ПРОБЛЕМИ ЗАСТОСУВАННЯ ВОДЯНИХ ЗНАКІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Іщук О.Р., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Цифровий водяний знак (ЦВЗ) – це інформація пов'язана з певним цифровим об'єктом. Застосування ЦВЗ є одним із методів захисту інформації від різного роду протиправних дій проти контенту. Досить простий метод і досі має шляхи розвитку в наш час, адже знаходяться нові способи його застосування з різними видами даних [1, 2].

Метою доповіді є висвітлення сучасного стану розвитку та застосування ЦВЗ, які є одним з інструментів захисту інформації, аналіз проблем їх застосування в інформаційно-комунікаційних системах.

Цифровий водяний знак вже застосовуються у таких напрямках, а саме нижчеперерахованих:

1. Захист авторських прав. Нанесений знак на різних типах контенту частково або взагалі унеможливлює копіювання інформації. Це є особливо актуальним для зображень, відео та цифрових документів, які легко поширюються мережею.

2. Захист автентичності даних. Водяний знак допомагає перевіряти цілісність даних. Якщо змінити інформацію, то водяний знак буде пошкоджено, що і є сигналом про втручання в структуру даних.

3. Відстеження витоків. Існують методи завдяки яким можна відстежувати джерело інформації шляхом вбудовування унікальних ідентифікаторів для кожного користувача.

4. Автентифікація. Є підходи до застосування певних видів ЦВЗ при автентифікації в системах, наприклад для підтвердження справжності цифрових документів або мультимедійного контенту.

Хоча ЦВЗ вже широко застосовуються у різних напрямках людської діяльності, вони мають ряд недоліків [3]:

– пошкодження візуального контенту. Якщо кажемо про зображення, то нанесенням водяного знаку ми псуємо певну область зображення, а іноді й значну його частину.

– можливість вирізати знак. Розвиток нейронних мереж дозволив створити сервіси по видаленню водяних знаків.

Незважаючи на значний потенціал, впровадження цифрових водяних знаків в ІКС супроводжується низкою проблем.

1. Обмежена стійкість до атак. У реальних умовах функціонування ІКС водяні знаки можуть піддаватися різним впливам: стисненню, фільтрації, масштабуванню або навмисному видаленню. Це знижує їх ефективність як механізму захисту.

2. Компроміс між непомітністю та надійністю. Чим менш помітний водяний знак, тим складніше забезпечити його стійкість до атак, і навпаки.

3. Обчислювальні витрати. Вбудовування та перевірка ЦВЗ потребують додаткових обчислювальних ресурсів, що є критичним для систем реального часу та ресурсно-обмежених пристроїв.

4. Проблеми масштабованості. У великих ІКС (наприклад, хмарних або IoT-системах) ускладнюється управління великою кількістю унікальних водяних знаків.

5. Вразливість до атак із використанням штучного інтелекту. Сучасні методи, зокрема нейронні мережі, дозволяють ефективно видаляти або модифікувати водяні знаки без суттєвої втрати якості контенту.

6. Відсутність уніфікованих стандартів. Наразі не існує єдиного підходу до реалізації ЦВЗ, що ускладнює їх інтеграцію в різні системи.

Паралельно розвитку водяних знаків йде розробка алгоритмів так званих нульових водяних знаків, які усувають недоліки звичайних ЦВЗ. Їх головна відмінність це відсутні візуальної складової в контенті, тобто у випадку застосування нульового водяного знаку в зображенні, ми абсолютно ніяк не змінюємо саме зображення [4]. Такий підхід надає можливість уникати недоліків звичайного нульового знаку, а саме проблем з погіршенням, спотворенням зображень і подібного контенту.

В основі створення нульового водяного знаку лежить підхід по виділенню певних ознак, наприклад коефіцієнтів перетворення (DWT, DCT), ключових точок або інших характеристик. На основі цих даних можна створити унікальний «відбиток», який при поєднанні з інформацією поміщається на зберігання як еталонна модель. При необхідності перевірки цілісності чи інших ознак, ми витягуємо ті самі ознаки із наданого контенту і порівнюємо з еталонним. Якщо ознаки збігаються – можна підтвердити цілісність даних.

Таким чином, цифрові водяні знаки залишаються ефективним інструментом захисту інформації, однак їх використання в ІКС пов’язане з низкою технічних і організаційних викликів. Подальший розвиток, зокрема у напрямі нульових водяних знаків, дозволяє підвищити надійність захисту без впливу на якість контенту.

Список літератури

1. Зубко І.С., Мартовицький В.О. Огляд методів нанесення цифрових водяних знаків для захисту зображень. Системи управління, навігації та звязку. 2024. №3, С. 121-125. DOI: https://doi.org/10.26906/SUNZ.2024.3.121

2. Gvozdov, R., Poddubnyi, V., Sieverinov, O., Buhantsov, A., Vlasov, A., & Sukhoteplyi, V. (2021, October). Method of Biometric Authentication with Digital Watermarks. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 569-571). IEEE.

3. Martovytskyi, V., Ruban, I., Bolohova, N., Sievierinov, O., Zhurylo, O., Permiakov, O., ... & Krylenko, I. (2021). Development of methods for generation of digital watermarks resistant to distortion. Eastern-European Journal of Enterprise Technologies, 6(2), 114.

4. Поддубний В.О. Методи та огляд багатофакторної автентифікації в інформаційно-комунікаційних системах на основі нульових водяних знаків. 2025. URL: https://nure.ua/poddubniy-vadym-oleksandrovich.