УДК 004.9 **doi: 10.26906/SUNZ.2024.3.101**

О. О. Галицька, Н. М Бологова, Д. О. Кібірєв, О. В. Скиба

Харківський національний університет радіоелектроніки, Харків, Україна

ОГЛЯД ПІДХОДІВ ДО ЗАХИСТУ ТРИВИМІРНИХ МОДЕЛЕЙ ВІД НЕСАНКЦІОНОВАНОГО РОЗПОВСЮДЖЕННЯ

Анотація. Стаття присвячена огляду сучасних підходів до захисту тривимірних (3D) моделей від несанкціонованого розповсюдження. У зв'язку з розвитком технологій тривимірного моделювання та широким використанням 3D моделей у різних галузях, питання захисту інтелектуальної власності набуває особливої актуальності. Розглянуто основні методи захисту, включаючи криптографічні техніки, цифрові водяні знаки, стеганографію та методи машинного навчання. Проведено аналіз переваг та недоліків кожного підходу, а також їх ефективності в різних контекстах застосування. Особлива увага приділена новітнім розробкам у сфері захисту 3D моделей та перспективам їх подальшого розвитку. На основі проведеного аналізу запропоновано рекомендації щодо вибору найбільш оптимальних методів захисту в залежності від специфіки використання тривимірних моделей.

Ключові слова: тривимірні моделі, захист інтелектуальної власності, криптографія, цифрові водяні знаки, стеганографія, машинне навчання, несанкціоноване розповсюдження.

Вступ

Тривимірні графічні моделі знаходять широке застосування в кіно, архітектурі, іграх, віртуальній реальності, автоматизованому проєктуванні (САПР), симуляції органів у медицині, військовій справі та біоінформатиці - і це лише деякі зі безлічі сфер застосування. З появою 3D-телевізорів та доступних високопродуктивних 3D-відеокарт для настільних комп'ютерів, 3D-моделі стають ще більш розповсюдженими. А з перспективою використання 3D-принтерів у побуті ринок створення цифрового 3D-контенту перетворився на багатомільярдну індустрію. Існують веб-сайти [1, 2], які дозволяють художникам завантажувати свої роботи і продавати ці 3D-моделі. Існують пошукові системи [3] для пошуку 3D-моделей, а також низка інструментів для створення таких 3D-моделей, зокрема [4–6]. Однак проєктування та створення високоякісних 3D-графічних моделей вимагає значних навичок та використання спеціалізованого програмного забезпечення та/або обладнання, наприклад, лазерних сканерів. Зважаючи на високий попит і популярність 3D-моделей, а також враховуючи вартість, час і зусилля, необхідні для створення таких моделей, виникає загроза широкого розповсюдження незаконного копіювання 3D-моделей. Водяні знаки - метод, який запобігає нелегальному копіюванню шляхом вставки прихованого повідомлення в 3D-модель.

Методи управління цифровими правами (DRM), засновані на технологіях шифрування, в минулому використовувалися для запобігання копіюванню цифрових мультимедійних матеріалів, які потрібно було розшифровувати і розблоковувати протягом декількох місяців, якщо не тижнів або днів. Алгоритми шифрування не залежать від формату мультимедіа, чи то аудіо, відео, пісні з альбомів, фільмів, електронних книг або 3D-моделей. Численні копії 3D-моделей Шрека (з фільму "Шрек"), 3D-модель Голлума з фільму "Володар перснів" можна знайти в Інтернеті. Голлівуд щорічно втрачає мільйони доларів через піратські фільми, які іноді розповсюджуються ще до того, як вони вийшли в кінотеатрах. Запобігти копіюванню мультимедійних матеріалів не лише важко, але й важко відстежити піратів або походження порушення в ланцюжку дистрибуції. Незважаючи на суворе законодавство навіть в США, яке було прийнято Законом про захист авторських прав у цифрову епоху (DMCA), та судові позови Американської асоціації звукозаписної індустрії (RIAA), незаконне копіювання мультимедійних матеріалів продовжується й досі. Системи DRM намагаються забезпечити антипіратські рамки, які обмежують використання контенту його законним користувачем. Провал DRM, що базується на шифруванні, можна підкреслити тим, що Apple відмовилася від свого FairPlay DRM в iTunes у січні 2009 року [7].

Водяні знаки - це технологія, яка вставляє повідомлення або код у цифровий контент. Ініціатива із захисту цифрової музики (Secure Digital Music Initiative, SDMI), консорціум компаній музичної індустрії, у 2000 році провела змагання, щоб перевірити надійність їхніх технологій нанесення водяних знаків. Едвард Фелтон (Edward Felton) та його команда з Прінстонського та Райсського університетів [8] перемогли всі чотири алгоритми водяних знаків, тим самим довівши, що самі по собі водяні знаки є неефективними. Однак, з 2000 року було проведено значну кількість важливих досліджень. У 2008 році Fox Studios почала використовувати систему водяних знаків на вимогу для автоматичного і безперешкодного вбудовування непомітної інформації в кожен кадр відеоконтенту з метою захисту від піратства. Хоча методи шифрування і водяних знаків, коли вони використовуються окремо, виявилися неефективними, коли вони використовуються разом в рамках DRM, вони можуть стати потужним підходом для виявлення незаконного копіювання. Наприклад, фільм "Люди Ікс: Росомаха" у квітні 2009 року незаконно розповсюджувався з видимими водяними знаками "Rising Sun Pictures" у піринговых мережах (P2P), і врешті-решт було заарештовано особу, яка завантажила цей фільм на сайт megaupload.com [9]. Хоча наявність водяного знаку, очевидно, не сприяла арешту, тим не менш, він дав змогу локалізувати джерело витоку інформації. Для кіностудій стало звичайною практикою додавати водяні знаки до своїх попередніх версій фільмів, щоб відстежити первісного завантажувача.

Стан досліджень у сфері нанесення водяних знаків на 3D-моделі (3D стеганографія) все ще перебуває на початковому етапі порівняно з опублікованими роботами у сфері нанесення водяних знаків на зображення та відео. Однак досвід, отриманий в кіноіндустрії, свідчить про те, що водяні знаки є життєздатною технологією, яка залишиться в тренді і може бути поширена на 3D-моделі. Сьогодні для художників-аматорів не є звичайною практикою вставляти водяні знаки під час продажу свого оригінального 3D-контенту продавцю, і вони довіряють продавцю, що той не порушить права власності художника. Хоча продавці 3D-моделей виплачують художникам роялті за право власності на 3D-моделі, не існує бізнес-моделей для підтримки перерозподілу 3D-моделей, які б захищали інтелектуальні права художників. Небагато роботи було зроблено щодо нанесення декількох водяних знаків для підтримки такої бізнес-моделі розповсюдження через торгових посередників. Таким чином, існує бізнес-потреба в надійних алгоритмах нанесення 3D водяних знаків.

Загальний принцип нанесення цифрових водяних знаків на 3D-моделі

Полігональна сітка (англ. Polygon mesh) — це набір вершин, ребер, та граней, що описують форму багатогранного об'єкта в тривимірній графіці та твердотілому моделюванні. Грані зазвичай складаються з трикутників (сітка з трикутників), чотирикутників, чи інших опуклих многокутників, що спрощує їх рендеринг, хоча можуть використовуватись і загальніші, неопуклі многокутники, чи багатокутники з дірками. Список вершин містить координати у тривимірному просторі кожної вершини моделі, а список граней описує, як вершини з'єднані одна з одною. Список ребер може бути отриманий шляхом обходу списку граней і списку вершин. Рис. 1 є прикладом каркасної сітки.

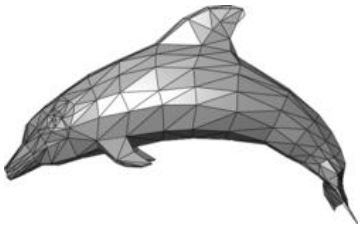

Рис. 1. Приклад трикутної сітки, яка використовується для зображення дельфіна

Технології водяних знаків вбудовують непомітні дані в мультимедійний контент. Приховані дані називаються цифровими водяними знаками і можуть складатися з унікального ідентифікатора користувача, криптографічних ключів, повідомлень про авторські права, умов доступу до контенту, логотипів, зображень, біометричних даних або інформації, що базується на контенті. Процес вбудовування та пошуку цифрових водяних знаків відбувається за допомогою секретного ключа, в якому міститься інформація про те, де і в якій мірі оригінальний контент був змінений для розміщення водяного знаку. Непомітність є важливою вимогою до кожної схеми нанесення цифрових водяних знаків, оскільки водяний знак не повинен спотворювати оригінальний вміст або заважати його використанню за призначенням чи виконанню функцій. Надійність необхідна для того, щоб гарантувати, що звичайна обробка сигналів, геометричні операції та зловмисні модифікації не вплинуть на виявлення або відновлення водяного знаку. Мета полягає в тому, щоб полегшити власникам контенту довести своє право власності шляхом вилучення водяного знаку з піратського носія, а потім подати позов проти порушника. На рис. 2 та 3 показано два компоненти системи захисту водяними знаками: вбудований пристрій та детектор.

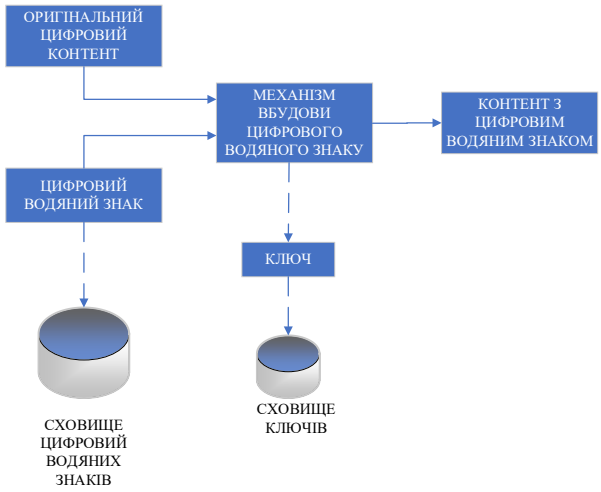

Рис. 2. Технологія нанесення цифрового водяного знаку

Рис. 3. Технологія виявлення цифрового водяного знаку

Процес виявлення водяних знаків може бути несліпим (процес пошуку вимагає доступу до повного оригінального вмісту), напівсліпим (детектору потрібен доступ до деякої побічної інформації та/або цифрового водяного знаку, але не до оригінального вмісту) або сліпим (виявлення виконується без доступу до оригінального вмісту). Несліпі методи виявлення є більш надійними, але непрактичними для використання в системах DRM. Оскільки несліпі методи вимагають, щоб оригінальний контент був доступний детектору, це призводить до необхідності доступу до оригінального контенту з боку програмного забезпечення системи DRM, що створює діру в безпеці системи. Напівсліпі методи є найбільш придатними для

використання в цьому контексті, оскільки сліпі методи не відповідають вимогам надійності.

Алгоритми водяних знаків також можна умовно поділити на перше, друге та третє покоління водяних знаків. Існуючі алгоритми водяного маркування в цій статті були класифіковані на два покоління алгоритмів водяного маркування. Покоління класифіковано на основі можливостей алгоритмів. З кожним наступним поколінням алгоритми водяних знаків мають більші можливості при вбудові, не спричиняючи при цьому помітних спотворень і залишаючись стійкими. На рис. 4 показано класифікацію алгоритмів за поколіннями на основі домену вставки.

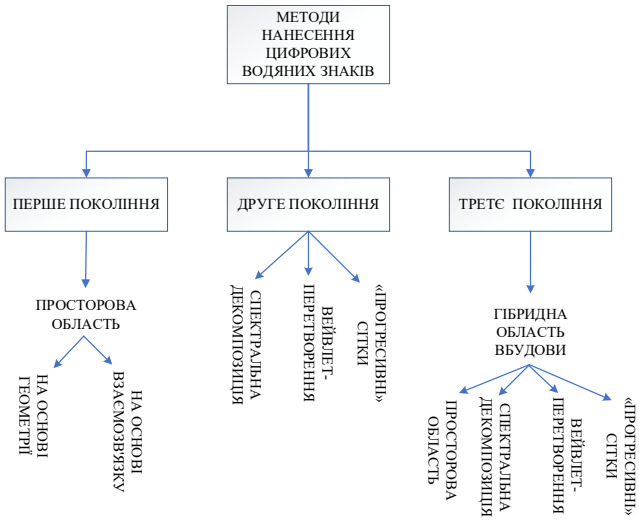

Рис.4. Класифікація алгоритмів за поколіннями на основі домену вставки

Методи третього покоління ґрунтуються на існуючих алгоритмах першого і другого поколінь, а також включають гібридні домени, що дозволяють об'єднувати інформацію з різних доменів. Запропоновані алгоритми третього покоління досліджують використання методів обчислювального інтелекту для вставки водяних знаків високої ємності як у просторову область, так і в область перетворення.

Більш детальний опис алгоритмів нанесення цифрових водяних знаків був висвітлений в огляді методів нанесення 3D водяних знаків [10], тому тут буде представлено лише короткий огляд.

Перше покоління методів нанесення цифрових водяних знаків

Алгоритми першого покоління вставляють водяний знак у просторову область, змінюючи положення вершин або змінюючи зв'язність вершин. На рис. 5 показано схему алгоритмів нанесення водяних знаків першого покоління. Ознаки витягуються з просторової області. Схеми 3D-водного маркування, які вбудовують дані в просторову область, можна розділити на дві основні категорії: схеми водяних знаків, що базуються на зв'язках, і схеми водяних знаків, що базуються на геометрії. Схеми просторових водяних знаків зазвичай менш стійкі до таких атак, як стиснення і додавання шуму. Однак вони витримують атаки обрізання і є менш складними. Алгоритми накладання водяних знаків на основі зв'язності - це алгоритми, які явно використовують зв'язність сітки (деякі автори також називають їх топологічними особливостями). Ці схеми, як правило, базуються на обході всіх трикутників сітки.

Рис. 5. Загальна схема алгоритмів нанесення водяних знаків першого покоління

Для кожного трикутника, що задовольняє функції допустимості, в локальні інваріанти вносяться невеликі модифікації шляхом зміни положення сусідніх точок. Як наслідок, вони є чутливими до модифікацій з додаванням шуму. Серед цього класу схем водяних знаків було запропонували чотири різні алгоритми водяних знаків у першій опублікованій роботі, присвяченій 3D-водяним знакам. Ці схеми відповідно називаються Triangle Similarity Quadruple (TSQ), Tetrahedral Volume Ratio (TVR), Triangle Strip Peeling Sequence (TSPS) та Macro Density Pattern (MDP) [11, 12]. В статті [13] автори вставляють випадковий водяний знак на основі коефіцієнта маскування у вершинах. Коефіцієнт маскування базується на оцінці середньої різниці між позицією та з'єднаними вершинами. Розрядність вставленого водяного знаку становить 100 біт, алгоритм було протестовано на двох моделях з кількістю граней від 3 500 до 5 000 граней. Алгоритм несліпого нанесення водяних знаків виявився стійким до адитивного шуму, стиснення MPEG4 та атак спрощення сітки. Однак стійкість алгоритму була зумовлена багаторазовим вставлянням водяного знаку та використанням кодів з надлишковою стійкістю до помилок, а отже, низькою здатністю до вбудовування.

Алгоритми накладання водяних знаків на основі зв'язності - це алгоритми, які явно використовують зв'язність сітки (деякі автори також називають їх топологічними особливостями). Ці схеми, як правило, базуються на обході всіх трикутників сітки. Для кожного трикутника, що задовольняє функції допустимості, в локальні інваріанти вносяться невеликі модифікації шляхом зміни положення сусідніх точок. Як наслідок, вони є чутливими до модифікацій з додаванням шуму. Серед цього класу схем водяних знаків було запропонували чотири різні алгоритми водяних знаків у першій опублікованій роботі, присвяченій 3D-водяним знакам. Ці схеми відповідно називаються Triangle Similarity Quadruple (TSQ), Tetrahedral Volume Ratio (TVR), Triangle Strip Peeling Sequence (TSPS) та Macro Density Pattern (MDP) [11, 12]. В статті [13] автори вставляють випадковий водяний знак на основі коефіцієнта маскування у вершинах. Коефіцієнт маскування базується на оцінці середньої різниці між позицією та

з'єднаними вершинами. Розрядність вставленого водяного знаку становить 100 біт, алгоритм було протестовано на двох моделях з кількістю граней від 3 500 до 5 000 граней. Алгоритм несліпого нанесення водяних знаків виявився стійким до адитивного шуму, стиснення MPEG4 та атак спрощення сітки. Однак стійкість алгоритму була зумовлена багаторазовим вставлянням водяного знаку та використанням кодів з надлишковою стійкістю до помилок, а отже, низькою здатністю до вбудовування.

Друге покоління методів нанесення цифрових водяних знаків

Порівняно з першим поколінням було зроблено кілька удосконалень, які покращили характеристики з точки зору ємності, невидимості та стійкості водяного знаку. На рис. 6 показано блок-схему алгоритмів водяних знаків другого покоління.

Алгоритми другого покоління використовують різні перетворення для вставки водяного знаку в коефіцієнти області перетворення для підвищення стійкості. У другому поколінні для декомпозиції 3D-моделі до більш низької роздільної здатності використовуються спектральна декомпозиція та методи з декількома роздільними здатностями, такі як вейвлет-перетворення та прогресивні сітки, а водяний знак вставляється в бітовий потік. Таким чином, алгоритми другого покоління дозволяють застосовувати підхід до нанесення водяних знаків до потокових сіток і підвищують надійність алгоритму, вставляючи водяний знак з різною роздільною здатністю. Вейвлет-перетворення дає багаторівневе представлення 3D-моделі. На кожному рівні вейвлет-перетворення в 3D-модель вставляється водяний знак.

Рис. 6. Загальна схема алгоритмів нанесення водяних знаків другого покоління

Таким чином, водяний знак існує навіть при більш низькій роздільній здатності 3D-моделі. Це дає дві основні переваги над традиційними підходами: По-перше, це допомагає захиститися від атаки методом зниженої вибірки. При атаці з використанням низхідної дискретизації зловмисник знижує роздільну здатність 3D-моделі і, таким чином, зменшує її роздільну здатність, щоб видалити водяний знак. Але оскільки водяний знак вставляється навіть у нижчу роздільну здатність 3D-моделі, він не знищується. Таким чином, підхід з використанням декількох роздільних здатностей робить водяний знак стійким до атак. По-друге, оскільки водяний знак додається навіть при низькій роздільній здатності, кількість доданого водяного знаку є більшою, ніж водяний знак, доданий без аналізу з декількома роздільними здатностями. Це збільшує ємність водяного знаку, що підвищує стійкість до таких атак, як згладжування, обрізання та додавання шуму. Обмеженням вейвлет-методів є те, що сітка повинна мати зв'язність від 1 до 4 підрозділів. Вейвлет-перетворення можна застосовувати лише до сіток з напіврегулярною зв'язністю через процес четвертинного поділу/спрощення.

Третє покоління методів нанесення цифрових водяних знаків

Методи нанесення водяних знаків третього покоління базуються на методах першого і другого поколінь, додаючи інтелектуальний рівень оптимізації для вставки водяних знаків високої щільності. Таким чином, ці алгоритми можуть бути розширені для використання на потокових сітках. На рис. 7 показано блок-схему алгоритмів накладання водяних знаків третього покоління.

Рис. 7. Загальна схема алгоритмів нанесення водяних знаків другого покоління

Нанесення водяних знаків можна розглядати як оптимізаційну задачу, де метою є максимізація кількості вершин для нанесення водяних знаків, а також максимізація кількості водяних знаків, які можна вставити, не спричиняючи помітних спотворень. Методи третього покоління також поширюються на алгоритми для крихких водяних знаків. Новизна цієї роботи полягає в оцінці методів обчислювального інтелекту для вирішення проблеми вставки водяних знаків високої щільності як оптимізаційної задачі. Еволюційні методи, такі як генетичні алгоритми, були включені в це покоління. Алгоритми на основі нечіткої логіки та нейронних мереж також входять до цієї нової генерації алгоритмів. Як приклад в роботі [14], в якій автори використовували квадратичне програмування (QP) для обмеженої оптимізації 3D-сіток. Було запропоновано метод на основі гістограми для нанесення водяних знаків на 3D полігональні сіті за допомогою квадратичного програмування для мінімізації середньоквадратичної похибки між вихідною сіткою та сіткою з водяними знаками. Однак цей метод має труднощі в роботі з великими сітками через

обмеження складності існуючих QP-розв'язувачів. Не існує жодної опублікованої роботи, яка б досліджувала використання генетичних алгоритмів, нечіткої логіки або штучних нейронних мереж для нанесення 3D водяних знаків. Однак генетичні алгоритми (ГА), нечітка логіка (НЛ) і штучні нейронні мережі (ШНМ) з частковим успіхом використовувалися для нанесення водяних знаків на зображення і відео.

Висновки

3D стеганографія є відносно новою та перспективною галуззю досліджень, що об'єднує аспекти комп'ютерної графіки, криптографії та інформаційної безпеки. У ході огляду було виявлено кілька ключових напрямів та тенденцій розвитку цієї сфери:

– використання 3D моделей для приховування інформації забезпечує вищий рівень захисту порівняно з традиційними 2D методами. Це обумовлено складністю та багатовимірністю 3D об'єктів, що ускладнює виявлення і витяг прихованих даних;

– існує багато методів 3D стеганографії, таких як методи на основі геометричних властивостей, спектрального аналізу, топологічних змін та методи з використанням текстур і матеріалів. Кожен з методів має свої переваги та недоліки, що робить їх придатними для різних застосувань;

– 3D стеганографія знаходить застосування в багатьох галузях, включаючи захист інтелектуальної власності, безпечний обмін медичними даними, військові технології та розваги. Це свідчить про широку корисність та потенціал для подальших досліджень;

– попри численні переваги, 3D стеганографія стикається з певними технічними викликами, такими як необхідність високих обчислювальних потужностей, складність у створенні стійких до атак методів, а також питання стандартизації та сумісності;

– подальші дослідження в цій сфері можуть зосередитися на розвитку більш стійких алгоритмів стеганографії, інтеграції з іншими технологіями захисту даних, а також на вирішенні проблем сумісності та стандартизації.

Загалом, 3D стеганографія є перспективною технологією, що має потенціал для значного впливу на галузь інформаційної безпеки. Подальші дослідження та розвиток у цій сфері можуть сприяти створенню більш ефективних та безпечних методів захисту даних, а також розширенню можливостей використання 3D технологій у різних галузях.

СПИСОК ЛІТЕРАТУРИ

1. 3D Materials | 3D Textures | Photoreal Textures. URL: https://www.a23d.co/textures
2. TurboSquid: 3D Models for Professionals [Електронний ресурс]. – Режим доступу: https://www.turbosquid.com/
3. Thingiverse [Електронний ресурс]. – Режим доступу: https://www.thingiverse.com/
4. Create massive worlds and high-quality designs. URL: https://www.autodesk.com/products/3dmax/overview?term=1-YEAR
5. Kuchuk, H., Kovalenko, A., Ibrahim, B.F. and Ruban, I. (2019), "Adaptive compression method for video information", International Journal of Advanced Trends in Computer Science and Engineering, vol. 8(1), pp. 66–69, doi: http://dx.doi.org/10.30534/ijatcse/2019/1181.22019
6. ZBrush [Електронний ресурс]. – Режим доступу: https://www.maxon.net/en/zbrush
7. FairPlay DRM – 5 Things to Know About DRM Technology [Електронний ресурс]. – Режим доступу: https://pallycon.com/blog/5-things-you-need-to-know-about-multi-drm-technology-part-3/
8. Reading Between the Lines: Lessons from the SDMI Challenge. S.A. Craver, M. Wu, B. Liu, A. Stubblefield, and E. W. Felten. Proc. of 10th USENIX Security Symposium, 2001. URL: https://www.usenix.org/legacy/events/sec01/craver.pdf
9. FBI makes arrest in 'Wolverine' uploading case. URL: https://www.cnet.com/culture/fbi-makes-arrest-in-wolverine-uploading-case/
10. Beugnon, S., Itier, V., & Puech, W. (2022). 3D Watermarking. Multimedia Security 1: Authentication and Data Hiding, 219.
11. Semenov, S., Mozhaiev, O., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Yu., Yevstrat, D., Chyrva, Yu. & Kuchuk, H. (2022), "Devising a procedure for defining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples", Eastern-European Journal of Enterprise Technologies, 2022, 6 (4(120)), pp. 40–49, doi: https://doi.org/10.15587/1729-4061.2022.269128
12. A. G. Bors, "Watermarking mesh-based representations of 3-D objects using local moments," in IEEE Transactions on Image Processing, vol. 15, no. 3, pp. 687-701, March 2006, doi: 10.1109/TIP.2005.863116
13. Wang, K., Lavoué, G., Denis, F., Baskurt, A. (2007). Three-Dimensional Meshes Watermarking: Review and Attack-Centric Investigation. Lecture Notes in Computer Science, vol 4567. Springer, Berlin, https://doi.org/10.1007/978-3-540-77370-2_4
14. Narendra, M., Valarmathi, M.L. & Anbarasi, L.J. Watermarking techniques for three-dimensional (3D) mesh models: a survey. Multimedia Systems 28, 623–641 (2022). https://doi.org/10.1007/s00530-021-00860-z

Received (Надійшла) 10.04.2024
Accepted for publication (Прийнята до друку) 19.06.2024

Review of approaches to protecting 3D models from unauthorized distribution

O. Galitska, N. Bolohova, D. Kibirev, O. Skiba

Abstract. The article is devoted to a review of modern approaches to protecting three-dimensional (3D) models from unauthorized distribution. In connection with the development of three-dimensional modeling technologies and the widespread use of 3D models in various industries, the issue of intellectual property protection is of particular relevance. Basic security methods are covered, including cryptographic techniques, digital watermarks, steganography and machine learning methods. The advantages and disadvantages of each approach, as well as their effectiveness in different application contexts, are analyzed. Particular attention is paid to the latest developments in the field of protecting 3D models and prospects for further development. Based on the analysis, recommendations are proposed for choosing the most optimal protection methods depending on the specific use of three-dimensional models.

Keywords: 3D models, intellectual property protection, cryptography, digital watermarking, steganography, machine learning, unauthorized distribution.