táto technológia mohla byť potenciálne zneužitá, a priblížili sme si, aké ohrozenia nám táto

technológia môže priniesť. Okrem toho sme si však aj ukázali možné spôsoby, ako sa voči týmto ohrozeniam brániť.

Na konci príspevku sme si ukázali dva typy produktívneho využitia deepfake technológie, ktoré aplikáciou v oblasti výskumu pomôže nespočetnému počtu profesionálov danej oblasti.

Zoznam použitých zdrojov

AGENCE FRANCE-PRESSE, (2023). *Filmmakers at Cannes Film Festival Grapple With 'Tectonic' AI Shift.* Gadgets360. Online. 2023-05-24. Dostupné na: https://www.gadgets360.com/entertainment/news/cannes-film-festival-2023-filmmakers-tectonic-ai-shift-chatgpt-tom-hanks-harrison-ford-deepfake-technology-4062617. [Zobrazené 2024-06-16]

BHARGAC, Sai, (2023). *Reality Reshaped: The Deep Impact of Deepfake Technology on Film and Television.* Analytics Insight. Online. 2023-11-21. Dostupné na: https://www.analyticsinsight.net/deepfake-technology/deepfake-in-entertainment-impact-on-film-and-television. [Zobrazené 2024-06-16]

BOSTON INSTITUTE OF ANALYTICS, (2024). *Deepfake technology: Unmasking the rise of synthetic media and its implications.* Online. 2024-04-02. Dostupné na: https://bostoninstituteofanalytics.org/blog/deepfake-technology-unmasking-the-rise-of-synthetic-media-and-its-implications/. [Zobrazené 2024-06-16]

BRDIČKA, Bořivoj, (2023). *Deep fake ve výuce*. Rvp.cz. Online. 2023-01-30 Dostupné na: https://spomocnik.rvp.cz/clanek/23410/DEEP-FAKE-VE-VYUCE.html. [Zobrazené 2024-06-16]

JAMAL, Anas et al., (2024). *How to safeguard against the menace of deepfake technology The battle against digital manipulation.* Deloitte.com. Online. Dostupné na: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-safeguarding-against-deepfake-technology-noexp.pdf [Zobrazené 2024-06-14]

FARLEY, John, (2024). *Deepfake Technology: The Frightening Evolution of Social Engineering*. Ajg.com Online. Dostupné na: https://www.ajg.com/us/news-and-insights/2023/jun/deep-fake-technology-the-frightening-evolution-of-social-engineering/ [Zobrazené 2024-06-14]

Federal office for information security. [s. a.].. *Deep Fakes – Threats and Countermeasures*.. Online. Dostupné na: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html [Zobrazené 2024-06-14]

FORTINET, (2024). *What Is A Deepfake?* Online. Dostupné na: https://www.fortinet.com/resources/cyberglossary/deepfake [Zobrazené 2024-06-14]

Galloway, Margie, (2022). *The history of deepfakes: From novelty to threat.* Popsci. Online. 2022-03-04. Dostupné na: https://www.popsci.com/technology/deepfakes-history-museum-exhibit/. [Zobrazené 2024-06-14]

Heikkilä, Melissa, (2024). *An AI startup made a hyperrealistic deepfake of me that's so good it's scary*. Technology Review. Online. 2024-04-25. Dostupné na: https://www.technologyreview.com/2024/04/25/1091772/new-generative-ai-avatar-deepfake-synthesia/

Homeland Security, [s. a.].. *Increasing Threat of DEEPFAKE Identities.* Online. Dostupné na: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf [Zobrazené 2024-06-12]

MIŠKERÍK, Martin, (2023). *Výskyt deepfake videí výrazne rastie. Odborník radí, na čo dávať pozor a čo si všímať.* Trend. Online. 2023-10-26. Dostupné na: https://www.trend.sk/technologie/vyskyt-deepfake-videi-vyrazne-rastie-odbornik-radi-co-davat-pozor-co-vsimat. [Zobrazené 2024-06-12]

OPPOS. [s. a.]. *Deepfake Threats: Dangers of AI-Manipulated Media.* Online. Dostupné na: https://getoppos.com/deep-fake-threats/ [Zobrazené 2024-06-12]

PORTER, John, (2023). *Google is embedding inaudible watermarks right into its AI generated music*. Online 2023-11-16. Dostupné na*:* *https://www.theverge.com/2023/11/16/23963607/google-deepmind-synthid-audio-watermarks* [Zobrazené 2024-06-12]

SEPEHR, Bo, (2024). *Photoplethysmography Is Improving Thanks to AI*. Uniwebb.com. Online.2024-04-30. Dostupné na: https://www.uniwebb.com/photoplethysmography-is-improving-thanks-to-ai/ [Zobrazené 2024-06-12]

SJOUWERMAN, Stu, (2024). *The evolution of deepfakes: Fighting the next big threat.* Online. 2024. Dostupné na: https://techbeacon.com/security/evolution-deepfakes-fighting-next-big-threat [Zobrazené 2024-06-12]

SOMERS, Meredith, (2020). *Deepfakes, explained.* MIT. Online. Dostupné na: https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained. [Zobrazené 2024-06-12]

VNUK, Peter, (2021). *Deepfake video: Hrozba alebo nástroj pokroku? Spôsobuje viac obáv než radosti.* Trend. Online. 2021-06-19. Dostupné na: https://www.trend.sk/technologie/deepfake-video-hrozba-nastroj-pokroku-sposobuje-viac-obav-nez-radosti. [Zobrazené 2024-06-12]

WESTERLUND, Mika, (2019). *Deepfake technology: Unmasking the rise of synthetic media and its implications.* Technology Innovation Management Review. Online. roč. 9 (2019), č. 11, s. 39-52. Dostupné na: https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf#:~:text=URL%3A%20https%3A%2F%2Ftimreview.ca%2Fsites%2Fdefault%2Ffiles%2Farticle_PDF%2FTIMReview_November2019%2520. [Zobrazené 2024-06-12]

WOOLDRIDGE, Michael J., (2021). *A brief history of artificial intelligence: what it is, where we are, and where we are going.* New York : Flatiron Books. ISBN 978-1-250-77074-5.

Autori

Bc. Martin Handlovský
martin.handlovsky@st.fhv.uniza.sk

Katedra mediamatiky a kultúrneho dedičstva
Fakulta humanitných vied
Žilinská univerzita v Žiline
Univerzitná 8215/1
010 26 Žilina
SLOVENSKÁ REPUBLIKA

Študent druhého stupňa študijného programu mediamatika a kultúrne dedičstvo so špecializáciou na oblasť médií a marketingu. V roku 2023 získal bakalársky titul z odboru mediálne a komunikačné štúdiá.

Bc. Zdenka Šmehylová
martin.handlovsky@st.fhv.uniza.sk

Katedra mediamatiky a kultúrneho dedičstva
Fakulta humanitných vied
Žilinská univerzita v Žiline
Univerzitná 8215/1
010 26 Žilina
SLOVENSKÁ REPUBLIKA

Študentka druhého stupňa študijného programu mediamatika a kultúrne dedičstvo so zameraním na médiá, kultúrne dedičstvo a marketing. V roku 2023 získala bakalársky titul z odboru mediálne a komunikačné štúdiá.