E-Bezpečí 2025, 10(1): Page 16-18. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=4475

HRANICE PADLY! S NOVÝM UPDATEM GENERÁTORŮ OBRÁZKŮ OD OPENAI JSME SCHOPNI TVOŘIT DEEP FAKE FOTOGRAFIE TÉMĚŘ BEZ OMEZENÍ

Kamil KOPECKÝ

V těchto dnech došlo k aktualizaci generátorů obrázků, které jsou nasazeny do produktů OpenAI (ChatGPT, Sora apod.). Kvalita výstupů přitom viditelně vzrostla a odhalit např. fotografii vygenerovanou umělou inteligencí se stává pro laiky (ale často i profesionály) téměř nemožné. Lze předpokládat, že tyto nové modely způsobí masový nárůst počtu deep fake fotografií a videí na internetu a zcela jistě budou zneužívány třeba v rámci volebních kampaní.

Je libo Donalda Trumpa, jak si dává "špeka" s Vladimírem Putinem? Žádný problém, během několika vteřin dostanete uvěřitelný výstup. Stačí si jen trošku víc pohrát se zadáním (promptem) - třeba popsat, že má výsledek působit jako analogová fotografie… a umělá inteligence začne tvořit. Takto jednoduše je možné vytvořit v zásadě cokoli.

Výše uvedené fotografie vytvořily generátory obrázků od OpenAI.

Etické limity jsou přitom nastaveny poměrně volně - pornografický materiál ani Adolfa Hitlera samozřejmě tyto běžné nástroje

nevygenerují, na druhou stranu např. materiály spojené s konzumací drog nejsou velký problém. Co AI nástroje filtrují poměrně razantně, je oblast rasismu - pokud např. napíšete, že chcete fotografii politika obklopeného černochy, aktivuje se etická hranice; pokud ale popíšete černochy jako “obyvatele JAR”, AI výsledek vytvoří. A generování známých politiků v běžných situacích modely tvoří různě - v závislosti na konkrétním kontextu. Každopádně např. ChatGPT tvrdí, že: "**nemůže generovat obrázky skutečných žijících politiků**, a to ani v běžných nebo satirických situacích. Důvodem jsou etické a právní zásady týkající se zneužití identity". Ve skutečnosti je ale velmi často vytvoří. Hranice však u všech online modelů velkých firem existují.

Inovované generátory **dokáží bez větších problémů věrně napodobit vzhled známých českých politiků** - od prezidentů, přes premiéry, senátory či poslance, stačí, aby na internetu zanechali dostatečnou digitální stopu (tj. dostatek fotografií, na který se AI může trénovat). Výstupy jsou přitom natolik kvalitní, že laické a nepoučené uživatele sociálních sítí mohou snadno zmást. Občas se při generování opět aktivuje etický filtr, ale ten jde poměrně snadno obejít.

Inovované modely rovněž umožňují tvořit grafiku všeho druhu (včetně **politických karikatur**), zlepšila se také jejich schopnost vkládat do obrázků vlastní texty, na vyšší úrovni je mimo jiného třeba tvorba pojmových/mentálních map. To může samozřejmě svádět k tomu, aby političní marketéři aktivně AI v kampaních používali - je to rychlé, snadné, s minimálními náklady.

Výše uvedené karikatury vytvořily generátory obrázků od OpenAI.

Schopnost generovat deep fake videa takto snadno klade zvýšené nároky na mediální gramotnost uživatelů internetu - především pak uživatelů sociálních sítí, po kterých se tyto produkty AI masově šíří.

Pro E-Bezpečí
Kamil Kopecký

P. S. Další ukázky deep fake fotografií generovaných AI najdete na mém profilu: https://facebook.com/kopeckyk.