DOI 10.15276/imms.v14.no1-2.45
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 45-55

РОЗРОБКА ПЛАГІНУ ДЛЯ ПРОГРАМИ BLENDER З МЕТОЮ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В 3D МОДЕЛЮВАННІ

А.В. Лозовський, Н.І. Кушніренко, В.О. Назаров, В.В. Подуфалов

Національний університет «Одеська Політехніка»,
1, Шевченка пр., Одеса, 65044, Україна;
email: infsec2011@gmail.com

Робота присвячена аналізу питань, пов'язаних із захистом прав інтелектуальної власності на тривимірні моделі. У сучасному світі 3D-моделювання набуло широкого поширення та застосування в різних галузях, включаючи кіноіндустрію, відеоігри, медицину, архітектуру та виробництво. Швидкий розвиток технологій 3D-друку та цифрових платформ створює нові можливості, але водночас і нові виклики для правовласників. Однією з ключових проблем є поширення незаконного копіювання та використання 3D-моделей, що може призвести до значних фінансових втрат для авторів та компаній, які інвестують у розробку таких моделей. Традиційні правові механізми захисту, такі як авторське право, патенти та товарні знаки, не завжди ефективно працюють у контексті цифрового середовища, де порушення прав може відбуватися миттєво і в глобальному масштабі. У статті розглядаються різні підходи до захисту інтелектуальної власності на 3D-моделі. Зокрема, аналізуються можливості використання цифрових водяних знаків, криптографічних методів та інших технологічних засобів для забезпечення захисту від незаконного копіювання та розповсюдження. Результатом роботи є розроблений плагін для програми Blender, який забезпечує автоматичний захист авторських прав на кінцеві зображення за допомогою накладання цифрових водяних знаків. За допомогою розробленого плагіну автор може непомітно додати свій унікальний код у кінцеве зображення. Також користувач має можливість перевірити авторство завантаженого зображення. Розроблене рішення може знайти широке застосування серед творчих професіоналів.
Ключові слова: захист 3D проектів, цифрові водяні знаки, плагін, інтелектуальна власність, захист авторських прав.

Вступ. Сьогодні, коли технологічні інструменти стають більш доступними та потужними, а цифрові платформи здатні передавати та обробляти складні дані, захист інтелектуальної власності стає особливо важливим. Особливо це стосується галузей, де творчість і технології переплітаються, наприклад, 3D-моделювання.

Це питання особливо актуальне в контексті широкого використання 3D-моделей у відеоіграх, кіноіндустрії, медицині, архітектурному проектуванні та інших сферах. Велика кількість різноманітних об’єктів, які можна створювати та використовувати в цих галузях, створює потенційні можливості для порушення прав інтелектуальної власності [1]. Наприклад, для створення віртуальних світів у відеоіграх або реалістичних сцен у фільмах може знадобитися використання різних моделей і текстур, які можуть бути об’єктами авторського права. У медичній сфері, наприклад, розробка та використання 3D моделей дозволяє точніше планувати операції та лікування, але водночас потребує надійного захисту від несанкціонованого доступу. Архітектори та інженери використовують 3D моделі для візуалізації проектів та уточнення дизайну, але при цьому стикаються з ризиком порушення конфіденційності та крадіжки інтелектуальної власності [1, 2].

Крім того, зі зростанням популярності 3D-друку – методу створення 3D-моделей, зростає ризик незаконного використання чужих творінь у власних цілях. Такі ситуації можуть призвести до серйозних конфліктів між творцями та користувачами, а також до значних втрат, наприклад, фінансових [2].

Невідповідальне ставлення до захисту 3D проектів та інтелектуальної власності може мати серйозні наслідки для галузей, в яких активно використовуються 3D моделі, та для суспільства в цілому. Крім фінансових втрат для компаній і авторів, порушення прав на інтелектуальну власність може призвести до втрати довіри споживачів та зниження конкурентоспроможності на ринку [3]. Без ефективного захисту, потенційні досягнення та переваги від використання 3D технологій можуть бути втрачені.

Розуміння та вирішення проблем захисту інтелектуальної власності в 3D-моделюванні стає надзвичайно важливим завданням для подальшого розвитку цієї галузі. Використання новітніх технологій і розробка спеціалізованих інструментів, таких як плагіни, можуть стати важливими кроками в забезпеченні ефективного правового захисту та сприянні творчості у сфері 3D-моделювання [1].

У цьому контексті розробка плагіна для захисту інтелектуальної власності в 3D-моделюванні стає важливим кроком у забезпеченні безпеки та юридичної прозорості для творців і власників контенту. Плагін на основі стеганографічних алгоритмів може приховувати інформацію про авторські права та вбудовувати її безпосередньо в модель, роблячи її невидимою для неавторизованих користувачів, але легко доступною для правовласника.

Мета і задачі дослідження. Мета роботи полягає в підвищенні рівня захищеності 3D проектів шляхом розробки плагіна для програми Blender, який забезпечує автоматичний захист авторських прав на кінцеві зображення за допомогою накладання цифрових водяних знаків. Для досягнення цієї мети необхідно виконати наступні задачі:

1. Провести аналіз сучасного стану питання захисту 3D проектів, включаючи вразливості систем та потенційні загрози для інтелектуальної власності.

2. Дослідити різноманітні підходи до захисту інтелектуальної власності, включаючи шифрування даних, контроль доступу, водяні знаки та інші методи, а також оцінити їх ефективність та придатність для застосування в галузі 3D моделювання.

3. Розробити програмний продукт, який забезпечує захист інтелектуальної власності в контексті 3D проектів.

Виконання цих задач дозволить досягти поставленої мети підвищення рівня захищеності 3D проектів і забезпечити надійний захист інтелектуальної власності у цифровому середовищі.

Основна частина. Захист інтелектуальної власності в 3D-моделюванні стає все більш актуальним у сучасному світі. В основному це пов'язано з тим, що технології 3D-моделювання стають все більш доступними і потужними. Однак із цим покращенням доступності ризик порушення [2] прав інтелектуальної власності, природно, також зростає. Незахищені проекти стають дієвими мішенями для кіберзлочинців, які можуть їх викрасти або використати для підробок та інших шахрайських дій

Розглянемо більш детально загрози інформаційної безпеки для 3D проектів.

- Видалення або пошкодження даних: Зловмисники можуть здійснювати атаки з метою видалення чи пошкодження 3D моделей чи інших даних проекту. Це може призвести до втрати важливої інформації або навіть неможливості використання проекту.

- Зміна даних: Іншою загрозою є можливість несанкціонованої зміни даних у 3D проекті. Зловмисники можуть внести зміни, які призведуть до порушення цілісності проекту або навіть втрати його цінності.

- Втрата контроля над проектом: Якщо зловмисники отримають доступ до проекту і впровадять зміни або видаляють дані, це може призвести до втрати контролю над проектом та його подальшого використання [3, 4].

- Фінансові втрати: Негативний вплив на проект також може мати фінансові наслідки. Наприклад, якщо проект стає непридатним через атаки з боку зловмисників, це може призвести до втрати інвестицій або навіть до фінансових збитків.

- Порушення авторських прав в сфері 3D проектів може мати серйозні наслідки для творців інтелектуальної власності та їх проектів. Ось деякі з основних аспектів порушення авторських прав:

1) Несанкціоноване копіювання та використання: Зловмисники можуть копіювати та використовувати 3D проекти без дозволу їхніх авторів, що призводить до порушення авторських прав. Це може стати причиною фінансових втрат для творців та зниження їхнього контролю над власною творчістю.
2) Недозволене використання в комерційних цілях: Іншою загрозою є неприпустиме використання 3D проектів у комерційних цілях без згоди авторів. Це може призвести до втрати прибутку та порушення прав власності.
3) Втрата конфіденційності: Якщо 3D проекти стають доступними для несанкціонованого використання, це може призвести до втрати конфіденційної інформації або секретів, які можуть бути включені в проект..
4) Підробка та зміна авторства: Зловмисники можуть намагатися підробити авторство 3D проектів або змінити авторську інформацію для власних цілей. Це може призвести до плутанини щодо справжнього автора та порушення його прав [4].

- Соціальна інженерія є одним з найбільш вразливих аспектів безпеки у сфері 3D проектів. Це метод атаки, при якому зловмисник використовує маніпуляцію людьми з метою отримання конфіденційної інформації або доступу до системи. Деякі з прикладів атак, які використовують соціальну інженерію у сфері 3D проектів, включають:

1) Фішингові атаки: Зловмисники можуть використовувати фішингові електронні листи або повідомлення для отримання конфіденційної інформації від користувачів, такої як паролі або доступ до облікових записів, що може призвести до несанкціонованого доступу до 3D проектів.
2) Соціальні інженери: Зловмисники можуть намагатися встановити довіру з користувачем, щоб отримати доступ до його проектів або конфіденційної інформації.

Для захисту від соціальної інженерії важливо навчати користувачів розпізнавати підозрілі ситуації та надавати їм інструменти та інформацію про безпеку та захист даних. Також важливо використовувати технічні засоби захисту, такі як двофакторна аутентифікація та обмеження доступу до конфіденційної інформації.

Заходи захисту відповідають на загрози та вразливості, що існують у сфері 3D проектів. Нижче наведено деякі ключові заходи захисту, які можуть бути використані для забезпечення безпеки та захисту цих проектів:

- Використання шифрування даних забезпечує конфіденційність та цілісність інформації, що передається або зберігається у системі. Застосування шифрування дозволяє захистити 3D проекти від несанкціонованого доступу та перегляду.

- Контроль доступу: Встановлення багаторівневого контролю доступу дозволяє обмежити доступ до 3D проектів лише авторизованим користувачам. Це запобігає несанкціонованому використанню або редагуванню даних.

- Використання водяних знаків та електронних підписів [4, 5] допомагає підтвердити автентичність та походження 3D моделей та проектів, а також захистити їх від незаконного копіювання чи внесення змін.

- Резервне копіювання даних дозволяє запобігти втраті інформації в разі виявлення атаки або випадкового видалення файлів.

- Освіта та навчання користувачів щодо безпеки в Інтернеті, розпізнавання загроз та правил безпеки є важливим кроком для запобігання соціальній інженерії та інших видів атак.

- Проведення регулярного аудиту системи безпеки дозволяє виявляти потенційні вразливості та ризики, що можуть бути використані зловмисниками для атак.

- Встановлення та підтримка актуального антивірусного та антишпигунського програмного забезпечення допомагає виявляти та блокувати шкідливі програми та загрози для безпеки.

Застосування цих заходів захисту допомагає забезпечити надійний та ефективний захист 3D проектів від потенційних загроз та атак, зберігаючи конфіденційність та цілісність даних.

Розглянемо більш детально питання захисту інтелектуальної власності та авторських прав, як складової. На сьогоднішній день існує безліч методів та технік захисту інтелектуальної власності, спрямованих на попередження незаконного використання та копіювання контенту. При розгляді захисту інтелектуальної власності у галузі 3D моделювання важливо розуміти і вивчати існуючі підходи та їхні переваги та недоліки.

Одним із найпоширеніших підходів до захисту інтелектуальної власності є використання технологій DRM (Digital Rights Management). DRM – це набір технологій, який дозволяє обмежувати доступ до цифрового контенту та контролювати його використання шляхом застосування різних захисних механізмів, таких як шифрування, цифрові підписи та управління правами доступу [3].

Переваги DRM:

- Захист інтелектуальної власності: DRM допомагає запобігти несанкціонованому копіюванню, розповсюдженню та використанню цифрового вмісту, забезпечуючи компенсацію авторам і правовласникам за їхню роботу.

- Гарантія доходу: Обмежуючи неавторизований доступ, DRM гарантує, що лише клієнти, які платять, зможуть отримати доступ до вмісту, таким чином максимізуючи дохід для творців і розповсюджувачів вмісту.

- Контроль над використанням контенту: DRM дозволяє правовласникам контролювати, як їхній вміст використовується, розповсюджується та ділиться. Вони можуть установлювати обмеження на копіювання, друк і спільний доступ.

- Запобігання піратству: DRM є ефективним інструментом боротьби з цифровим піратством, яке може суттєво вплинути на доходи та сталість таких галузей, як музика, кіно, програмне забезпечення та видавництво.

- Покращена безпека: Технології DRM часто включають шифрування та безпечні методи автентифікації, які підвищують загальну безпеку цифрового контенту.

Однак, деякі експерти вважають, що DRM може бути неефективним у деяких випадках і навіть призводити до обмежень для законних користувачів [2].

Серед недоліків DRM слід виділити:

- Незручності для користувачів: DRM може ускладнити доступ законних користувачів до вільного використання вмісту, що призводить до розчарування та незадоволення. Обмеження на копіювання, спільний доступ і сумісність пристроїв можуть бути громіздкими.

- Проблеми сумісності: Вміст, захищений DRM, може бути несумісним з усіма пристроями та платформами, що обмежує можливість користувачів отримати доступ до придбаного вмісту на різних пристроях.

- Питання конфіденційності: Деякі системи DRM відстежують поведінку користувачів і шаблони використання, що викликає занепокоєння щодо конфіденційності серед споживачів, які цінують свою цифрову конфіденційність.

- Високі витрати: Впровадження та підтримка систем DRM може бути дорогим для творців і розповсюджувачів контенту. Ці витрати можуть бути перекладені на споживачів у вигляді вищих цін.

- Обмежене добросовісне використання: DRM може обмежувати можливість користувачів брати участь у діях добросовісного використання, таких як створення резервних копій, створення похідних робіт або використання вмісту в освітніх цілях.

- Можливість зловживання: Правовласники можуть зловживати надто обмежувальним режимом DRM для здійснення надмірного контролю над вмістом, пригнічуючи інновації та обмежуючи свободу користувачів використовувати вміст, який вони придбали законним шляхом.

Хоча DRM пропонує значні переваги з точки зору захисту інтелектуальної власності та забезпечення прибутку, він також створює проблеми, пов’язані зі зручністю для користувачів, сумісністю та конфіденційністю.

Поширеним підходом є індивідуальне використання водяних знаків (watermarks) [4] для захисту авторських прав. Водяні знаки є невидимими або малопомітними образами або текстом, які вбудовуються безпосередньо у контент. Вони дозволяють ідентифікувати автора чи власника контенту та встановлювати його права, а також служити попередженням для потенційних порушників. Однак, водяні знаки також можуть бути видалені або змінені недобросовісними користувачами, що зменшує їхню ефективність. Також, вони можуть впливати на якість візуального сприйняття моделі. Крім того, існують технології стеганографії, які дозволяють приховувати інформацію безпосередньо у цифрових файлах, зокрема, у 3D моделях. Ці технології дозволяють вбудовувати інформацію про авторство та власність без зміни зовнішнього вигляду моделі. Стеганографічні методи захисту можуть бути відносно ефективними, оскільки ускладнюють виявлення та видалення захисної інформації без відома автора.

Криптографія є одним із ключових інструментів для захисту авторських прав у цифровому середовищі. Застосування криптографічних методів дозволяє забезпечити конфіденційність, цілісність та автентичність інформації, що важливо для захисту творів інтелектуальної власності [5]. Нижче наведені основні способи використання криптографії для захисту авторських прав:

- Шифрування файлів: Використання шифрування для захисту цифрових файлів (музики, відео, програмного забезпечення, електронних книг) від несанкціонованого доступу та копіювання.
- Шифрування під час передачі: Шифрування даних під час їх передачі через мережу (наприклад, HTTPS для веб-сайтів), що запобігає їх перехопленню та несанкціонованому використанню.
- Аутентифікація авторства: Цифрові підписи забезпечують підтвердження авторства та цілісності твору, що допомагає запобігти його підробці та несанкціонованому використанню.
- Захист документів: Використання цифрових підписів для захисту важливих документів, таких як контракти, угоди про авторські права, забезпечує їх юридичну силу та захист від модифікацій.

Розглядаючи застосування водяних знаків та шифрування до 3D моделей, приходимо до наступних висновків:

- Водяні знаки можуть бути особливо корисними для ідентифікації авторства [1, 4] та власності у випадку об'ємних та складних 3D моделей, де вони можуть бути менш помітними для користувачів, аніж у двомірних зображеннях.
- Шифрування може бути ефективним для захисту конфіденційної інформації та комерційних секретів у випадку, коли доступ до моделі має бути у обмеженого кола осіб.

Враховуючи особливості кожного методу та їх застосування до 3D моделей, оптимальне рішення може полягати в комбінації цих методів для досягнення максимального рівня захисту інтелектуальної власності у галузі 3D моделювання.

Наступним важливим аспектом є правовий захист інтелектуальної власності, що включає в себе авторські права, патенти та інші юридичні механізми. Ці механізми дозволяють власникам захищати свої права на контент та відстежувати порушення через судову систему.

Захист інтелектуальної власності у сфері 3D моделювання має свої власні особливості та складності, які важливо враховувати при розробці та впровадженні методів захисту. Розглянемо деякі з них.

1. Складність структури 3D моделей: 3D моделі можуть бути дуже складними та містити велику кількість деталей, шарів та компонентів. Це може ускладнювати процес захисту, оскільки потрібно забезпечити захист для кожного елементу моделі.

2. Ризик інформаційних втрат [2] під час обміну даними: Передача 3D моделей між користувачами або учасниками проекту може призвести до ризику втрати конфіденційної інформації. Недобросовісні користувачі можуть намагатися витіснити чи використати моделі без дозволу власника.

3. Необхідність збереження якості та продуктивності: При застосуванні методів захисту до 3D моделей важливо зберігати якість та продуктивність моделі. Деякі методи захисту можуть впливати на продуктивність програм та процесів, пов'язаних зі створенням та редагуванням моделей.

4. Потреба у спеціалізованому програмному забезпеченні: Для ефективного захисту 3D моделей може знадобитися використання спеціалізованого програмного забезпечення, яке може бути дорогим або складним у використанні.

Враховуючи ці особливості та складності, важливо розробляти та впроваджувати методи захисту, які забезпечують ефективний рівень захисту, при цьому не погіршуючи продуктивність та якість 3D моделей. Крім того, необхідно враховувати потреби та очікування користувачів у плані зручності та ефективності використання захисних методів.

Плагін для захисту авторських прав у 3D проектах в пакеті Blender. Для розробки 3D проектів, а також реалізації їх захисту важливо обрати потужні та надійні інструменти та програмне забезпечення. На ринку існує багато програм для створення 3D моделей та проектів, серед яких можна виділити такі відомі програми як Autodesk Maya, 3ds Max, Cinema 4D, SolidWorks та Blender.

Autodesk Maya та 3ds Max є досить популярними програмами, які широко використовуються у сфері 3D моделювання та анімації. Вони мають розширений набір інструментів і можливостей, але вимагають певного часу для вивчення та експлуатації.

Cinema 4D також відомий своєю простотою використання та інтуїтивним інтерфейсом, що робить його популярним серед початківців у сфері 3D.

SolidWorks використовується переважно для промислового дизайну та інженерії, але також має інструменти для створення 3D моделей.

Однак, серед усіх цих програм можна виділити Blender. Blender є безкоштовним та відкритим програмним забезпеченням з потужним функціоналом для створення 3D моделей, анімації та рендерингу. Він підтримує всі необхідні функції для реалізації проектів у сфері 3D, включаючи моделювання, текстування, анімацію, композитинг та багато іншого.

Ось декілька переваг Blender [6], які роблять його найкращим вибором для реалізації захисту проектів у сфері 3D:

1. Відкритий код: Blender є безкоштовним та має відкритий вихідний код, що дозволяє розробникам та користувачам перевіряти, адаптувати та вдосконалювати програму з метою забезпечення безпеки.

2. Активна спільнота: Blender має велику активне ком’юніті користувачів та розробників, яка постійно вносить покращення та забезпечує підтримку.

3. Широкі можливості: Blender має широкий набір інструментів для реалізації різноманітних проектів у сфері 3D, що дозволяє створювати складні та захищені моделі.

4. Підтримка різних платформ: Blender підтримує різні операційні системи, що робить його доступним для широкого кола користувачів.

Узагальнюючи, Blender є найкращим вибором для реалізації захисту проектів у сфері 3D завдяки своїй потужній функціональності, відсутності плати за використання

та відкритості вихідного коду, активній спільноті та широким можливостям [7]. Саме на основі цього програмного забезпечення розроблено плагін для захисту авторських прав, запропонований а даній роботі.

У даній роботі пропонується нове розширення для програмного забезпечення Blender. Плагін надає можливість для реєстрації та авторизації користувача. Після чого користувачу присвоюється індивідуальний код. Під час рендеру цей унікальний код непомітно вбудовується у кінцеве зображення за допомогою методу Коха і Жао [8].

Ця розробка також може працювати й у зворотному напрямку. Після авторизації виконавець має можливість дізнатися, чи належить йому авторство того чи іншого завантаженого зображення. Після встановлення розширення в 3D Viewport з'являться нова вкладка Render in safety, в якій стає доступним інтерфейс реєстрації (рис. 1).

Рис.1. Інтерфейс плагіна до авторизації

На початковому екрані з'являється панель реєстрації та авторизації. Дані користувача зберігаються на сервері, тому один акаунт можна зареєструватися лише раз, код прив'язаний лише до однієї пошти й не може збігатися з іншими номерами, тобто він однозначно ідентифікує користувача.

У плагіна є вимоги до паролю, якщо пароль користувача їм не відповідає, то з'являється відповідне повідомлення, яке інформує, що щось не так. Також є і інші повідомлення про помилки, наприклад, для таких випадків: невірні дані для логіна, відсутність імейла в системі і тому подібне (рис. 2).

Приклад повідомлення про помилку:

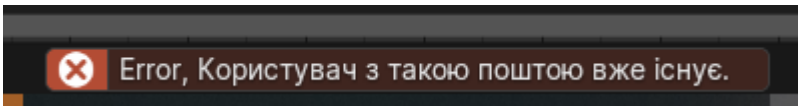

Рис.2. Демонстрація помилки

Спочатку користувачу необхідно зареєструватися, ввівши свою пошту та пароль. Після цього на цю пошту прийде лист з підтвердженням. Після підтвердження з'явиться можливість увійти в обліковій запис і вільно користуватися ним.

Після авторизації з'являться функціонал, наведений на рисунку 3.

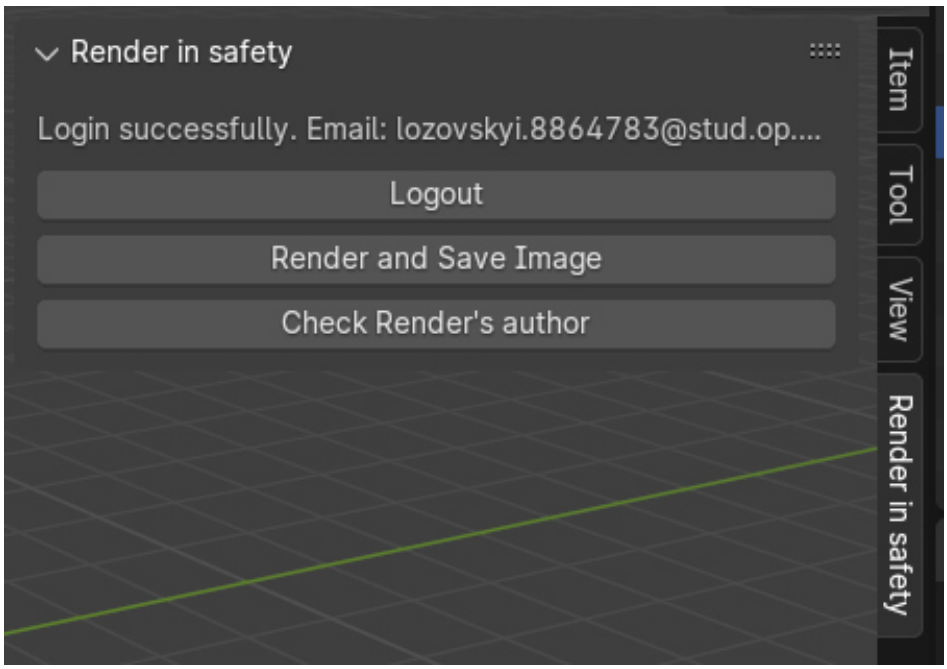

Рис.3. Інтерфейс плагіна після авторизації

Тепер виникла можливість вийти з акаунта, зробити рендер з вбудованим в зображення унікального коду користувача за алгоритмом Коха і Жао та перевірити зображення на збіг коду. Якщо натиснути на Render and Save Image, з'явиться інтерфейс збереження рендеру з назвою за замовчування render.png та можливістю обрати шлях для збереження кінцевого зображення. Після використання плагіна, в робочому просторі буде існувати 2 файли: default – звичайний рендер, render – рендер з вбудовуванням індивідуального коду за допомогою плагіна (рис. 4).

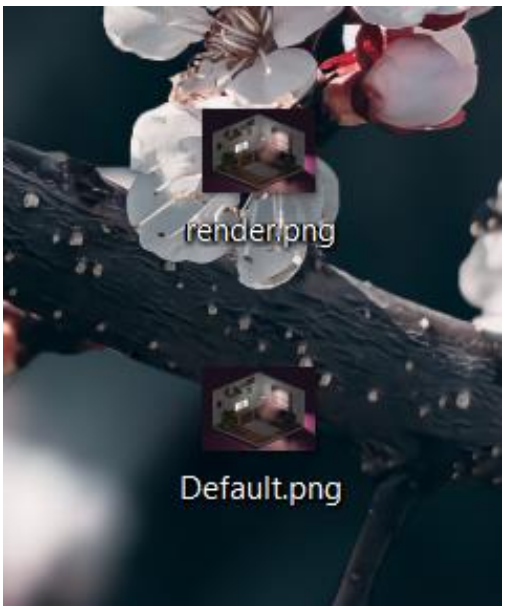

Рис.4. Збережені файли

Через те, що вбудовування інформації в зображення за допомогою алгоритму Коха і Жао абсолютно непомітне неозброєним оком, ми можемо бути впевнені, що різниця між зображеннями відсутня (рис. 5 а та б).

а) звичайне зображення б) зображення з вбудовуванням

Рис. 5. Порівняння звичайного та модифікованого зображення

Далі, за допомогою функціоналу Check render author, перевіримо зображення render.png на авторство (рис. 6). Під час перевірки зображення файлу render.png, плагін видав повідомлення, що «Я автор цього зображення» (рис. 7), а для іншого зображення – ні, бо в нього код власника не вбудовувався.

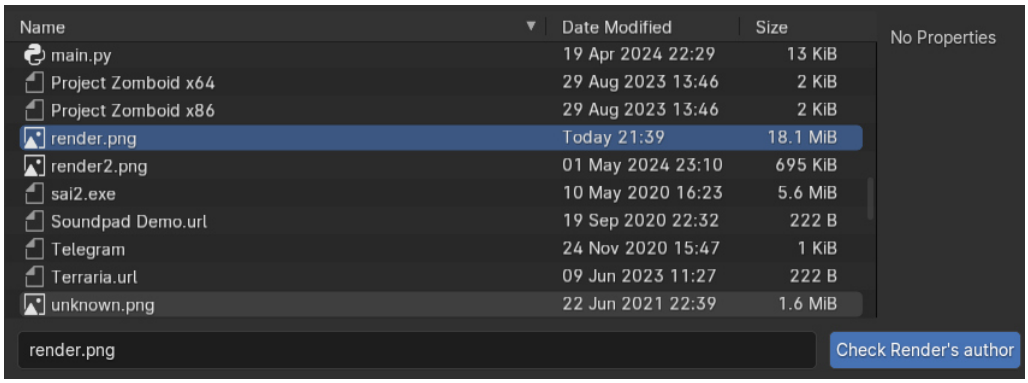

Рис. 6. Перевірка зображення на авторство

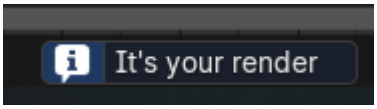

Рис. 7. Повідомлення плагіна, яке підтверджує авторство

Розроблений плагін реалізує кілька важливих функцій, спрямованих на збереження права власності виконавців та запобігання незаконному використанню їхніх робіт, серед яких:

1. Захист права власності виконавця. Однією з ключових функцій є забезпечення надійного захисту авторських прав на зображення, створені в Blender. Плагін дозволяє виконавцям вбудовувати невидимі водяні знаки у свої роботи, які важко видалити або змінити без значного погіршення якості зображення. Це забезпечує впевненість у тому, що права на створені зображення будуть збережені, навіть якщо вони поширюються через Інтернет або інші цифрові канали
2. Інтеграція з Blender. Плагін розроблений для безшовної інтеграції з Blender, що дозволяє користувачам легко використовувати його функції без необхідності переходу на інше програмне забезпечення. Це знижує бар'єри для впровадження технології захисту авторських прав та забезпечує ширше використання плагіна серед творчих професіоналів.

3. Використання методу Коха і Жао. Плагін використовує метод Коха і Жао для вбудовування унікальних кодів у зображення. Цей метод є одним з найбільш ефективних для створення стійких водяних знаків, які витримують різні типи обробки зображень, включаючи стиснення, фільтрацію та зміну формату. Водяні знаки, створені за цим методом, залишаються невидимими для людського ока, але можуть бути легко розпізнані спеціальними алгоритмами, що забезпечує надійний захист авторських прав.

4. Універсальність. Плагін розроблений для роботи в обох напрямках – як для захисту нових зображень, так і для перевірки авторства існуючих. Це дозволяє користувачам не лише захищати свої роботи, але й перевіряти, чи їхні роботи не були незаконно використані іншими особами. Користувач може завантажити будь-яке зображення, і система визначить, чи є воно захищеним, і хто є його автором. Це особливо корисно для виконавців, які хочуть перевірити, чи не були їхні зображення використані без дозволу.

5. Простота використання: Одним з важливих аспектів розробки є створення зручного та інтуїтивно зрозумілого інтерфейсу користувача. Це забезпечує легкість реєстрації, авторизації та використання функцій плагіна без необхідності глибоких технічних знань. Інтерфейс дозволяє користувачам швидко отримати доступ до всіх необхідних функцій та інструментів для захисту їхніх робіт.

Висновки. Розглянуто проблему захисту інтелектуальної власності у контексті 3D моделювання. Проведено аналіз сучасних методів захисту цифрового контенту та їх застосування до тривимірних моделей, а також розробку практичного рішення у вигляді плагіна для програми Blender.

У процесі дослідження виявлено, що захист 3D моделей стає все більш актуальною задачею у зв'язку з розвитком комп'ютерних технологій та зростанням числа цифрових творів. Застосування сучасних методів стеганографії та цифрових водяних знаків, зокрема алгоритм Коха та Жао, демонструють високу ефективність у захисті авторських прав, забезпечуючи стійкість до атак та збереження якості зображення.

Аналіз економічних, юридичних та етичних аспектів підкреслив важливість захисту інтелектуальної власності як для індивідуальних творців, так і для компаній, що інвестують у розробку цифрових продуктів. Практична реалізація розробленого плагіна для Blender підтвердила можливість впровадження передових технологій у повсякденну практику, забезпечуючи автоматизовану охорону інтелектуальної власності.

Плагін реалізовано для платформи Blender, оскільки вона відзначається не лише потужним функціоналом у галузі тривимірного моделювання, але й активною спільнотою розробників та підтримкою відкритого програмного коду. Вибір Blender підкріплюється порівнянням з іншими платформами, що дозволяє зрозуміти переваги використання даного інструменту для реалізації задачі захисту інтелектуальної власності у контексті 3D моделювання. У перспективі планується модифікувати створений плагін, щоб зробити його більш зручним і функціональним. Також буде додано ще декілька методів захисту проектів, що унеможливить несанкціонований доступ до файлів.

Список літератури

1. Watermarking 3D Models: A Comprehensive Guide URL: https://www.researchgate.net/publication/224725105_Watermarking_3D_models.
2. Актуальність методів захисту 3D проектів URL: https://inmad.vntu.edu.ua/portal /static/D8C3236E-DFEF-4A14-87A6-8A71AB8DE59D.pdf
3. Courtney K. K. Digital Rights Management: The Librarian's Guide. Rowman & Littlefield Publishers. 2016.
4. Кулик М. Дослідження сучасних алгоритмів побудови цифрових водяних знаків для відео-контенту. URL: https://ela.kpi.ua/server/api/core/bitstreams/9d614fb3-27e3-4059-8392-3f0d76f32b1b/content

5. Реута Г. Забезпечення цілісності даних з використанням цифрових підписів і сертифікатів. URL: https://ela.kpi.ua/server/api/core/bitstreams/04f65f51-8ee4-4e42-a012-02d09585fc45/content
6. Створення доповнення (аддону) для Blender. URL: https://blender3d.com.ua/sozdaniye-dopolneniya-addona-dlya-blender/
7. Create your first Blender add-on. URL: https://community.osarch.org/discussion/759/blender-create-your-first-blender-add-on
8. Rubel A.S, Fedorov A. Detection of Hidden Data Embedded by the Koch and Zhao Method. *International conference on advanced information and communication technologies*. *Lviv, Ukraine* . 2015. P. 147-148.

DEVELOPMENT OF A PLUGIN FOR BLENDER TO PROTECT INTELLECTUAL PROPERTY IN 3D MODELING

A. Lozovskyi, N. Kushnirenko, V. Nazarov, V. Podufalov

National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine;
email: infsec2011@gmail.com

This work is dedicated to the analysis of issues related to the protection of intellectual property rights in three-dimensional models. In the modern world, 3D modeling has gained wide popularity and application in various fields, including the film industry, video games, medicine, architecture, and manufacturing. The rapid development of 3D printing technologies and digital platforms creates new opportunities but also new challenges for rights holders. One of the key issues is the proliferation of illegal copying and use of 3D models, which can lead to significant financial losses for authors and companies investing in the development of such models. Traditional legal mechanisms of protection such as copyright, patents, and trademarks do not always effectively operate in the digital environment where rights violations can occur instantaneously and on a global scale. The article discusses various approaches to protecting intellectual property in 3D models. Specifically, it analyzes the possibilities of using digital watermarks, cryptographic methods, and other technological means to safeguard against illegal copying and distribution. The outcome of the work is a developed plugin for the Blender software, which provides automatic protection of copyrights on final images by applying digital watermarks. Using the developed plugin, an author can invisibly embed their unique code into the final image. Additionally, users can verify the authorship of uploaded images. This solution can find broad application among creative professionals.
Keywords: protection of 3D projects, digital watermarks, plugin, intellectual property, copyright protection.