УДК 004.932-026.374:004.056.5

Ласкавчук М. А., здобувач вищої освіти,
Загоруйко Л. В., канд. техн. наук, доцент,
доцент кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

ПРИХОВУВАННЯ ДАНИХ У СТАТИЧНИХ ЗОБРАЖЕННЯХ ТА СПОСОБИ ЇХ СПОТВОРЕННЯ

Анотація. У цій роботі розглянуто два види статичних зображень, проведено порівняльний аналіз методів приховування даних, наведено найпростіші типові атаки під час приховування даних у статичних зображеннях.

Ключові слова: статичне зображення, захист інформації, атаки на зображення, спотворення зображення.

Вступ. Приховування даних – це широке поняття, яке в основному визначає будь-яку систему, в якій дані вбудовуються в інші дані. Зазвичай вбудовування може бути візуальним, наприклад, фільм з водяним знаком логотипу, або непомітним, наприклад, прихований зв’язок. Приховування даних визначається як вбудовування непомітних даних в інший цифровий сигнал-носій.

Актуальність. У сучасному світі приховування даних має важливе значення для багатьох застосувань, як-от захист каналів зв’язку, безпека даних та виявлення підробок. Наприклад, водяні знаки використовуються для захисту авторських прав, забезпечуючи автентичність і непідробність інформації. Сучасні методи спотворення зображень також активно застосовуються для захисту даних, що дає змогу запобігти їх несанкціонованому відновленню та використанню, що є актуальним викликом у цифрову епоху.

Статичне зображення – це фіксоване візуальне представлення, яке не змінюється з часом, це один кадр або картинка [1].

а) б)

Рисунок 1 – Кольорове та монохромне зображення

Статичні зображення у відтінках сірого називають монохромними (рис. 1б), або одноколірними. Вони містять лише інформацію про яскравість, без інформації про колір. Кількість бітів, що використовується для кожного пікселя, визначає кількість доступних рівнів яскравості. Типове зображення містить 8 біт/піксель, що дає змогу мати 256 (0–255) різних рівнів яскравості (відтінків сірого). Таке

представлення забезпечує більш ніж адекватну роздільну здатність за яскравістю для систем технічного зору і забезпечує «шумовий запас», даючи приблизно вдвічі більше рівнів сірого. До того ж 8-бітове представлення є типовим через те, що байт, який відповідає 8 бітам даних, є стандартною малою одиницею у світі цифрових технологій [1–2].

Кольорові статичні зображення (рис. 1а) – це такі, що містять інформацію про кольори об'єктів у сцені. На відміну від монохромних, які представляють лише зміни інтенсивності (або яскравості), кольорові зображення містять інформацію про кольори різних точок зображення. У цифровій обробці зображень кольорові зображення зазвичай представляють за допомогою колірної моделі *RGB* [1–2]. Кожен із цих типів статичних зображень може бути використаний для приховування даних.

Приховування даних можна розділити на дві основні області: стеганографію та нанесення водяних знаків. Ці галузі тісно пов'язані між собою, але мають невеликі відмінності, які впливають на алгоритми вбудовування та пов'язані з ними атаки. У системах водяних знаків захищені дані вбудовані безпосередньо у зображення. Типовий метод нанесення водяних знаків на цифрові зображення складається з двох етапів: вбудовування та виявлення [3–4].

У стеганографічних системах захищені дані не пов'язані із зображенням-носієм. Класичним методом, що використовується в області стеганографії зображень, є різниця значень пікселів. Зображення прикриття використовується як канал для прихованої комунікації, наприклад, терористи, які можуть використовувати інтернет-зображення як засіб комунікації. У табл. 1 наведено коротке порівняння між водяними знаками та стеганографією [3–4].

Таблиця 1 – Порівняння методів приховування даних [3–4]

Критерій	**Водяний знак**	**Стеганографія**
Надійність	Активні атаки	Пасивні та активні атаки
Можливість вбудовування	Низький	Високий
Зв'язок між зображенням і повідомленням	Існує	Не існує
Непомітність	Неважливо	Дуже важливо
Шифрування повідомлень	Неважливо	Дуже важливо

Процедури нанесення водяних знаків повинні бути більш стійкими до активних атак, ніж до пасивних, тоді як стеганографія повинна бути стійкою і до пасивних, і до активних атак [3–4].

Атаки на образ носія можуть бути зловмисними і незловмисними. Зловмисні атаки відбуваються, коли метою зловмисника є вплив на процес вилучення повідомлення шляхом фальсифікації зображення-носія. Наприклад, зображення-носій атакується шляхом додавання шуму або обрізання [5].

Атака може бути зловмисною і незловмисною одночасно. Зображення може бути стиснене, наприклад, для публікації або з метою видалення водяного знака [5].

Погіршення якості зображення може бути зловмисним або незловмисним. Сигнал може бути погіршений шумовими перешкодами під час передачі від відправника до одержувача. Зловмисник погіршує зображення, додаючи шум, наприклад, «білий шум» [6].

Висновки. Розглянуто два види статичних зображень та методи приховування даних, зокрема стеганографію та водяні знаки. Описано способи впровадження цих методів приховування даних у статичних зображеннях, а також наведено типові приклади найпростіших атак, які можуть бути зловмисними або незловмисними.

Список використаних джерел

1. Types of Images. URL: https://www.javatpoint.com/dip-types-of-images (дата звернення: 18.10.2024).

2. Grayscale-to-Color: Scalable Fabrication of Custom Multispectral Filter Arrays. URL: https://pubs.acs.org/doi/pdf/10.1021/acsphotonics.9b01196 (19.10.2024).

3. Digital image watermarking method based on DCT and fractal encoding. URL: https://ietresearch.onlinelibrary.wiley.com/doi/pdfdirect/10.1049/iet-ipr.2016.0862 (дата звернення: 19.10.2024).

4. Swain G. Very high capacity image steganography technique using quotient value differencing and LSB substitution. 2019. Vol. 44, № 4, Apr. P. 2995–3004.

5. Adversarial Deep Learning: A Survey on Adversarial Attacks and Defense Mechanisms on Image Classification. URL: https://shorturl.at/zXqIg (дата звернення: 21.10.2024).

6. Noise2Void. Learning Denoising from Single Noisy Images. URL: https://t.ly/CWtN-https://t.ly/CWtN-(дата звернення: 21.10.2024).