WayScience

2nd International Scientific and Practical Internet Conference

«Progressive Opportunities and Solutions of Advanced Society»

ISBN 978-617-8293-36-9

WayScience

2nd International Scientific and Practical Internet Conference

«Progressive Opportunities and Solutions of Advanced Society»

ISBN 978-617-8293-36-9

Editorial board of International Electronic Scientific and Practical Journal «WayScience» (ISSN 2664-4819 (Online)

Progressive Opportunities and Solutions of Advanced Society: Proceedings of the 2nd International Scientific and Practical Internet Conference, November 7-8, 2024. FOP Marenichenko V.V., Dnipro, Ukraine, 311 p.

ISBN 978-617-8293-36-9

2nd International Scientific and Practical Internet Conference "Progressive Opportunities and Solutions of Advanced Society" is devoted to research and discussion in various aspects of modern world development.

Topics cover all sections of the International Electronic Scientific and Practical Journal "WayScience", namely:

- public administration sciences;
- philosophical sciences;
- economic sciences;
- historical sciences;
- legal sciences;
- agricultural sciences;
- geographic sciences;
- pedagogical sciences;
- psychological sciences;
- sociological sciences;
- political sciences;
- philological sciences;
- technical sciences;
- medical sciences;
- chemical sciences;
- biological sciences;
- physical and mathematical sciences;
- other professional sciences.

Dnipro, Ukraine – 2024

АНАЛІЗ МЕТОДІВ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Романюк О.Н.
д.т.н., професор кафедри програмного забезпечення
Вінницький національний технічний університет
Нечипорук М.Л.
аспірант кафедри захисту інформації
Вінницький національний технічний університет
Хрипченко В.М.
магістрант кафедри програмного забезпечення
Вінницький національний технічний університет

Стеганографія [1-4] – це метод приховування інформації всередині іншої інформації або носія, що дозволяє передавати секретні дані непомітно.

Метод LSB (Least Significant Bit) використовується для приховування інформації в зображеннях шляхом заміни менш значущих бітів пікселів зображення на біти секретного повідомлення. Це найпростіший спосіб стеганографії зображень.

Кожен піксель у цифровому зображенні зазвичай складається з трьох кольорових каналів: червоного (R), зеленого (G) та синього (B). Кожен канал представлений бітами (наприклад, 8 бітами), де кожен біт визначає інтенсивність кольору. Метод LSB використовує менш значущий біт (останній біт) кожного кольорового компонента для заміни його на біт секретного повідомлення. Через те, що зміни відносяться лише до останнього біту, візуальна різниця в зображенні є мінімальною і практично непомітною для людського ока.

Однак, незважаючи на його простоту, метод LSB має свої недоліки. По-перше, він дуже чутливий до обробки зображень; якщо зображення буде стиснуте або модифіковане, приховані дані можуть бути втрачені. По-друге, оскільки зміни в бітовій структурі досить прості, такі зміни можуть бути виявлені за допомогою статистичного аналізу.

Інший метод – використання частотного перетворення, який застосовується шляхом модифікації частотних компонентів зображення. Цей метод передбачає перетворення зображення у частотну область за допомогою дискретного косинусного перетворення (DCT) або дискретного хвильового перетворення (DWT). Прихована інформація вбудовується у частотні коефіцієнти, що дозволяє передавати дані більш надійно. Це ускладнює виявлення прихованих даних, оскільки вони змішуються з основним сигналом.

Однак реалізація цього методу є складнішою, ніж у випадку з LSB, і вимагає більше обчислювальних ресурсів. Це може обмежити його використання, особливо в реальному часі.

Існують також методи заміни кольорів, коли кольори пікселів змінюються на дуже близькі відтінки. Наприклад, якщо піксель має значення RGB (100, 150, 200), його можна змінити на (100, 151, 200) або (99, 150, 200). Ці зміни можуть бути непомітними для людського ока, але при правильному підході можуть нести приховану інформацію. Обсяги даних, які можна вмістити, є обмеженими, що робить цей метод менш привабливим для великих обсягів інформації.

Методи маскування використовують напівпрозорі зображення або маски для інтеграції даних. Цей підхід дозволяє зберегти високу якість зображення, але його реалізація може бути досить складною і вимагати знань у галузі графіки. Обмеження цього методу полягають у тому, що він може бути менш ефективним для зображень з низьким контрастом або простими зображеннями.

Методи, що використовують межі зображення, дозволяють приховувати дані в краях або контурах пікселів. Цей підхід дозволяє зберегти загальний вигляд зображення, при цьому

надаючи можливість вміщення даних у специфічні ділянки, які можуть бути менш помітними для спостерігача.

Критерії графічної стеганографії використовуються для оцінки ефективності та надійності методів приховування інформації в зображеннях. Один із найважливіших критеріїв – це стійкість до виявлення, що визначає, наскільки складно виявити наявність прихованих даних у зображенні. Метод має бути таким, щоб виявлення прихованої інформації через статистичний або візуальний аналіз було ускладненим.

Якість зображення також є важливим критерієм. Зміни, що відбуваються в результаті стеганографії, повинні бути мінімальними, оскільки помітні зміни можуть привернути увагу. Якість оцінюється за такими параметрами, як співвідношення сигнал/шум (SNR) або середньоквадратична помилка (MSE) між оригінальним і модифікованим зображеннями.

Обсяг прихованої інформації визначає, скільки даних можна вмістити в зображення без значних змін. Чим більше даних можна приховати, тим краще, проте це потрібно збалансувати з якістю зображення та стійкістю до виявлення. Стійкість до обробки є ще одним важливим критерієм, що вказує на здатність методу витримувати обробку зображень, таку як стиснення чи зміна розміру, зберігаючи при цьому приховану інформацію.

Адаптивність методу означає його здатність оптимально використовувати доступні ресурси зображення для приховування даних залежно від типу зображення. Швидкість виконання оцінює, наскільки швидко відбувається процес приховування і вилучення даних, що є важливим у реальному часі. Сумісність методів з різними форматами зображень забезпечує їх універсальність у різних програмах та системах.

Простота реалізації також має велике значення. Методи повинні бути зрозумілими і простими для впровадження, що може зменшити ймовірність помилок. Безпека критично важлива, оскільки визначає, наскільки важко розкрити інформацію, що прихована в зображенні. Висока безпека гарантує, що навіть якщо дані виявлені, їх важко буде прочитати або декодувати.

На додаток до цього, методи стеганографії мають бути масштабованими, тобто здатними обробляти зображення різних розмірів та типів, не втрачаючи своїх характеристик. Ці критерії є ключовими для оцінки та порівняння різних методів графічної стеганографії, допомагаючи вибрати найбільш підходящий метод для конкретних задач і вимог.

Розглянемо поширені методи виявлення, які використовуються для аналізу використання стеганографії LSB.

Аналіз гістограми: зміни LSB можуть вплинути на гістограму кольорів зображення. Аналізуючи гістограму, можна виявити незвичайні піки або нерівномірності, які можуть вказувати на стеганографічні втручання.

Тест χ^2: використовується для визначення, чи відрізняється розподіл значень пікселів від очікуваного нормального розподілу, що може свідчити про втручання в LSB.

Візуальний аналіз: аналіз змінених бітів може виявити аномалії, якщо зміни в LSB були недостатньо дискретні і вплинули на візуальну якість зображення.

Порівняльний аналіз: зміни можуть бути виявлені шляхом порівняння оригінального зображення з підозрілим. Якщо оригінал доступний, аналіз різниці між кожним бітом відповідних пікселів може виявити змінені LSB.

RS-аналіз: базується на властивості, що регулярність пікселів в зображенні змінюється, коли в LSB вносяться зміни. RS-аналіз використовує цю властивість для виявлення стеганографії.

Послідовний аналіз: використовується для виявлення закономірностей у змінених бітах, які можуть вказувати на втручання в послідовність бітів зображення.

Фазове кодування: дозволяє виявити зміни у фазових характеристиках зображення, що можуть виникнути через зміни в LSB.

Кожен із цих методів має свої переваги та недоліки, і вибір методу залежить від специфіки задачі та доступних ресурсів. Часто для більшої точності виявлення використовують комбінацію кількох методів [4].

Важливою є розробка нових і вдосконалених алгоритмів стеганографії, які забезпечують кращу стійкість до виявлення. Це може включати використання машинного навчання для адаптації методів до конкретних типів зображень або форматів даних, що дозволить підвищити ефективність приховування інформації.

Нейронні мережі можуть бути застосовані для автоматичного виявлення оптимальних місць у зображеннях для приховування даних, а також для створення нових методів кодування, які буде важче виявити. Це може призвести до створення більш складних і стійких стеганографічних систем.

Розробка адаптивних методів стеганографії, які враховують характеристики конкретного зображення (наприклад, текстуру або контрастність) для визначення найкращих способів приховування даних, може підвищити якість зображення після вставки даних.

Використання кількох каналів для приховування інформації, таких як комбінація RGB і альфа-каналу, може дозволити зберігати більший обсяг даних без значного впливу на якість зображення.

Інтеграція стеганографії з іншими технологіями, такими як блокчейн для аутентифікації даних або криптографічні методи для додаткового захисту, може підвищити безпеку інформації.

Список літератури:

1. Романюк О.Н. Система стеганографічного захисту повідомлень [Текст] / О.Н. Романюк, К.В. Огородник, В.В. Мартинюк // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2013. – №1. – С. 126–129.

2. Хрипченко В.М., Романюк О.Н., Шевчук Р.П. Аналіз алгоритму дискретного косинусного перетворення для стеганографічного захисту інформації. The 53rd International Scientific and Practical Conference «New Trends in Science and Technology: Global Challenges» (June 5–6, 2023). Myśl Naukowa, Poland, Warsaw. 2023. pp. 93–99.

3. Jessica Fridrich. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2010: 437 p.

4. Пузиренко О.Ю., Прогонов Д.О., Конахович Г.Ф. Комп’ютерна стеганографічна обробка й аналіз мультимедійних даних: Підручник. – 558 с.