

СТЕГАНОГРАФИЯ И ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ В МЕДИИТЕ: ВЪЗМОЖНОСТИ И ПРЕДИЗВИКАТЕЛСТВА В ЕПОХАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

Елена Симова, Христо Мичев

Университет по библиотекознание и информационни технологии

Резюме: Настоящият доклад разглежда взаимодействието между стеганографията, медиите и интелектуалната собственост, като акцентира върху възможностите и предизвикателствата на стеганографските техники, подпомогнати от изкуствения интелект и подкрепени с примери. Методологията включва анализ на приложенията на стеганографията за защита на авторските права чрез невидими водни знаци, както и рисковете, свързани със скриването на незаконно съдържание. Резултатите подчертават необходимостта от балансиран подход, който да насърчава иновациите в медийната индустрия, като същевременно гарантира етични и сигурни практики.

Ключови думи: стеганография; изкуствен интелект; медии; етика; интелектуална собственост

ВЪВЕДЕНИЕ

Стеганографията като метод за скрито предаване на информация намира все по-широко приложение в съвременните медии, особено с напредъка на изкуствения интелект. В контекста на интелектуалната собственост тази технология предлага иновативни решения за защита на авторските права чрез вграждане на невидими водни знаци в дигитални носители, като изображения, видео- и аудиофайлове. Въпреки това потенциалът ѝ не е еднозначен – същите техники могат да бъдат използвани за скриване на незаконно или неетично съдържание, което повдига въпроси относно сигурността и регулацията в медийната индустрия.

Настоящото изследване разглежда именно този двойствен характер на стеганографията. От една страна, тя предоставя мощни инструменти за защита и управление на цифрови права, а от друга – поражда предизвикателства, свързани с етиката и злоупотребата с технологиите. В този контекст възниква необходимостта от балансиран подход, който да съчетава иновациите с отговорност и регулаторни механизми.

В този доклад анализираме основните принципи на стеганографията, нейните приложения в медийната индустрия и възможните регулаторни решения, които могат да минимизират рисковете, без да ограничават креативността и технологичния напредък.

Основни принципи на стеганографията в медиите

Стеганографията е техника за скриване на информация в дигитални носители – изображения, видео- и аудиофайлове, без това да бъде видимо за човешкото око или стандартните методи за обработка на данни (Kien 2014). Прилагането ѝ в медиите се основава на няколко ключови принципа:

Вграждане на информация без значителна промяна.

Основният принцип на стеганографията е използването на малки, почти незабележими модификации в медийния файл, които не променят неговото възприемане от потребителите. Фотографите променят в авторските си изображения най-маловажните битове на цветовите пиксели (Least Significant Bit – LSB) за вграждане на воден знак, без това да се отрази на визуалното качество. Чрез минимални промени в най-маловажните битове на пикселите се вграждат тайни данни, без да се нарушава визуалното качество на изображението. LSB се използва в компресионни алгоритми като JPEG, за да се намали размерът на файла. Въпреки че това води до известна загуба на качество, разликата обикновено не е забележима за човешкото око (Stoilov 2021).

При цифровото аудио LSB играе роля при определянето на качеството на звука. Ако LSB е твърде груб (с голям интервал между стойностите), може да се появи квантов шум, което да доведе до загуба на аудиодетайли. По-фина настройка на LSB подобрява звуковото качество, намалява изкривяванията и не влияе на възприеманото качество на звука.

При видеофайловете LSB се използва както за стеганография, така и за водни знаци, които могат да удостоверят авторството на съдържанието. Тъй като видеото съдържа множество кадри, информацията може да бъде разпределена равномерно в различни кадри, което затруднява разкриването ѝ.

В цифровото водно маркиране за защита на авторските права LSB се прилага чрез модифициране на най-маловажните битове в изображения, аудио или видео, като се вгражда невидима информация за собствеността върху съдържанието, без това да се отрази върху качеството му.

Използване на алгоритми за разпределение на информацията

За да бъде трудно откриваема, скритата информация се разпределя равномерно или в предварително зададени зони на медийния файл. Например в изображенията може да се използват техники като Least Significant Bit (LSB) стеганография, при която данните се внедряват в най-маловажните битове на пикселите, без да се променя видимо изображението.

Във видеоклипове данни могат да се скриват само в определени кадри, като например в ключови кадри (I-frames) или в по-малко значими кадри (B-frames), за да останат незабележими при стандартно възпроизвеждане. Друга техника е промяна в амплитудата или фазата на аудиосигналите във видеото, което позволява вмъкване на информация, която не може да бъде доловена от човешкото ухо.

При аудиофайловете разпределението на данни може да се извършва чрез манипулация на честотни спектри, например чрез фазова кодировка или ехо модификация.

В документите, например PDF или Word файлове, алгоритмите могат да разпределят скрит текст в бели пространства, в метаданни или в специфични символи с неразличими разлики, като минимални промени в шрифтовете или разстоянията между буквите.

Тези методи правят извличането на скритата информация без точния алгоритъм или ключ изключително трудно, което ги прави ценни за осигуряване на дискретна комуникация и защита на чувствителни данни.

Комбинация със защита чрез криптография

Често стеганографските техники се съчетават с криптографски методи, за да осигурят по-високо ниво на сигурност. В дигиталните водни знаци информацията за авторските права може първо да бъде криптирана и след това вградена в медийното съдържание, за да бъде достъпна само за притежателите на съответния ключ. Например в аудиофайлове музикалните лейбъли могат да внедрят криптиран воден знак, който съдържа идентификатор на притежателя на правата. Дори ако файлът бъде копиран или променен, вградената информация остава и може да бъде разкрита само чрез използване на правилния дешифриращ алгоритъм. Друг пример е в цифровата фотография – професионални фотографии и медийни агенции често използват техники като разширена стеганография за вграждане на криптирана информация в метаданните на снимките. Така дори при редактиране на изображението собствеността може да бъде удостоверена чрез извличане и дешифриране на водния знак.

Извличане на вградената информация чрез изкуствен интелект

Извличането на вградения код трябва да се извършва чрез специализирани алгоритми, които осигуряват пълно възстановяване на оригиналната информация. Пример за това е използването на алгоритми за корекция на грешки, които позволяват възстановяване на данни дори при частична загуба на информация, например при компресия или обработка на медийните файлове. Един такъв алгоритъм може да бъде ВСН код, който осигурява възстановяване на данни при малки промени или загуба на части от стеганографския носител.

Приложения на стеганографията в медийната индустрия

Стеганографията играе ключова роля в съвременната медийна индустрия, като предоставя инструменти за защита на авторското право, сигурност на информацията и проследяване на съдържание. Техниките за скрито вграждане на данни се прилагат в различни медийни формати – текст, изображения, аудио и видео. Цифровите водни знаци са едно от най-широко използваните приложения на стеганографията в медиите. Те позволяват идентифицирането на собствеността върху съдържанието и проследяването на нелегалното му разпространение. Cox, Miller и др. в книгата си „Digital Watermarking and Steganography“ описват методите за скрито вграждане на водни знаци в изображения и видео с цел защита на авторски права (Cox 2025). Книгата разглежда принципите, приложенията и технологиите, свързани с цифровото водно маркиране (digital watermarking) и стеганографията. Структурирана е така, че да представи основни концепции, математически модели, методи за внедряване и сигурност, както и анализ на различни техники за откриване на скрито съдържание. Те дефинират разликите между стеганография и водни знаци. Докато водните знаци се използват за защита на авторските права и удостоверяване на съдържание, стеганографията цели скриване на информация в дигитални носители, така че да остане незабелязана.

Резултати от изследването

Стеганографията е ефективен инструмент за защита на авторски права и творците могат да удостоверяват авторството си и да проследяват нелегалното разпространение на съдържание. Съчетаването на стеганография и криптография повишава сигурността и се създават многослойни защиты, особено в чувствителни сфери като журналистика, правителствени комуникации и музикална индустрия. Има доказателства за използване на стеганография при заобикаляне на цензурата в репресивни режими. Исторически и съвременни примери потвърждават реалното приложение на скрити комуникации. Налице са сериозни етични и правни предизвикателства, защото стеганографията може да бъде използвана и за скриване на незаконно съдържание, за манипулиране на общественото мнение и за нарушаване на правата на потребителите, което налага нуждата от регулация и етични насоки.

ИЗВОДИ

Изкуственият интелект (ИИ) и медиите са тема с широки възможности за изследване. В последните години ИИ преобразява медийната индустрия по няколко начина: от създаването на съдържание и автоматизираното редактиране до персонализирането на потребителския опит. ИИ може да генерира текстове, новини и дори визуални материали. Алгоритми за обработка на естествен език като GPT-3 могат да пишат статии, сценарии и други видове текст. Автоматизирани системи редактират видеоклипове и аудиоматериали, както и следят социални медии за тенденции и новини. Но ИИ повдига и въпроси относно етиката, прозрачността и потенциалните злоупотреби и проблеми, като фалшивите новини и дезинформацията. ИИ и медиите са в постоянно развиващ се процес и бъдещето им е неясно, но безспорно вълнуващо. Благодарение на изкуствения интелект стеганографията – изкуството и науката за скриване на съобщения, намира приложение в медиите. Методът, който позволява вмъкване на скрити съобщения в изображения, видео- и аудиофайлове, се развива и благодарение на изкуствения интелект прави скритата информация още по-трудна за откриване. Медиите използват стеганография за защита на авторските права чрез вградени водни знаци, които са невидими за обикновеното око, но могат да бъдат разпознати от алгоритми. Стеганографията, подкрепена от изкуствения интелект, предлага иновативни методи за сигурност и креативност, но изисква внимание и отговорност при употребата си. Както при ИИ, и в медиите има етични и правни въпроси. Скритата информация може да бъде използвана за злонамерени цели, като например скриване на неетично или незаконно съдържание.

Пресечната точка на стеганографията, медиите и интелектуалната собственост представлява интригуващо поле за изследване, като повдига въпроси относно етиката и сигурността в медийната индустрия. Така взаимодействието между стеганографията и медиите изисква балансиран подход за осигуряване на креативност и иновации, съчетани с отговорност и етика.

ЗАКЛЮЧЕНИЕ

Стеганографията продължава да бъде ключов инструмент в медийната индустрия, като предлага защита на авторското съдържание, сигурна комуникация, маркетингови иновации и борба с фалшификациите. Технологиите за скрито вграждане на информация постоянно се развиват, намирайки все по-широко приложение в цифровата ера. Докладът представя задълбочен анализ на ролята на стеганографията в контекста на съвременните медии, интелектуалната собственост и изкуствения интелект. Изследването подчертава двойствения характер на стеганографските технологии – от една страна, като мощен инструмент за защита на авторски права и конфиденциална комуникация, а от друга, като потенциален вектор за злоупотреба чрез скриване на незаконно или манипулативно съдържание.

Ключов научен принос на доклада е очертаването на пресечната точка между стеганографията и изкуствения интелект. Представени са конкретни приложения, като цифрово водно маркиране, комбиниране с криптографски алгоритми и автоматизирано извличане на скрити данни чрез ИИ. Освен техническите аспекти, докладът разглежда и етичните и правните предизвикателства, свързани с използването на тези технологии в журналистиката, музикалната индустрия и социалните мрежи.

Заключението е, че съществува остра необходимост от балансиран, мултидисциплинарен подход към прилагането на стеганографията – такъв, който да насърчава технологичните иновации, но същевременно да гарантира етичност, прозрачност и защита на правата на участниците в медийната екосистема. Това налага създаване на адекватни регулаторни и етични рамки, както и междусекторно сътрудничество между технологичната, правната и журналистическата общност.

ЛИТЕРАТУРА

БЪРНСТИЙН, Джейк, 2018. *Големите офшорни афери – Досиетата „Панама“*. София: НСМ – Медиа. 264 стр. ISBN 9789549913651.

КИЕН, Фам Т., 2014. Стеганография. *Българска наука*, бр. 65, с. 172 – 178. Available from: <https://nauka.bg/2014/65/Steganografiq-2014.pdf>.

ОРУЕЛ, Джордж, 2021. *Фермата на животните*. София: Сиела. 152 стр. ISBN 9789542833703.

ФЕЙСБУК се споразумява по делото с Cambridge Analytica. От този скандал започнаха големите проблеми за социалната мрежа. 29 август 2022. ISSN 2682-9606.

© 2001 – 2025 Електронно издание LexNews.bg. [viewed 25.05.2025]. Available from: <https://news.lex.bg/pregled-na-pechata/facebook-%D1%81%D0%B5-%D1%81%D0%BF%D0%BE%D1%80%D0%B0%D0%B7%D1%83%D0%BC%D1%8F-%D0%BF%D0%BE-%D0%B4%D0%B5%D0%BB%D0%BE%D1%82%D0%BE-%D1%81-cambridge-analytica/>.

REFERENCES

- BARNSTIYN, Dzheyk, 2018. *Golemite ofshorni aferi - Dosietata „Panama“*. Sofia: NSM – Media. 264 str. ISBN 9789549913651.
- COPYRIGHT. Infringement. The official site of IFPI. © London 2025. [viewed 25.05.2025]. Available from: <https://www.ifpi.org>.
- COX, Ingemar J.; MILLER, Matthew L.; BLOOM, Jeffrey A.; FRIDRICH, Jessica; KALKER, Ton. *Digital watermarking and steganography*. Morgan Kaufmann publications. United States of America, p. 567. ISBN 978-0-12-372585-1. [viewed 15.05.2025]. Available from: <https://stb.iau.ir/faculty/file/download/course/1619191468-digital-watermarking-and-steganography-2nd-ed.pdf>.
- FACEBOOK se sporazumya po deloto s Cambridge Analytica. Ot tozi skandal zapochnaha golemite problemi za sotsialnata mreza. 29 avgust 2022. Elektronno izdanie LexNews. Bg. ISSN 2682-9606. © 2001 – 2025 LexNews.bg. [viewed 15.05.2025]. Available from: <https://news.lex.bg/pregled-na-pechata/facebook-%D1%81%D0%B5-%D1%81%D0%BF%D0%BE%D1%80%D0%B0%D0%B7%D1%83%D0%BC%D1%8F-%D0%BF%D0%BE-%D0%B4%D0%B5%D0%BB%D0%BE%D1%82%D0%BE-%D1%81-cambridge-analytica/>.
- FRIDRICH, Jessica, 2014. *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press. 466 p. ISBN 9781139192903. DOI: <https://doi.org/10.1017/CBO9781139192903>.
- HANDELSBLATT: Evropa pretarpya strategichesko porazhenie v ukrainskia konflikt. Glasove.com © 2025. [viewed 15.05.2025]. Available from: <https://glasove.com/komentari/handelsblatt-evropa-pretarpya-strategichesko-porazhenie-v-ukrainskiya-konflikt>.
- KIEN, Fam T., 2014. Steganografia. *Balgarska nauka*, br. 65, s. 172 – 178. [viewed 15.05.2025]. Available from: <https://nauka.bg/2014/65/Steganografiq-2014.pdf>.
- LOU, Der-Chyuan; LIU, Jiang-Lung, 2002. *Steganographic Method for Secure Communications*. Department of Electrical Engineering Chung Cheng Institute of Technology National Defense University Tahsi, Taoyuan 33509, Taiwan. [viewed 15.05.2025]. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S0167404802005151>.
- ORUEL, Dzhordzh, 2021. *Fermata na zhivotnite*. Sofia: Siela, 152 s. ISBN 9789542833703.
- PAPA FRANTSISK: Vse po-trevozhni stsenarii za Ukrayna zastrashavat mira. 23.02.2022. © Actualno.com 2003 – 2025. [viewed 15.05.2025]. Available from: https://www.actualno.com/europe/papa-francisk-vse-po-trevojni-scenarii-za-ukrajna-zastrashavat-mira-news_1715260.html.
- STOILOV, Petar; HRISTOV, Georgi; ZAHARIEV, Plamen, 2021. Analysis of the least significant bit substitution algorithm for image steganography. *Proceedings of University of Ruse „Angel Kanchev“*, vol. 60, book 3.2. pp. 207 – 213. [viewed 15.05.2025]. Available from: <https://conf.uni-ruse.bg/bg/docs/cp21/3.2/3.2-28.pdf>.
- TRAD, Ruslan, 2025. Voynata na Rusia v Ukrayna e i konflikt za kontrol varhu resursi.

Polis – zhurnal za politika i sigurnost. 1.02.2025 © Polis.bg. [viewed 15.05.2025]. Available from: <https://polis.bg/articles/konflikt-za-kontrol>.

XIAO, Chang; ZHANG, Cheng; ZHENG, Changxi, 2018. *FontCode: Hiding information in plain text, unobtrusively and across file types*. Website of Columbia University in the City of New York. [viewed 15.05.2025]. Available from: <https://www.cs.columbia.edu/2018/fontcode-hiding-information-in-plain-text-unobtrusively-and-across-file-types/>.

STEGANOGRAPHY AND INTELLECTUAL PROPERTY IN MEDIA: OPPORTUNITIES AND CHALLENGES IN THE AGE OF ARTIFICIAL INTELLIGENCE

Abstract: *This paper examines the interplay between steganography, media and intellectual property, focusing on the opportunities and challenges of steganographic techniques, aided by artificial intelligence, and supported by examples. The methodology includes an analysis of steganography applications for copyright protection through invisible watermarks, as well as the risks associated with hiding illegal content. The results highlight the need for a balanced approach that encourages innovation in the media industry while ensuring ethical and secure practices.*

Keywords: *steganography; artificial intelligence; media; ethics*

Elena Simova, PhD Candidate

Scientific Advisor: Prof. Tereza Trencheva, PhD & Prof. DSc Stoyan Denchev
University of Library Studies and Information Technologies
Sofia, Bulgaria
E-mail: e.simova@unibit.bg

Hristo Michev, Student

Scientific Advisor: Prof. Tereza Trencheva, PhD
University of Library Studies and Information Technologies
Sofia, Bulgaria
E-mail: 137nsr@unibit.bg