

Засіб стеганографічного захисту інформації на основі оцінки візуального маскування

Вінницький національний технічний університет

Анотація

У сучасних умовах цифровізації критично важливим є забезпечення конфіденційності передачі даних у відкритих каналах зв'язку. Традиційні методи стеганографії часто створюють статистичні аномалії, які легко виявляються сучасними нейромережевими аналізаторами, що ставить під загрозу безпеку інформації. Для розв'язання цієї задачі запропоновано інформаційну технологію стеганографічного захисту на основі оцінки візуального маскування та мінімізації статистичних спотворень. Система дозволяє автоматично виявляти текстурні області зображення-контейнера, де вбудовування даних є найменш помітним для людського ока та програмних детекторів. Впровадження запропонованого підходу дозволить підвищити прихованість зв'язку та забезпечити цілісність переданих повідомлень завдяки адаптивному вибору параметрів вбудовування.

Ключові слова: стеганографія, адаптивне вбудовування, візуальне маскування, статистичні аномалії, JPEG, стеганоаналіз.

Abstract

In modern conditions of digitalization, ensuring the confidentiality of data transmission in open communication channels is critically important. Traditional steganography methods often create statistical anomalies that are easily detected by modern neural network analyzers, which endangers information security. To solve this problem, a steganographic information security technology based on the assessment of visual masking and minimization of statistical distortions is proposed. The system allows for the automatic identification of texture areas within the cover image where data embedding is least noticeable to both the human eye and software detectors. The implementation of the proposed approach will increase the stealth of communication and ensure the security of transmitted messages through the adaptive selection of embedding parameters.

Keywords: steganography, adaptive embedding, visual masking, statistical anomalies, JPEG, steganalysis.

Вступ

У сучасних умовах цифровізації захист конфіденційної інформації при її передачі відкритими каналами зв'язку є критично важливим. Традиційні методи стеганографії часто створюють мікроскопічні викривлення, які легко виявляються сучасними нейромережевими аналізаторами, що ставить під загрозу безпеку даних. Основними проблемами є виникнення статистичних аномалій у структурі контейнера та недостатнє врахування особливостей візуального сприйняття.

Для розв'язання цієї задачі запропоновано інформаційну технологію на основі адаптивного вбудовування, що враховує принципи візуального маскування. Система аналізує текстурні області зображення та мінімізує вплив на його статистичні характеристики. Це дозволяє приховати факт передачі повідомлення не лише від людського ока, а й від методів автоматизованого стеганоаналізу. Впровадження такого підходу забезпечить високу стійкість каналу зв'язку та надійний захист інформації в цифровому середовищі.

Основна частина

Головна ідея адаптивної стеганографії полягає в математичному описі впливу зміни кожного пікселя (або коефіцієнта) як скалярного числа (вартості) та мінімізації сумарної вартості цих змін. На відміну від класичних підходів, адаптивна стеганографія обирає для вбудовування області

зображення зі складним «шумом» або текстурою. Саме в таких зонах зміни є найменш помітними як для людського ока (візуальне маскування), так і для статистичних детекторів.

Процес вбудовування базується на присвоєнні кожному елементу зображення «ціни» зміни [1]. Коді синдромної решітки (Syndrome-Trellis Codes, STC) виступають у ролі математичного оптимізатора, що реалізує метод багатопланового вбудовування через побудову динамічної структури – решітки Вітербі. Використання кодів синдромної решітки дозволяє знайти такий шлях модифікації даних, який забезпечує передачу секретних бітів при мінімальній сумарній вартості, уникаючи гладкого тла зображення та концентруючи зміни в областях з високою енергією сигналу. Це дозволяє максимізувати обсяг вбудованих даних за умови збереження мінімального рівня статистичних спотворень контейнера.

Процес реалізації адаптивного вбудовування базується на аналізі характеристик контейнера для визначення найбільш придатних областей приховування даних. Загальну логіку функціонування розробленого стеганографічного засобу, що забезпечує автоматичне виявлення текстурних зон та адаптивний вибір параметрів для одного окремого зображення-контейнера, наведено на рисунку 1 [2].

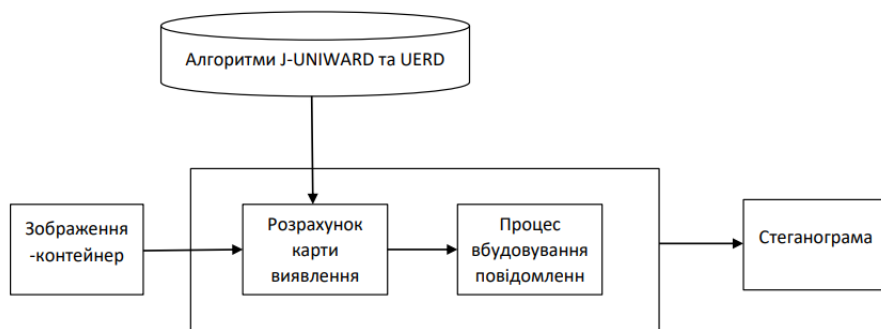


Рисунок 1 – Структурна схема адаптивного вбудовування даних у зображення-контейнер на основі алгоритмів J-UNIWARD та UERD

Оскільки формат JPEG залишається найбільш розповсюдженим стандартом цифрових зображень, розробка стеганографічних засобів для нього зосереджена на маніпуляціях у домені дискретного косинусного перетворення. Основним викликом при роботі з DCT-коефіцієнтами є необхідність збереження цілісності статистичних характеристик, оскільки будь-яке неконтрольоване вбудовування порушує структуру квантування та легко виявляється методами стеганоаналізу.

Одним із найбільш ефективних рішень у цьому напрямку є алгоритм J-UNIWARD, який використовує універсальну функцію спотворення для оцінки придатності кожного коефіцієнта до модифікації. Алгоритм розраховує зміни через аналіз вейвлет-декомпозиції зображення, що дозволяє автоматично спрямовувати дані у складні текстурні області, де енергія сигналу вбудовування маскується природними деталями сцени. Це забезпечує високий рівень візуальної невидимості та ускладнює роботу автоматизованих детекторів [3].

Важливим доповненням є алгоритм UERD (Uniform Embedding Revisited Distortion). На відміну від складних моделей, що вимагають значних обчислювальних ресурсів, UERD базується на принципі рівномірного розподілу енергії вбудовування в межах блоків зображення. Він визначає вартість модифікації кожного коефіцієнта DCT залежно від його величини та позиції в матриці квантування. Пріоритет надається зміні ненульових коефіцієнтів у високочастотних областях, що дозволяє уникнути виникнення артефактів на монотонних ділянках зображення. Такий підхід робить UERD надзвичайно стійким до атак, заснованих на аналізі багатьох статистичних ознак (Rich Models), та дозволяє підтримувати високу швидкість обробки даних [3].

Ефективність обох алгоритмів значно підвищується завдяки інтеграції з кодами синдромної решітки. Ці коди виконують функцію математичного оптимізатора, який обирає таку комбінацію змін у контейнері, що забезпечує передачу необхідного обсягу інформації при мінімально можливій сумарній ціні спотворення. У поєднанні з оцінкою візуального маскування це дозволяє мінімізувати статистичні аномалії та забезпечити надійний захист інформації в умовах активного стеганоаналізу.

Для перевірки стійкості розроблених засобів до статистичного виявлення використовуються глибокі згорткові нейромережі (CNN). Зокрема, архітектура Xu-Net використовує спеціальний шар абсолютних значень (ABS), що дозволяє «підсвічувати» слабкі сліди вбудовування, які зазвичай пригнічуються стандартними CNN. Більш сучасний стандарт – SRNet (Steganalysis Residual Network) – розроблений для виявлення адаптивної стеганографії шляхом мінімізації проблеми «зникаючого градієнта» у дуже глибоких мережах [3].

Для забезпечення високого рівня прихованості розроблена технологія передбачає етап верифікації стійкості через протидію глибоким згортковим нейромережам. Схему процесу тестування та навчання системи на масивах даних представлено на рисунку 2 [2].

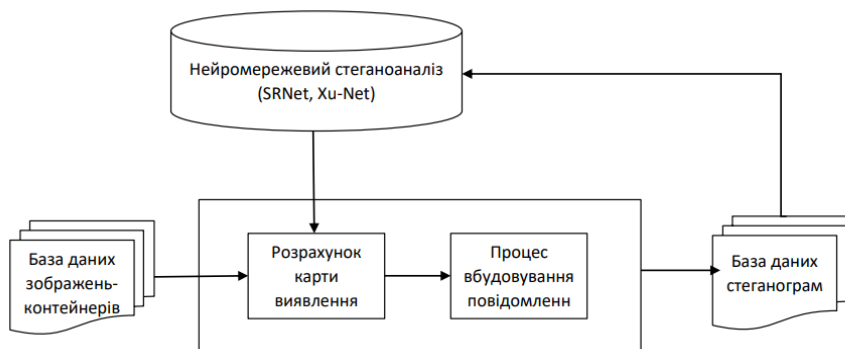


Рисунок 2 – Схема оцінки стійкості стеганографічного засобу до методів автоматизованого стеганоаналізу

Ефективність таких архітектур, як Xu-Net, зумовлена їхньою здатністю фокусуватися на силі зміни сигналу, а не на його знаку, що критично важливо для виявлення адаптивних методів подібних до J-UNIWARD. На відміну від класичних мереж для розпізнавання об'єктів, які намагаються придушити шум для виділення контурів, стеганоаналітичні мережі діють навпаки: вони використовують високочастотну фільтрацію та залишкові зв'язки для посилення ледь помітних аномалій. Загальну схему процесу тестування стійкості стеганографічного засобу до подібних нейромережевих аналізаторів наведено на рис. 2. Це змушує розробників постійно вдосконалювати функції вартості, щоб модифікації контейнера за своїми характеристиками були максимально наближені до природного шуму матриці сенсора або похибок квантування, роблячи їх невідрізними для глибокого навчання.

Висновки

Запропонована інформаційна технологія дозволяє реалізувати надійний стеганографічний канал зв'язку шляхом поєднання психовізуальних моделей маскування та алгоритмів мінімізації статистичних спотворень. Використання методів J-UNIWARD та UERD у комбінації з кодами синдромної решітки забезпечує ефективне вбудовування даних у складні текстурні області зображень. Це не лише гарантує візуальну непомітність повідомлення, а й робить його стійким до сучасних методів стеганоаналізу, зокрема нейромереж Xu-Net та SRNet. Впровадження такого підходу відкриває нові можливості для прихованої передачі критично важливих даних у відкритих цифрових мережах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Filler T., Judas J., Fridrich J. Minimizing embedding impact in steganography using trellis-coded quantization. Proc. SPIE. 2010.
2. General scheme of the Adaptive Steganography by Oracle (ASO) [Електронний ресурс]/ResearchGate. – 2014. – Режим доступу до ресурсу: https://www.researchgate.net/figure/General-scheme-of-the-Adaptive-Steganography-by-Oracle-ASO_fig1_261491484.
3. Deep Residual Network for Steganalysis of Digital Images (SRNet) [Електронний ресурс]. – Режим доступу: <https://www.scribd.com/document/669196111/Deep-Residual-Network-for-Steganalysis-of-Digital-Images>.
4. Xu-Net: Convolutional Neural Networks for Steganalysis [Електронний ресурс]. – Режим доступу: <https://d-nb.info/1217184333/34>.

Платонова Олександра Сергіївна – студентка групи 1БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: [easasha.platonova@gmail.com](mailto: easasha.platonova@gmail.com).

Лукічов Віталій Володимирович – доцент, кафедри захисту інформації, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: [lukichov.vitalyi@vntu.edu.ua](mailto: lukichov.vitalyi@vntu.edu.ua).

Platonova Oleksandra Serhiivna – student of group 1BS-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: [easasha.platonova@gmail.com](mailto: easasha.platonova@gmail.com).

Lukichov Vitaliy Volodymyrovych – associate professor, Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: [lukichov.vitalyi@vntu.edu.ua](mailto: lukichov.vitalyi@vntu.edu.ua).