УДК 004.056.5

Я. О. Безпалько
Є. В. Радченко

МЕТОДИ ПРИХОВАНОГО МАРКУВАННЯ ГРАФІКИ ДЛЯ ЗАПОБІГАННЯ ПІРАТСТВУ

Вінницький національний технічний університет

Анотація

Досліджено методи впровадження прихованих цифрових водяних знаків у графічні об'єкти з метою захисту авторських прав та запобігання несанкціонованому копіюванню контенту.

Ключові слова: інформаційна безпека, цифрові водяні знаки, стеганографія, авторське право, захист графіки.

Abstract

The methods of embedding hidden digital watermarks in graphic objects for the purpose of protecting copyright and preventing unauthorized copying of content are investigated.

Keywords*:* information security, digital watermarks, steganography, copyright, graphics protection.

Вступ

У сучасних умовах глобалізації цифрового простору проблема несанкціонованого розповсюдження графічного контенту набуває критичного значення. З розвитком соціальних мереж, штучного інтелекту та стокових платформ, швидкість копіювання візуальних активів стала майже миттєвою. Традиційні методи захисту, такі як відкриті водяні знаки, часто виявляються неефективними. Вони не лише псують естетичне сприйняття твору, що критично для професійного дизайну та цифрового мистецтва, а й легко видаляються сучасними редакторами на базі нейромереж. Саме тому розробка та впровадження методів, що дозволяють зберігати ідентифікаційні дані всередині самої структури файлу без візуальних змін, є одним із найважливіших завдань кібербезпеки в креативних індустріях.

Метою даної роботи є аналіз та обґрунтування методів прихованого маркування (цифрових водяних знаків), що інтегруються безпосередньо у структуру графічного файлу. Основне завдання полягає у дослідженні балансу між стійкістю маркування до технічних модифікацій та збереженням високої візуальної якості продукту для підтвердження його автентичності.

Об'єкт дослідження – процес захисту авторських прав на графічний контент у цифровому середовищі.

Предмет дослідження – стеганографічні методи та алгоритми прихованого маркування зображень, що забезпечують стійкість до технічних модифікацій.

Результати дослідження

Під час проведення дослідження було проаналізовано ефективність застосування стеганографічних алгоритмів для захисту інтелектуальної власності. На сьогодні в науковій спільноті виділяють два основні підходи до прихованого маркування: просторовий та частотний. Кожен із них має унікальні механізми інтеграції даних та різні показники стійкості до модифікацій.

1. Просторовий метод

Суть просторового методу полягає у безпосередній маніпуляції значеннями пікселів зображення. Найбільш розповсюдженим прикладом є алгоритм LSB (Least Significant Bit**)** — метод заміни найменш значущих бітів.

Метод полягає у заміні найменш значущих бітів пікселів ідентифікаційним кодом. Оскільки зміна молодшого біта змінює інтенсивність кольору лише на 1/256 частину, людське око не здатне помітити

різницю. Це забезпечує візуальну непомітність (PSNR понад 45 дБ), що важливо для професійної графіки. Проте він є надзвичайно вразливим до найменшого стиснення, зміни формату (наприклад, перетворення з PNG у JPEG) або базових фільтрів, оскільки будь-яка трансформація пікселів руйнує вбудовану інформацію.

2. Частотний метод

Частотний підхід вважається найбільш перспективним (зокрема у галузі цифрової криміналістики). Він базується на зміні не самих пікселів, а їхніх спектральних характеристик після застосування математичних перетворень,

Цей метод передбачає вбудовування даних у коефіцієнти спектральних перетворень. Використання вейвлет-алгоритмів та психовізуальних моделей дозволяє інтегрувати мітку в низькочастотні області. Такий підхід робить маркування стійким до агресивного редагування, кадрування та типових методів зачистки авторства. Зокрема, вейвлет-алгоритми дозволяють зберегти водяний знак навіть після JPEG-стиснення зі зниженням обсягу файлу до 70%.

Порівнюючи ці підходи, можна сказати, що просторовий метод є простішим у реалізації та забезпечує чудову візуальну якість, проте він втрачає дані при будь-якій спробі змінити формат або стиснути файл. Частотний метод, навпаки, складніший математично, але набагато надійніший, оскільки дозволяє маркуванню «виживати» навіть після агресивного редагування та сильного стиснення зображення. Таким чином, якщо просторовий метод підходить для швидких завдань, то частотний є кращим вибором для серйозного захисту авторських прав у цифровому середовищі.

Висновки

Приховане маркування – це як сукупність технічних обмежень, так і стратегічний актив майбутнього фахівця. Вона формує внутрішній механізм контролю за поширенням продукту, що допомагає орієнтуватися у складних правових ситуаціях. Проведене дослідження підтверджує, що сучасні алгоритми здатні забезпечити надійний захист без шкоди для естетики контенту. Тільки через впровадження сучасних стандартів безпеки можна виховати покоління розробників, здатних до сталого захисту власних цифрових здобутків. Подальші зусилля мають бути спрямовані на автоматизацію процесу виявлення вкраденого контенту в глобальній мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Тема 8. Методи стеганографічного захисту інформації лекція 10 // Сайт StudFiles [Електронний ресурс] URL: https://studfile.net/preview/8875886/page:28/
2. Хорошко В. О., Азаров О. Д. Основи інформаційної безпеки : підручник. Вінниця : ВДТУ, 2020. 256 с.
3. Закон України «Про авторське право і суміжні права» від 01.12.2022 № 2811-IX. // Відомості Верховної Ради України. 2023. № 10.
4. Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression technique. // Сайт IEEE Xplore [Електронний ресурс] URL: https://ieeexplore.ieee.org/document/7509352

Безпалько Яна Олегівна – студентка групи 1БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yanabezpalko1259@gmail.com

Науковий керівник: ***Радченко Євгеній Валентинович*** *– доцент кафедри Захисту інформації, ВНТУ, eradchenko@vntu.edu.ua*

Bezpalko Yana Olegivna – student in group 1BS-24b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: yanabezpalko1259@gmail.com

Scientific supervisor: ***Radchenko Yevgeniy Valentynovych*** *– assistant professor in the Department of Information Security, VNTU, eradchenko@vntu.edu.ua*