УДК 004.9 **doi: 10.26906/SUNZ.2024.3.121**

І. С. Зубко, В. О. Мартовицький, А. В. Пунченко, Д. Д. Карачевцев

Харківський національний університет радіоелектроніки, Харків, Україна

ОГЛЯД МЕТОДІВ НАНЕСЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ ДЛЯ ЗАХИСТУ ЗОБРАЖЕНЬ

Анотація. Стаття присвячена огляду методів нанесення цифрових водяних знаків з метою захисту зображень від несанкціонованого використання та копіювання. Об'єктом дослідження є самі методи нанесення цифрових водяних знаків, їхні технічні особливості, ефективність у захисті зображень та вартість впровадження. Автори досліджують різні підходи до вбудовування водяних знаків у зображення та проводять їх порівняльний аналіз з точки зору ефективності, стійкості до атак та вартості впровадження. Стаття детально розглядає різні підходи до вбудовування цифрових водяних знаків у зображення, включаючи методи на основі текстури, частотного домену, та алгоритмічні підходи. Кожен метод аналізується з точки зору його ефективності, стійкості до різних видів атак, таких як ретушування або обрізання, а також вартості впровадження та обслуговування. Наслідком дослідження є комплексне порівняльне обгрунтування методів нанесення водяних знаків, яке допомагає вибрати оптимальний підхід для конкретних потреб захисту зображень у цифровому середовищі. Висновки статті можуть бути корисними для фахівців у сфері цифрових медіа, авторів контенту та розробників програмного забезпечення, які цікавляться збереженням інтелектуальної власності та захистом авторських прав в онлайн-середовищі. Результати огляду допомагають визначити найбільш оптимальні методи для конкретних потреб захисту зображень у цифровому середовищі.

Ключові слова: стеганографія, цифровий водяний знак, захист інформації, зображення.

Вступ

Метод вбудовування цифрового водяного знаку в зображення дає змогу розв'язати проблему права власності, тому дослідження в області стеганографії має ширший спектр застосування, наприклад, захист авторських прав, автентифікація контенту, ідентифікація власника тощо. Яремчук та інші [1], Рубан та інші [2], A Ray та інші [3] представили огляд сучасних методів вбудовування цифрових водяних знаків в зображення, які застосовують у різних галузях. У цій статті представлено мотивацію подальших досліджень, області застосування, вимоги та питання проектування, класифікацію атак і методів вбудовування цифрового водяного знаку. Крім того, визначено деякі проблеми в галузі цифрових водяних знаків для зображень.

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями

У наш час спостерігається зростання кількості різноманітних електронних пристроїв, призначених для зберігання та обробки мультимедійних даних, такі як:

– смартфони;

– планшетні комп'ютери;

– вбудовані мультимедійні програвачі;

– фотоапарати з підтримкою Wi-Fi або Bluetooth;

– портативні жорсткі диски та флеш-накопичувачі;

– електронні книги з можливістю відтворення аудіо та відеофайлів;

– портативні геймінгові консолі;

– умовно-портативні компактні комп'ютери, такі як ноутбуки та нетбуки.

Разом з появою портативних пристроїв також з’являються ефективні методи стиснення мультимедійних даних. Це в сукупності з високошвидкісним інтернет-з'єднання, сприяло поширенню різноманітних програм та сервісів, що базуються на використанні цифрового контенту. Незважаючи на те, що цифрові дані мають багато переваг порівняно з аналоговою версією, їх справжність або право власності на них є найбільшою проблемою. Цифрові мультимедійні дані можна легко дублювати та/або маніпулювати ними, що створює реальну загрозу неправомірного використання мультимедійних даних для власника контенту. Щоб вирішити проблему неправомірного використання мультимедійних даних в мережі Інтернет треба забезпечити надійність і оригінальність переданих мультимедійних даних. У світлі цих негативних факторів, в сучасній ері цифрових технологій стає важливим забезпечити захист мультимедійних даних від незаконного використання.

Сьогодні власники мультимедійного контенту шукають технології, здатні захистити їхні права та убезпечити контент від піратства, несанкціонованого використання, а також ті технології, що дають змогу відстежувати й засуджувати медіапіратів. За останні десятиліття дослідники запропонували різні рішення для захисту мультимедійних даних від несанкціонованого використання. Одним із рішень цієї проблеми є вбудовування невидимих ідентифікаторів у вихідні мультимедійні дані для доказу їхньої приналежності. Цей тип методів називається приховуванням інформації, яке можна розділити на різні підкласи, такі як криптографія, стеганографія та водяні знаки [4–6]. Криптографія - найпоширеніший метод захисту цифрових мультимедійних даних, де мультимедійний контент шифрують перед виданням, а ключ для розшифрування надають тим, хто придбав справжні або легальні копії [7, 8]. Однак криптографія не може допомогти контент-провайдерам контролювати вміст після процесу розшифрування; зловмисник може легко викрасти

справжню або легальну копію, а потім перепродати її або розповсюдити безплатно в загальнодоступній мережі. Стеганографія - це запобігання виявленню зашифрованих даних, які були захищені криптографічними алгоритмами. Однак повідомлення, приховане за допомогою стеганографії, не є надійним. До водяних знаків порівняно з алгоритмами стеганографії висуваються додаткові вимоги щодо стійкості до різних атак, пов'язаних з обробкою сигналу та геометричними перетвореннями. Тому вкрай важливо знайти спосіб захисту цифрового мультимедійного контенту за допомогою більш точного методу, який дав би змогу власникам контенту бути впевненими в розміщенні та поширенні своїх матеріалів в Інтернеті. Таким засобом може стати водяний знак.

Тому виникає завдання з дослідження застосування різних методів водяних знаків.

Результати досліджень

Сфери застосування водяних знаків. Методи вбудовування цифрових водяних знаків мають багато застосувань, а саме:

– захист авторських прав: одним з причин розробки методів нанесення водяних знаків є захист авторських прав. У цьому випадку дані/інформація про авторське право вбудовуються в основний об'єкт без втрати якості [9]. Вбудовані дані перешкоджають іншим сторонам претендувати на право власності на ці дані. Крім того, водяний знак повинен бути відомий лише автору і повинен бути стійким до різних атак;

– прихована комунікація: методи нанесення водяних знаків також можуть використовуватися для прихованої передачі інформації, оскільки різні відомства або уряди встановлюють обмеження на використання шифрування. У цьому випадку люди можуть надсилати свої секретні повідомлення, використовуючи методи вбудови цифрових водяних знаків [10];

– контроль копіювання: ця функція обмежує незаконне копіювання матеріалів, захищених авторським правом, шляхом вбудови цифрового водяного знаку, який не можна копіювати, або обмеження кількості разів копіювання [11]. Наприклад, сьогодні в Інтернеті доступно багато документів, які не можна зберегти та роздрукувати, щоб контролювати незаконне копіювання;

– автентифікація вмісту: крихкий водяний знак може бути вбудований у зображення хоста для перевірки автентичності даних. Крихкий водяний знак вказує на те, чи були дані змінені, а також надає інформацію про те, де ці дані були змінені [12]. Тому ця задача не вимагає надійного водяного знаку, оскільки нам потрібно лише виявити зміни;

– зчитування цифрового відбитка: метод зчитування цифрового відбитка, застосовується власником для того, щоб відстежити джерело нелегальних копій. Для цього власник може вбудовувати різні водяні знаки в кожну копію, яка розповсюджується серед різних клієнтів [13]. Наприклад, унікальні серійні номери присвоюються покупцям і використовуються для ідентифікації покупця;

– моніторинг трансляції: власники захищених авторським правом телепрограм повинні знати про нелегальну трансляцію або рекламу, що транслюється телеканалами в певний час і в певному місці відповідно до умов контракту. Водяні знаки можуть бути вбудовані в будь-який тип даних для трансляції в мережі автоматизованими системами, які здатні контролювати канали розповсюдження, щоб відстежувати контент у потрібний час і в потрібному місці [14];

– медична безпека: останнім часом телемедицина полегшує медичну діагностику, надсилаючи медичні дані/звіт пацієнта через загальнодоступну мережу для подальшого аналізу там, де доступне сучасне медичне обладнання. Це обладнання виробляє велику кількість даних щодня. Отже, необхідно захистити ці важливі дані. Нанесення водяних знаків на медичні зображення є підходящим методом для підвищення безпеки та автентифікації медичних даних, які використовуються для подальшої діагностики та довідок [15]. Вбудовані дата та ім'я пацієнта в медичні зображення можуть бути корисними заходами безпеки;

– індексування: Одним з відомих застосувань цифрових водяних знаків є індексування мультимедійного контенту, такого як фільми, новини, відеопошта, зображення тощо [16]. При цьому коментарі або будь-який тег/жанр вбудовуються у вміст таким чином, щоб ці коментарі або теги використовувалися будь-якою пошуковою системою для пошуку цього вмісту в Інтернеті.

Вимоги та особливості проектування методів вбудови цифрових водяних знаків. Існують різні аспекти проектування та вимоги, пов'язані з будь-яким методом нанесення водяних знаків, такі як прозорість, надійність, пропускна здатність, безпека тощо. Завданням дослідників у галузі нанесення водяних знаків є максимізація всіх цих параметрів для конкретного методу.

Крім того, ці параметри взаємозалежні один від одного, як показано на рис. 1.

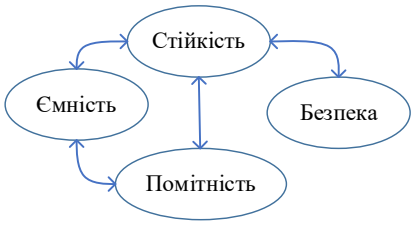

Рис. 1. Взаємна залежність між параметрами проектування

Три параметри, а саме: прозорість, стійкість та ємність обернено пропорційно пов'язані між собою, тобто, якщо прозорість методу водяних знаків зростає, то його стійкість погіршується, і навпаки. Цей взаємозв'язок зображено на рис. 2.

Отже, відносна важливість цих параметрів залежить від конкретного застосування, як зазначено в попередньому розділі. Крім того, деякі програми вимагають більшої надійності у порівнянні з непомітністю.

Рис. 2. Три основні суперечливі аспекти використання водяних знаків

Таким чином, процес розробки методу нанесення водяних знаків включає в себе компроміс між суперечливими параметрами.

Систематизація атак на цифрові водяні знаки. Будь-яку процедуру, яка може знизити результативність методу нанесення водяних знаків, можна назвати атакою. Тестування стійкості та безпеки методу нанесення водяних знаків до атак є настільки ж важливим, як і процес розробки. Атаки не завжди видаляють або знищують водяний знак, але також унеможливлюють його виявлення.

Спотворення, спричинені будь-якими атаками, погіршують функціонування методу нанесення водяних знаків.

Загалом, атаки на цифрові водяні знаки можна розділити на два класи, а саме: ненавмисні та навмисні атаки. Щоб досягти високої надійності виявлення цифрових водяних знаків, процес виявлення повинен бути стійким до змін у даних, спричинених як ненавмисними, так і навмисними атаками. Ненавмисні атаки відбуваються за допомогою операцій обробки сигналів над даними з цифровими водяними знаками, а саме: стиснення, друк, сканування, фільтрація, зашумлення, геометричні перетворення, обрізання тощо. Наприклад, мультимедійні дані зазвичай зберігаються у стислому форматі з втратами для того, щоб використовувати менше пам'яті. Ці алгоритми стиснення відкидають неважливі частини даних. Таке спотворення може призвести до пошкодження даних із вставленими водяними знаками. Це означає, що проста атака полягає в стисненні мультимедійних даних з втратами. Крім того, обертання або масштабування може змінити значення пікселів і знищити дані водяного знаку. Операції обробки сигналу, такі як квантування, декомпресія, повторна вибірка і зменшення кольору, можуть зіпсувати водяний знак. У випадку навмисних атак, людина може цілеспрямовано атакувати вставлені дані цифрового водяного знаку, щоб скопіювати мультимедійні дані. В обох випадках будь-який метод нанесення цифрових водяних знаків повинен бути здатним виявити і витягти водяний знак після атаки. Таксономія різних навмисних і ненавмисних атак на методи нанесення водяних знаків наведена в табл. 1.

Таблиця 1 – **Систематизація атак на водяні знаки**

Атака	Короткий опис
Шум	Будь-який випадковий небажаний сигнал із заданим розподілом, а саме: гауссіан, «сіль і перець», Пуассона.
Фільтрація	Атаки типу фільтрації - це лінійна фільтрація, а саме: фільтрація нижніх/середніх частот, гауссова фільтрація, фільтрація з підвищенням різкості тощо.
Стиснення	Якщо цифровий водяний знак повинен протистояти різним рівням стиснення, зазвичай рекомендується виконувати вбудовування водяного знаку в той самий домен, де відбувається стиснення.
Множинні водяні знаки	Одним з рішень такого типу проблем є включення інформації про час нанесення ЦВЗ сертифікаційним центром
Геометричні атаки	Геометричні атаки спотворюють цифровий водяний знак шляхом просторових змін зображення. Найпоширенішими геометричними атаками є обертання, масштабування тощо.
Обрізання	Це дуже поширена атака, яка обрізає потрібну область від зображення з цифровим водяним знаком.
Атаки на видалення водяних знаків і перешкоди	Мета таких атак - визначити або підмінити водяний знак.
Статистичне узагальнення	Метою таких атак є відновлення основного зображення та/або даних водяного знаку шляхом статистичного дослідження декількох наборів даних з водяними знаками.

Зазначимо, що з розвитком технологій захисту й аналізу цифрових даних, з'являються нові методи захисту від цих атак, а також нові способи їх виявлення та протидії.

Огляд підходів нанесення водяних знаків на зображення. Цифрове зображення може бути представлене/зберігатися або в просторово-часовій області, або в області перетворень. Зображення в просторово-часовій області характеризується пікселями, тоді як зображення в області перетворення описується в термінах його коефіцієнтів перетворення. Іншими словами, представлення зображення в області перетворення розділяє коефіцієнти перетворення на декілька частотних діапазонів. Для перетворення зображення в область перетворення можна використовувати різні доступні методи зворотнього перетворення, а саме: дискретне перетворення Фур'є (DFT), дискретне косинусне перетворення (DCT),

дискретне вейвлет-перетворення (DWT), кероване пірамідальне перетворення (SPT) та інші. Кожен з цих методів перетворення має свої специфічні характеристики та представлення зображення.

Нанесення водяних знаків на цифрові зображення – це процес непомітного вбудовування водяного знаку (у вигляді підпису, випадкової послідовності або якогось зображення) в зображення (носій або обкладинку), який може бути використаний для перевірки автентичності його власника. Отримане в результаті цього процесу зображення називається зображенням з водяним знаком. Методи нанесення водяних знаків можуть виконуватися як у просторовій області, так і в області перетворень. У просторовому методі водяні знаки можуть бути вбудовані в зображення шляхом зміни значень пікселів або значень найменш значущих бітів (LSB). У той час як у методі на основі домену перетворення водяний знак може бути вбудований шляхом модифікації коефіцієнтів домену перетворення. Однак, більш стійкий водяний знак може бути вбудований в область перетворення зображень шляхом модифікації коефіцієнтів області перетворення порівняно з методом водяного маркування зображень на основі просторової області

Метод нанесення водяних знаків на основі просторового доменного підходу, приховує дані водяного знаку дані водяного знаку в значеннях пікселів основного зображення. Цей клас методів вносить незначні незначні зміни в інтенсивності пікселів основного зображення.

Одним з найпоширеніших прикладів такого методу є вбудовування водяного знаку в LSB пікселів зображення. Іншими словами, значна частина низькочастотних компонентів зображення повинна бути модифікована для того, щоб вставити дані водяного знаку надійним і стійким способом. Інший приклад: зображення розбивається на однакові за розміром блоки, і до підблоків додаються певні дані водяного знаку. Непомітність даних водяного знаку досягається на основі постулату, що біти LSB є візуально незначущими. Хоча метод просторових доменних водяних знаків може бути легко реалізований і дуже швидкий, він має багато недоліків. Ці методи дуже чутливі до звичайних операцій обробки сигналів і можуть бути легко порушені та послаблені. Наприклад, стиснення з втратами може повністю знищити дані водяного знаку. Таким чином, просторовий метод нанесення водяних знаків дуже легко зруйнувати за допомогою деяких атак, таких як низькочастотна фільтрація, адитивний шум тощо. Іншими словами, методи просторового доменного водяного маркування зображень не є стійкими до звичайних операцій обробки сигналу на основному зображенні.

Області перетворення зображення – це просто інша форма представлення. Воно не змінює вміст, присутній у зображенні. Методи водяного маркування зображень на основі трансформованих доменів мають багато переваг над методами на основі просторових доменів. Як зазначено в літературі, методи водяного маркування зображень на основі трансформованих доменів є більш стійкими до різних атак на водяні знаки та операцій обробки сигналів, оскільки домен перетворення не використовує вихідне зображення для нанесення даних водяного знаку.

Крім того, водяні знаки на основі домену перетворення розподіляють дані водяного знаку по всій частині основного зображення. Крім того, методи на основі перетворення доменів здатні вбудовувати більше бітів водяного знаку в основне зображення і є більш стійкими до атак.

Проблеми у сфері нанесення водяних знаків на зображення. Незважаючи на те, що було запропоновано багато різноманітних методів вбудови цифрових водяних знаків на зображення, але все ще існують певні проблеми, які потребують вирішення. Однією з головних проблем застосування водяних знаків є досягнення кращого компромісу між надійністю, прозорістю, пропускною здатністю та безпекою. Для того, щоб вирішити вищезгадану проблему (тобто знайти компроміс) для досягнення кращої продуктивності, багато дослідників представили її рішення для цієї проблеми в своїх роботах. Однак для того, щоб виправдати очікування індустрії, потрібні вдосконалення. Розглянемо деякі з найважливіших проблем, пов'язаних з нанесенням водяних знаків на зображення.

Більшість робіт у цій галузі за останнє десятиліття було присвячено захисту кольорових зображень або зображень у відтінках сірого (хост-зображень) шляхом вбудовування водяних знаків у відтінках сірого або бінарних зображень. Для вбудовування бінарного зображення або зображення у відтінках сірого потрібно перетворити його з кольорового, оскільки в мультимедіа використовується кольорові зображення. Однак, існує дуже мало методів, які вбудовують кольорові водяні знаки для захисту зображень [17-19]. З цієї точки зору, існує ще багато можливостей для вдосконалення в галузі водяних знаків зображень для вбудовування кольорового водяного знаку в кольорове основне зображення.

Висновки

За результатами огляду методів нанесення цифрових водяних знаків для захисту зображень можна зробити наступні висновки:

– дослідження показує, що існує широкий спектр методів нанесення водяних знаків, від класичних до складних алгоритмічних підходів;

– кожен метод має свої властивості та обмеження, що варто враховувати при виборі для конкретної задачі;

– важливо оцінювати стійкість кожного методу до потенційних атак, таких як ретушування, обрізання або розмиття зображень;

– вибір методу повинен базуватися на потребах та вимогах користувачів, включаючи зручність використання та якість захисту.

Загалом, огляд методів нанесення цифрових водяних знаків дає можливість краще зрозуміти доступні варіанти та вибрати оптимальний метод для конкретної ситуації або завдання.

СПИСОК ЛІТЕРАТУРИ

1. Ю. Є. Яремчук, В. В. Карпінець, І. С. Зоря, і Д. О. Козак, «ПІДВИЩЕННЯ СТІЙКОСТІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ПОТОКОВИХ ВІДЕОЗАПИСАХ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНОГО ВБУДОВУВАННЯ ЕНЕРГІЇ (DEW)», Вісник ВПІ, вип. 1, с. 55–64, Лют. 2023.
2. Рубан І. В. Інформаційна технологія підтвердження права власності на цифрові зображення / І. В. Рубан, Н. М. Бологова, В. О. Мартовицький // Сучасні інформаційні системи = Advanced Information Systems. – 2022. – Т. 6, № 1. – С. 118-123.
3. Ray, A., Roy, S. Recent trends in image watermarking techniques for copyright protection: a survey. Int J Multimed Info Retr 9, 249–270 (2020). https://doi.org/10.1007/s13735-020-00197-9
4. Guerriero M., Michele G. Adoption, support, and challenges of infrastructure-as-code: Insights from industry. In: 2019 IEEE international conference on software maintenance and evolution (ICSME). IEEE, 2019. p. 580-589.
5. 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
6. Griffin, J., Noussia, K., Nedeva, S., Zervoudakis, S., Lux, J., & McNamara, J. (2023). Artificial Intelligence (AI) and Watermarking to Transform Copyright Arbitration and Dispute Resolution for Three-Dimensional (3D) printing: An Empirical Analysis. Europan Journal of Law and Technology.
7. Бодня, М., ЄсінаМ., & Пономар, В. (2024). Дослідження можливостей застосування стеганографічних та криптографічних алгоритмів для приховування інформації. Комп'ютерні науки та кібербезпека, (2), 43-57
8. Л. Тарасенко. АВТОРСЬКЕ ПРАВО У ЦИФРОВУ ЕПОХУ: ОСНОВНІ ТЕНДЕНЦІЇ І ЗМІНИ. Вісник Львівського університету. Серія юридична. 2022. Випуск 75. С. 61–72.
9. Martovytskyi, Vitalii and Ruban, Igor and Bolohova, Nataliia and Sievierinov, Oleksandr and Zhurylo, Oleg and Permiakov, Oleksandr and Nosyk, Andrii and Nepokrytov, Dmytro and Krylenko, Ivan, Development of Methods for Generation of Digital Watermarks Resistant to Distortion (December 29, 2021). Eastern-European Journal of Enterprise Technologies, 6 (2 (114)), 103–116. doi: https://doi.org/10.15587/1729-4061.2021.246641
10. Рубан И. В. Модель обработки TCP-соединений для стеганографической передачи данных в информационно-телекоммуникационных сетях / И. В. Рубан, А. А. Смирнов // Сучасні інформаційні технології у сфері безпеки та оборони. - 2015. - № 3. - С. 108-112
11. Tarhouni, N., Charfeddine, M. & Ben Amar, C. Novel and Robust Image Watermarking for Copyright Protection and Integrity Control. Circuits Syst Signal Process 39, 5059–5103 (2020). https://doi.org/10.1007/s00034-020-01401-1
12. Kozina, G. L., Savchenko, I., Voskoboynik, V., & Karpukov, L. (2023). Steganographic photo protection system using fragile watermarks. Systems and Technologies, 64(2), 75-81. https://doi.org/10.32782/2521-6643-2022.2-64.10
13. F. Regazzoni, P. Palmieri, F. Smailbegovic, R. Cammarota and I. Polian, "Protecting artificial intelligence IPs: A survey of watermarking and fingerprinting for machine learning," CAAI Trans. on Intellig. Techn., vol. 6, no. 2, pp. 180–191, 2021.
14. Megías, D.; Mazurczyk, W.; Kuribayashi, M. Data Hiding and Its Applications: Digital Watermarking and Steganography. Appl. Sci. 2021, 11, 10928. https://doi.org/10.3390/app112210928
15. Anand, A., Singh, A.K. Watermarking techniques for medical data authentication: a survey. Multimed Tools Appl 80, 30165–30197 (2021). https://doi.org/10.1007/s11042-020-08801-0
16. Fernandez, Pierre, et al. "Active image indexing." arXiv preprint arXiv:2210.10620 (2022). URL: https://arxiv.org/abs/2210.10620
17. Wang H, Yuan Z, Chen S, Su Q. Embedding color watermark image to color host image based on 2D-DCT. Optik (stuttg) 2023;274:170585. https://doi.org/10.1016/j.ijleo.2023.170585.
18. Su, Q., Zhang, X. & Wang, G. An improved watermarking algorithm for color image using Schur decomposition. Soft Comput **24**, 445–460 (2020). https://doi.org/10.1007/s00500-019-03924-5
19. Hu, F., Cao, H., Chen, S. et al. A robust and secure blind color image watermarking scheme based on contourlet transform and Schur decomposition. Vis Comput 39, 4573–4592 (2023). https://doi.org/10.1007/s00371-022-02610-2

Received (Надійшла) 08.04.2024
Accepted for publication (Прийнята до друку) 12.06.2024

Features of automatic deployment of infrastructure as code for cloud services review of digital watermarking methods for image protection

I. Zubko, V. Martovytskyi, A. Punchenko, D. Karachevtsev

Abstract. The article is devoted to the review of digital watermarking methods for protecting images from unauthorised use and copying. The object of the study is the methods of digital watermarking, their technical features, effectiveness in protecting images and the cost of implementation. The authors investigate different approaches to embedding watermarks in images and conduct a comparative analysis of them in terms of efficiency, attack resistance and implementation costs. The paper takes a closer look at various approaches to embedding digital watermarks in images, including texture-based, frequency domain, and algorithmic approaches. Each method is analysed in terms of its effectiveness, resistance to various types of attacks, such as retouching or cropping, as well as implementation and maintenance costs. The result is a comprehensive comparative study of watermarking methods, which helps to choose the best approach for the specific needs of image protection in the digital environment. The conclusions of the article may be useful for digital media professionals, content creators and software developers interested in preserving intellectual property and copyright protection in the online environment. The results of the review help to determine the most optimal methods for the specific needs of image protection in the digital environment.

Keywords: steganography, digital watermark, information security, images.