УДК 004.056.5

Владислав ВОЛОШИН

Національний університет Одеська політехніка

РОЗРОБКА ПРОГРАМНОГО ЗАСТОСУНКУ ДЛЯ ШИФРУВАННЯ І ПЕРЕДАЧІ СТЕГАНОГРАФІЧНОГО ПОВІДОМЛЕННЯ

Вступ. В сучасному цифровому світі, де зберігається величезна кількість конфіденційної інформації та обмін даними відбувається щохвилини, безпека є надзвичайно важливою. Одним із ефективних способів забезпечення безпеки є використання криптографії, методи шифрування та стеганографії. Дослідження та розробка програмного застосунку спрямовані на шифрування і передачу конфіденційної інформації в надійний спосіб. Особлива увага приділяється методам, які поєднують в собі шифрування та стеганографію, зокрема, метод Коха і Жао, що базується на вбудовуванні стеганографічного повідомлення безпосередньо в цифрове зображення (ЦЗ).

Мета: підвищення ефективності передачі секретних повідомлень шляхом розробки програмного застосунку.

1. Стеганографічний метод Коха і Жао

Розглянемо один зі стеганографічних методів який позиціонується, як стійкий до незначних атак проти вбудованого повідомлення. Метод відносної заміни величин коефіцієнтів дискретного косинусного перетворення (метод Коха і Жао) - це один з найпоширеніших сьогодні методів приховування конфіденційної інформації в частотній області зображення, який полягає у відносній заміні величин коефіцієнтів дискретного косинусного перетворення (ДКП) [1].

На початковому етапі первинне зображення стандартним чином розбивається на 8×8 −блоки. До кожного блоку, який будемо позначати B, застосовується ДКП і здійснюється переведення кожного блоку із просторової в частотну область. У результаті виходить 8×8 −блок коефіцієнтів ДКП. Кожний блок призначено для приховування одного біта додаткової інформації (ДІ).

Існує дві реалізації алгоритму:

- Для вбудови біта ДІ використовуються 2 коефіцієнта ДКП.
- Для вбудови біта ДІ використовуються 3 коефіцієнта ДКП.

Розглянемо детально перший варіант.

Під час організації прихованого каналу зв'язку абоненти повинні попередньо домовитися (зв'язатися по захищеному каналу зв'язку) про два конкретних коефіцієнта ДКП із кожного блоку, які будуть використовуватися для приховування даних. Задамо дані коефіцієнти їх індексами (u_1, v_1) і (u_2, v_2) в масивах коефіцієнтів ДКП:

$$\begin{bmatrix} (1,1) & \cdots\cdots\cdots & (1,8) \\ \vdots & \cdots \quad (u_1, v_1) & \cdots \quad \vdots \\ \vdots & \cdots \quad (u_2, v_2) & \cdots \quad \vdots \\ (8,1) & \cdots\cdots\cdots & (8,8) \end{bmatrix}.$$

Зазначимо, що ці індекси повинні відповідати середньочастотним коефіцієнтам ДКП, що забезпечить прихованість інформації та те що вбудована інформація не спотворюватиметься при Jpeg-стиску зі значними коефіцієнтами

якості (або, що те ж саме, з малими коефіцієнтами стиску) [2].

На практиці найчастіше використовуються

$$(u_1, v_1) = (4,5) \text{ і } (u_2, v_2) = (5,4).$$

Нехай у процесі стеганоперетворення треба вбудувати черговий біт $b_k \in \{0,1\}$ ДІ. Відповідно до секретного ключа для цього обираємо блок B ЦЗ-контейнера. Відповідний йому блок коефіцієнтів ДКП позначимо $B^{\text{ДКП}}$:

$$B^{\text{ДКП}} = \begin{bmatrix} b_{11}^{\text{ДКП}} & b_{12}^{\text{ДКП}} & \dots & b_{18}^{\text{ДКП}} \\ b_{21}^{\text{ДКП}} & b_{22}^{\text{ДКП}} & \dots & b_{28}^{\text{ДКП}} \\ \dots & \dots & \dots & \dots \\ b_{81}^{\text{ДКП}} & b_{82}^{\text{ДКП}} & \dots & b_{88}^{\text{ДКП}} \end{bmatrix}.$$

Для вбудови b_k використовуються коефіцієнти $b_{u_1,v_1}^{\text{ДКП}}$, $b_{u_2,v_2}^{\text{ДКП}}$. Вбудова біта b_k відбувається таким чином: якщо $b_k = 0$, то різницю абсолютних значень використовуваних для вбудовування коефіцієнтів ДКП роблять більше деякої заданої додатної величини P, а якщо $b_k = 1$, то цю різницю встановлюють менше -P:

$$\begin{cases} \left|b_{u_1,v_1}^{\text{ДКП}}\right| - \left|b_{u_2,v_2}^{\text{ДКП}}\right| > P, \quad \text{при} \quad b_k = 0, \\ \left|b_{u_1,v_1}^{\text{ДКП}}\right| - \left|b_{u_2,v_2}^{\text{ДКП}}\right| < -P, \quad \text{при} \quad b_k = 1. \end{cases}$$

Після відповідного внесення корекції в значення коефіцієнтів ДКП проводять зворотне ДКП блоку. У результаті пересилання стеганоповідомлення зазнає спотворення, спотворення зазнає й ДІ. Для витягу ДІ виконується аналогічна процедура вибору коефіцієнтів ДКП у кожному блоці, що використовувались в стеганоперетворенні, а розв'язок про переданий біт отримують у відповідності з наступним правилом:

$$\begin{cases} b_k = 0, \quad \text{при} \quad \left|\overline{b}_{u_1,v_1}^{\text{ДКП}}\right| > \left|\overline{b}_{u_2,v_2}^{\text{ДКП}}\right|, \\ b_k = 1, \quad \text{при} \quad \left|\overline{b}_{u_1,v_1}^{\text{ДКП}}\right| < \left|\overline{b}_{u_2,v_2}^{\text{ДКП}}\right| \end{cases},$$

де $\overline{b}_{u_1,v_1}^{\text{ДКП}}$, $\overline{b}_{u_2,v_2}^{\text{ДКП}}$ - коефіцієнти ДКП блоку, можливо зміненого при передачі стеганоповідомлення [3].

2. Програмний застосунок

Після аналізу існуючих застосунків виявлено, що їх переважну кількість застосунків використовує метод заміни значущого біту (LSB), який відомий своєю вразливістю до атак стиснення та геометричних атак. Крім того, в більшості випадків для використання застосунку необхідно ввести ключ, який передають адресату повідомлення. Відомо, що передача ключа у відкритому вигляді є ризикованою практикою з точки зору безпеки.

У цьому контексті пропонується адаптувати метод Коха і Жао, який передбачає вставку інформації у вибіркові блоки Дискретного косинусного перетворення, замість відтворення інформації у всіх послідовних блоках. Крім того, для підвищення безпеки передачі ключа запропоновано використовувати базу даних для автоматизованого витягування ключової інформації замість ручного введення користувачем. Також в рамках програмного застосунку

передбачено використання інтерфейсу програмування додатків (API) для забезпечення зв'язку між базою даних та застосунком. Цей підхід забезпечує автоматизований обмін даними між додатком та базою даних, що сприяє ефективній роботі застосунку та забезпечує безпеку обробки інформації.

Для зручності використання застосунку розроблено програмний інтерфейс, який наведено на рисунку 1.

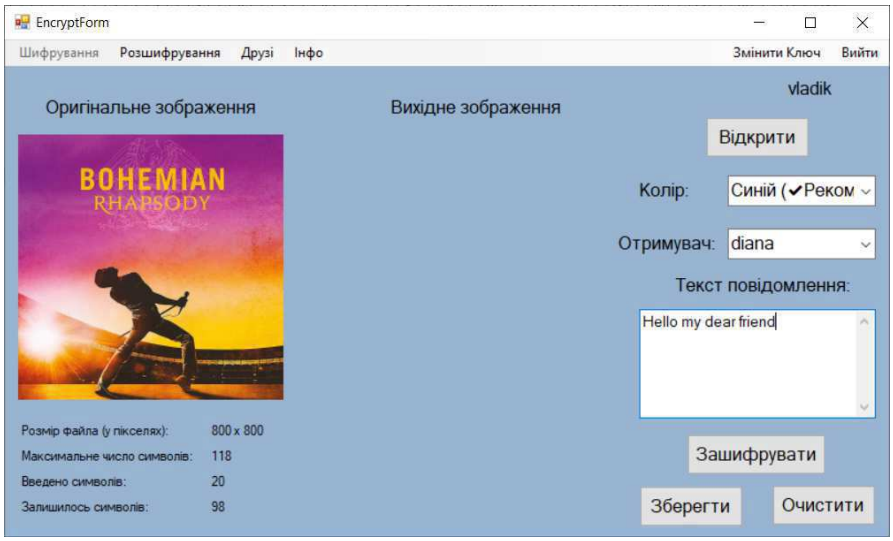

Рисунок 1 - Програмний інтерфейс

Отже, було створено програмний продукт для шифрування і передачі стеганографічного повідомлення.

Загалом, створений застосунок поєднує в собі надійний алгоритм шифрування та зручний графічний інтерфейс, що робить його ефективним інструментом для захисту інформації в процесі комунікації. Цей підхід забезпечує високий рівень безпеки, залишаючись при цьому доступним та простим у використанні для кінцевих користувачів.

Висновок. Розроблено програмний застосунок для шифрування і передачі стеганографічного повідомлення з простим у використанні інтерфейсом. Запропонована альтернатива у вигляді адаптації методу Коха і Жао. Цей метод передбачає вставку інформації у вибіркові блоки ДКП, що сприяє підвищенню стійкості до атак та забезпечує вищу ефективність вбудовування інформації у зображення дозволяючи користувачеві зашифровувати стеганографічні повідомлення.

Перелік використаних джерел.

1. Vilkhovskiy D. E. Steganalysis for DCT inserts with the Koch-Zhao steganographic method in low stego-payload images. Journal of Physics: Conference Series. 2022. P. 012101.

2. Кобозєва А.А. Аналіз захищеності інформаційних систем / Кобозєва А.А., Хорошко В.А., Мачалін І.О. К.: Вид.ДУІКТ, 2010. 316 с.

3. Laskar B., Bouzid M. Enhancing secure communication: a QIM-based steganography approach for G. 722.2 speech streams with Stable Roommate Index Division. Multimedia Tools and Applications. 2024. P. 1-19.