

АНАЛІЗ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНИХ ІГОР

Вінницький національний технічний університет

Анотація

У роботі розглянуто сучасні методи цифрового водяного знаків для захисту комп'ютерних ігор від несанкціонованого використання. Аналізуються різні підходи до вбудовування водяних знаків, їх стійкість до атак та ефективність у збереженні авторських прав. Досліджено особливості застосування водяних знаків у різних цифрових носіях, таких як зображення, відео, 3D-графіка та аудіо. Запропоновано рекомендації щодо вибору необхідного методу на основі типу контенту та бажаного рівня захисту.

Ключові слова: цифрові водяні кібербезпека, захист, комп'ютерні ігри, авторське право, захист контенту.

Abstract

The article considers modern methods of digital watermarking to protect computer games from unauthorized usage. Different approaches of watermarks embedding, their robustness to attacks and efficiency of preserving copyright are analyzed. The features of watermarks using in various digital media, such as images, videos, 3D graphics, and audio are studied. Recommendations are offered for choosing of a method depending on the type of content and the required level of protection.

Key words: digital watermarks, cybersecurity, computer games, copyright, content protection.

Вступ

Розвиток штучного інтелекту, зокрема генеративних моделей, спричинив масове використання ігрових зображень для тренування нейромереж без згоди розробників. Це ставить під загрозу авторські права, сприяє поширенню несанкціонованого контенту та ускладнює контроль за використанням цифрових ресурсів. Цифрові водяні знаки стають ключовим методом захисту графічного контенту, оскільки дозволяють відстежувати витoki, запобігати автоматичному збору візуальної інформації та дозволяють творцям захистити свої ігрові ресурси, контролювати їхнє використання в мережі та протидіяти несанкціонованому використанню в ШІ-моделях. Це сприятиме збереженню інтелектуальної власності та зменшенню ризиків незаконного поширення ігрового контенту.

Метою цього дослідження є покращення захисту контенту комп'ютерних ігор від несанкціонованого використання.

Результати дослідження

Цифровий водяний знак — це використання свого роду маркера, приховано вбудованого в цифровий носій, наприклад аудіо, відео, зображення чи текстуру гри, це дозволяє дізнатися джерело або власника авторських прав [1]. Цей метод використовується для відстеження порушень авторських прав. Існує кілька підходів до їх вбудовування [2, 3].

Найбільш поширеним є метод на основі пікселів. Цей метод передбачає зміну окремих пікселів зображення, наприклад, модифікацію найменш значущих бітів (LSB). Хоча цей підхід є простим у реалізації, він є вразливим до обробки зображень, таких як стиснення або фільтрація, що може призвести до втрати водяного знаку.

Також поширеними є частотні методи. Ці методи вбудовують водяний знак у частотні компоненти зображення, використовуючи перетворення, такі як дискретне косинусне перетворення (DCT) або дискретне вейвлет-перетворення (DWT). Такий підхід забезпечує більшу стійкість до атак та обробки сигналів.

Цікавість також викликають методи розширеного спектру. Ці методи розподіляють інформацію водяного знака по багатьох частотах, що робить його менш помітним та більш стійким до видалення. Вони запозичують принципи з технологій зв'язку з розширеним спектром.

Особливістю підходів на основі моделей є те, що ці методи використовують математичні моделі вихідного файлу для вбудовування водяного знаку, враховуючи особливості зображення.

Статистичні підходи до вбудовування цифрових водяних знаків використовують математичні

властивості вихідного файлу для додавання та пошуку водяних знаків. Він часто використовує спеціальні тести для пошуку водяних знаків.

Рекомендації щодо вибору методів нанесення цифрових водяних знаків залежать від типу носія інформації, його особливостей та вимог до захисту. Різні методи цифрових водяних знаків мають свої переваги та обмеження, що робить їх ефективними для різних типів контенту.

Для зображень і відео найкраще підходять частотні методи та розширений спектр, частотні методи (DCT, DWT, SVD) дозволяють вбудовувати водяні знаки у високочастотні або середньочастотні області зображення/відео. Це робить їх менш помітними для людського ока, але стійкими до стиснення JPEG, змін яскравості та контрасту. Методи розширеного спектру додають слабкий, але розпізнаваний сигнал у весь файл, що підвищує стійкість до атак.

Тоді як для документів ефективними є текстові та стилістичні підходи, текстові методи (свідоме введення граматичних або лексичних змін) дозволяють приховати водяний знак, зберігаючи читабельність документа. Стилiстичні методи (змiна мiжрядкового iнтервалу, шрифтів, розташування слів) важче виявити, але вони зберігають оригінальний зміст тексту.

У 3D-графіці використовуються геометричні водяні знаки, їх можна вбудовувати у координати вершин, нормалей або текстурні координати. Використання топологічних змін або варіацій у формах робить знаки менш вразливими до атак.

А для аудіофайлів – частотні методи та методи розширеного спектру. Частотні методи дозволяють вставити водяний знак у певні частоти, що робить його невидимим для людського слуху, але розпізнаваним для аналізу. Метод розширеного спектру розподіляє інформацію на широкий діапазон частот, роблячи її стійкою до фільтрації та стиснення.

Найефективнішим підходом є гібридні методи, які поєднують просторові, частотні, геометричні та криптографічні техніки. Таке рішення забезпечить: непомітність (просторові методи), стійкість до атак (частотні, розширений спектр), високу точність виявлення (криптографічні методи), захист від змін формату та редагування (геометричні та динамічні методи) [4]. Для захисту цифрових ресурсів, таких як ігрові активи, відео, аудіо чи документи, найкраще використовувати комбінацію частотних, криптографічних і геометричних методів.

Кожен метод обраний через свою ефективність для відповідного типу контенту. Основні фактори вибору – стійкість до атак, збереження якості контенту та прихованість водяного знаку. Інші методи можуть бути менш ефективними через особливості цифрових носіїв.

Висновки

Дослідження цифрових водяних знаків демонструє їхню ефективність у захисті комп'ютерних ігор від несанкціонованого використання, зокрема від витоку контенту та використання в штучних інтелектуальних моделях без дозволу розробників. Запропоновано рекомендації щодо вибору методів вбудовування цифрового водяного знаку залежно від типу контенту. Важливим напрямком подальших досліджень є розробка адаптивних алгоритмів вбудовування цифрового водяного знаку, які зможуть динамічно змінювати параметри вбудовування відповідно до типу контенту та рівня загрози. Таким чином, використання цифрових водяних знаків є важливим інструментом для захисту авторських прав розробників ігор, а подальший розвиток цієї технології сприятиме підвищенню безпеки цифрових ресурсів у сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ScoreDetect. Digital Watermarking Techniques: Benefits and Examples. URL: <https://www.scoredetect.com/blog/posts/digital-watermarking-techniques-benefits-and-examples> (дата звернення: 18.03.2025).
2. GeeksforGeeks. Digital Watermarking and its Types. URL: <https://www.geeksforgeeks.org/digital-watermarking-and-its-types> (дата звернення: 18.03.2025).
3. І. С. Зубко, В. О. Мартовицький, А. В. Пунченко, Д. Д. Карачевцев. Огляд методів нанесення цифрових водяних знаків для захисту зображень. Системи управління, навігації та зв'язку. 2024. № 3. С. 121-125. URL: <https://journals.nupp.edu.ua/sunz/article/download/3457/2878> (дата звернення: 19.03.2025).
4. В. В. Лукічов, Ю. В. Баришев, Н. Р. Кондратенко, В. І. Маліновський. Метод адаптивного багатопланового захисту інформації на основі стеганографії та криптографії Інформаційні технології та комп'ютерна інженерія. Том 58 № 3. 2023. С. 4-11 URL: <https://itce.vntu.edu.ua/index.php/itce/article/view/966> (дата звернення: 19.03.2025).

Діденко Крістіна Валеріївна — студентка групи БКС-21б, факультет захисту інформації, Вінницький національний технічний університет, Вінниця

Науковий керівник: **Баришев Юрій Володимирович** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Didenko Kristina — Faculty of Information Protection, Vinnytsia National Technical University, Vinnytsia

Supervisor: **Baryshev Yurii** — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia