

УДК 004.056.53

Корнієнко С.К.¹, Романюта І.В.²

¹ доц. ЗНТУ

² студ. гр. КНТ-724сп ЗНТУ

АВТОМАТИЗОВАНА СТЕГАНОГРАФІЧНА СИСТЕМА

В основі роботи системи покладено використання стеганографічних методів вбудовування інформації до контейнера [1]. Система призначена для прихованого додавання текстових повідомлень до цифрового зображення.

Таким чином можна захистити цінну інформацію від несанкціонованого доступу. Ця програма є прикладом програмних методів захисту інформації, подібним чином можна організувати приховування будь-якої інформації в картинці та його подальшого вилучення з картинки.

На відміну від криптографії, яка приховує зміст секретного повідомлення, стеганографія приховує сам факт його існування. Стеганографії зазвичай використовують спільно з методами криптографії, таким чином, доповнюючи її [2].

Розроблений програмний продукт виконує приховування інформації наступним чином. При використанні моноalfавітної заміни окремі букви відкритого тексту замінюються іншими буквами або числами, або якимись іншими символами. Для цього вводиться ключ, який знає тільки людина, що шифрує текст. Програма розбиває текстове повідомлення на окремі символи, потім перетворює символи в двійковий код і розбиває його на окремі біти. Зображення розбивається на окремі пікселі, у кожного пікселя виділяються RGB-компоненти, потім до кожного з них додається окремий біт двійкового коду текстового повідомлення. Таким чином шифруємо текст в зображення.

Для вилучення інформації з контейнера потрібно взяти два зображення (оригінал і зашифровану копію), завантажити їх до програми та ввести ключ, отриманий по захищеному каналу від відправника. В процесі вилучення інформації зображення будуть розбиватися на окремі пікселі. У кожного пікселя виділяються RGB-компоненти, з яких будуть виводитися окремі біти двійкового коду. Далі програмно визначається різниця результатів виконання цих операцій: відповідні біти двійкового коду будуть відніматися. Двійковий код перетворюється в окремі символи, які виводяться на екран як розшифрована відкрита інформація.

Алгоритм роботи програми:

1. Вбудовування інформації в контейнер:

- 1.1. Завантаження зображення.
- 1.2. Визначення кількості пікселів, з яких воно складається.
- 1.3. Отримання максимального розміру текстового повідомлення, що може бути зашифровано в цьому зображенні, шляхом ділення отриманого в попередньому пункті значення на 8.
- 1.4. Введення тексту, що підлягає шифрації.
- 1.5. Визначення розміру тексту та порівняння його з максимально припустимим.
- 1.6. Визначення кроку просування по бітовій мапі.
- 1.7. Організація двох вкладених циклів:
 - зовнішнього: обхід по символам;
 - внутрішнього: обхід по бітам символу.
- 1.8. Заміна у циклах бітів зображення бітами тексту, рухаючись по зображенню з заданим кроком.
- 1.9. Збереження отриманого результату.
- 1.10. Запис до файлу "ключа", який дозволить розшифрувати повідомлення.

2. Вилучення інформації з контейнера:

- 2.1. Завантаження зображення.
- 2.2. Завантаження ключа.
- 2.3. Організація двох вкладених циклів:
 - зовнішнього: обхід по символам;
 - внутрішнього: обхід по бітам символу.
- 2.4. Зчитування у циклах з кроком, зазначеним у ключі, значення останніх бітів пікселів.
- 2.5. Групування бітів у символи та формування з символів текстового рядку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко – К: "МК-Пресс", 2006. – 288 с.
2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев – М.: СОЛОН-ПРЕСС, 2016. – 262 с.