

# Nová metoda šifrování využívá obsah generovaný umělou inteligencí ke skrytí informací na očích

[interestingengineering.com/innovation/new-steganographic-encryption-method-developed](https://interestingengineering.com/innovation/new-steganographic-encryption-method-developed)

8. března 2023



S růstem ChatGPT a dalšího generativního obsahu AI online může být nezamýšlenou výhodou bezpečnější digitální komunikace.

Na předtiskovém serveru arXive byl právě zveřejněn nový šifrovací algoritmus, který popisuje novou steganografickou techniku, která se opírá o obrázky generované umělou inteligencí a skrytý obrázek v něm zakódovaný způsobem, který skrývá skutečnost, že se dokonce něco skrývá.

Viz také

Steganografie není nová myšlenka, ale stávající steganografické techniky zanechávají ve své distribuci informací výmluvné artefakty, které lze detekovat, což pozorovatele vede k tomu, že se v obsahu něco skrývá.

S obsahem generovaným umělou inteligencí , jako jsou obrázky, však nový algoritmus používá techniku zvanou spojení minimální entropie, aby maximalizoval překrytí mezi distribucí informací neškodného obsahu a obsahem, který chceme zakódovat, aby mezi nimi nebyl žádný statistický rozdíl. dvě distribuce.

Algoritmus můžete v podstatě použít ke generování obsahu AI, který dokonale maskuje informace, které se snažíte skrýt, a vzhledem k nárůstu obsahu AI online by takový obsah – jako snímky DALL-E 2 – sám o sobě nebyl příčinou. pro podezření. Zakódované informace jsou však snadno dostupné, pokud máte klíč nebo šifru pro informace, které chcete z obrázku extrahovat.

"Hlavním přínosem práce je ukázka hlubokého spojení mezi problémem zvaným propojení minimální entropie a dokonale bezpečnou steganografií," uvedl v prohlášení spoluautor Samuel Sokota z Carnegie Mellon University's Machine Learning Department . "Využitím tohoto spojení představujeme novou rodinu steganografických algoritmů, které mají dokonalé záruky zabezpečení."

A co víc, nový algoritmus také vykazuje až o 40 % lepší efektivitu při kódování informací, takže i když není zaručena zvýšená úroveň zabezpečení, algoritmus se může stále ukázat jako užitečný pro své výhody komprese dat a ukládání.

Nejoblíbenější

"Naši metodu lze aplikovat na jakýkoli software, který automaticky generuje obsah, například pravděpodobnostní video filtry nebo generátory memů," řekl spoluautor Dr. Christian Schroeder de Witt z Oxford's Department of Engineering Science. "To by mohlo být velmi cenné například pro novináře a humanitární pracovníky v zemích, kde je šifrování nezákonné. Uživatelé však stále musí postupovat

opatrně, protože jakákoli šifrovací technika může být zranitelná vůči útokům postranním kanálem, jako je detekce steganografie." aplikace v telefonu uživatele."

## **Vzestup obsahu generovaného umělou inteligencí vytváří dokonalou kouřovou clonu pro skrytí citlivých informací**

---

Výzkumníci požádali o patent na algoritmus a již zveřejnili neefektivní implementaci algoritmu na populárním úložišti kódu Github jako otevřený zdrojový kód.

I když algoritmus pravděpodobně získá patentovou ochranu, vědci uvedli, že mají v úmyslu zpřístupnit algoritmus volně prostřednictvím licence třetí strany pro nekomerční a odpovědné použití, jako jsou akademické a humanitární účely.

Takové šifrovací schéma je důležité zejména v místech, kde by šifrování mohlo být nezákonné nebo zakázané, aby se omezilo svobodné vyjadřování nebo potlačoval nesouhlas, a jak se vyrábí a šíří stále více obsahu generovaného umělou inteligencí, bude čím dál nemožnější vůbec vědět, kde hledat. pro zakódované informace, čímž je zabezpečení nové metody mnohem silnější.

1. [Domov](#)
2. [Inovace](#)

 ZOBRAZIT KOMENTÁŘ ( 0 ) 