УДК 681.3.069

ДОСЛІДЖЕННЯ РЕЗУЛЬТАТІВ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ПОВІДОМЛЕНЬ У ФАЙЛАХ ЗОБРАЖЕННЯ ЯК ЗАСОБУ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Навроцький Д.О., аспірант.
Національний авіаційний університет, м. Київ, Україна

Вступ

В області комунікації, безпека є однією з головних проблем сучасного світу. Найрізноманітніші методи захисту інформації та алгоритми приховування даних були розроблені в останні десятиліття. У цій статті, показане порівняння систем, які дозволяють звичайному користувачеві захистити текстове повідомлення, помістивши його в цифровий файл зображення, використовуючи деякі характеристики зображення. Проведене дослідження цих систем виявило не тільки межі приховування данних в зображенні, але також показує видимі межі спотворення, що можуть виникнути в зображенні після обробки. Стеганографічні програмні засіб приховування інформації забезпечують перевагу перед іншими видами програмної інформаційної безпеки, оскільки ховається текст у зображенні, яке не сприймається як носій текстової інформації. У статті описані деякі нюанси, які роблять її цікавою для розробників.

Постановка задачі

Стеганографія може бути визначена як мистецтво і наука про невидиму комунікацію [1]. Це реалізується приховуванням інформації в іншій інформації, таким чином, відбувається приховування існування переданої інформації. Хоча поняття стеганографії та криптографії схожі, але все ж стеганографії відрізняється від криптографії. У криптографії [2] основна увага приділяється шифруванню даних, в стеганографії основна увага приділяється приховуванню самого факту присутності даних. Стеганографія та криптографія це способи захисту інформації від несанкціонованого доступу, але ці технології окремо не досконалі, і можуть бути скомпрометовані. Як тільки наявність прихованої інформації виявляється або якщо виникне якась підозра, то стеганографія частково зазнає поразки. Ефективність стеганографії, можна підсилити шляхом об'єднання її з криптографією.

Різні програмні додатки використовують різні формати графічних файлів. Серед усіх цих графічних форматів, формат JPEG файлу найпопулярніший в Інтернеті, із-за малих розмірів зображення.

Головним завданням є дослідження доступних стеганографічних та шифрувальних алгоритмів, для визначення кращої комбінації надійного шифрування, зручності і продуктивності. А також пошук меж використання стегонагофічного методу приховування повідомлення у просторовій і частотній області. Основна перевага цього дослідження – наочність результатів спотворення зображення. Що дуже важливо для успішного вибору і застосування обраної системи.

Аналіз системи.

Великі розміри зображення і велика глибина кольору, роблять об'єм зображення занадто великим, що уповільнює передачу його через Інтернет. Для перегляду зображень у розумні строки, задіються методи зменшення розміру файлу зображення. Використовують математичні методи для аналізу і стиснення даних зображень, в результаті отримують менший розмір файлу. Цей процес називається стиснення [3]. Для зображень є два типи стиснення: з втратами і без втрат [3]. Стиснення має велике значення при виборі стеганоалгоритмів. Стиснення з втратами в результаті дає менший розмір файлу, але воно збільшує ймовірність того, що вбудоване повідомлення може бути частково втрачено через те, що надлишкові дані зображення будуть видалені. Стиснення без втрат, зберігає оригінал цифрового зображення недоторканим, хоча в результаті виходить файл не такого малого розміру, як при стисненні з втратами.

Процес стиснення за схемою JPEG включає ряд етапів (рис. 1):

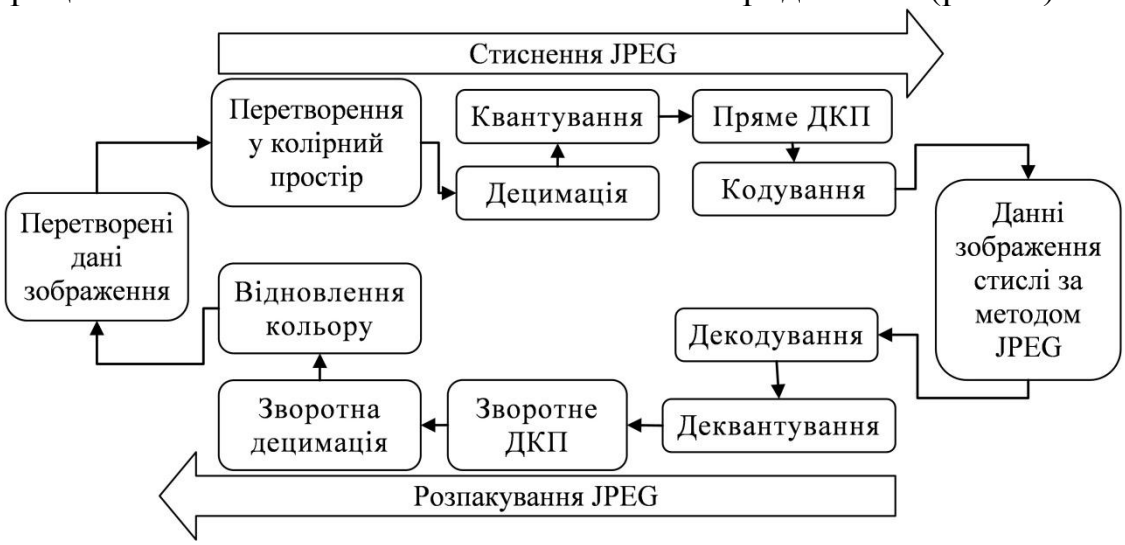

Рис. 1 Структура JPEG – перетворень

- Перетворення зображення в оптимальний колірний простір.

- Децимація компонентів кольоровості усередненням груп пікселів.

- Застосування дискретних косинус-перетворень (ДКП) для зменшення надлишковості даних зображення.

- Квантування кожного блоку коефіцієнтів ДКП із застосуванням вагових функцій, оптимізованих з урахуванням візуального сприйняття людиною.

- Кодування результуючих коефіцієнтів (даних зображення) із застосуванням алгоритму Хаффмена для видалення надмірності інформації.

При цьому хотілося б звернути увагу на те, що декодування JPEG здійснюється у зворотному порядку.

Практичні рекомендації вбудовування даних.

Класичним є наступний принцип вбудовування даних [4]. Нехай сигнал контейнера представлений послідовністю з N біт. Процес приховання інформації починається з визначення біт контейнера, які можна змінювати без внесення помітних спотворень — стеганошляху. Далі серед цих біт, зазвичай у відповідності до ключа, обираються біти, що замінюються бітами приховуваного повідомлення.

Можна запропонувати й інші можливі способи вбудовування до контейнера бітів повідомлення:

1) *Інверсія біта*. Значення бітів стеганошляху заміняються на протилежні. При цьому, наприклад, «1» відповідає заміна 0→1, «0» — заміна 1→ 0.

2) *Вставлення біта*. Перед бітом стеганошляху вставляється біт повідомлення. При цьому значення останнього повинне бути протилежним значенню біта контейнера.

3) *Видалення біта*. Обираються пари «01» або «10» бітів стеганошляху, які відповідають різним значенням біта повідомлення. Потім перший біт пари видаляється.

4) *Використання біта-мітки*. На той факт, що наступний біт контейнера (незмінний) є бітом прихованого повідомлення вказує інверсія попереднього біта-мітки.

5) *Застосування порогових бітів*. Як і у попередньому методі використовується біт-мітка. Але, одному бітові повідомлення відповідає декілька наступних за міткою біт (непарна кількість). Якщо серед цих біт більше одиниць, то біт повідомлення дорівнює «1».

6) *Використання табличних значень*. Для визначення біта повідомлення у попередньому методі, фактично, використовувалася перевірка на парність. Також можна застосовувати і будь-яке інше відображення множини біт в один біт, або знаходити його значення за таблицею.

7) *Динамічно змінювана таблиця*. Метод той самий, що й у попередньому випадку, але таблиця змінюється на кожному кроці. Наприклад, використане значення з таблиці може бути замінене на випадкове.

Метод найменшого значущого біта (просторова область).

Перед імпортом зображення-контейнера його необхідно підготувати у відповідному редакторі і записати у вигляді файлу. Формати *BMP* і *GIF*, TIFF (без стискання) дозволяють зберігати зображення без втрати їх якості і тому є більш придатними в ролі носіїв інформації.

Розглянемо структуру *BMP*-файлу: він містить точкове (растрове) зображення і складається з трьох основних розділів: заголовку файлу, заголовку растру і растрових даних. *Заголовок файлу* містить інформацію про файл (його тип, об'єм і т.п.). До *заголовку растру* винесена інформація про ширину і висоту зображення, кількість бітів на піксель, розмір растру, глибину кольору, коефіцієнт компресії тощо. Нас цікавитимуть *растрові дані* — інформація про колір кожного пікселя зображення. Колір пікселя визначається сполученням трьох основних колірних складових — червоного, зеленого і синього (скорочено — RGB), кожній з яких відповідає своє значення інтенсивності, яке може змінюватися від 0 до 255. Альфа канал (що відповідає за прозорість, bmp формат не підтримує). Отже, за кожен з колірних каналів відповідає 8 бітів (1 байт), а глибина кольору зображення в цілому — 24 біти (3 байти) [1],[5].

Запакування прихованого повідомлення відбувається наступним чином:

1. Імпорт графічного файлу;
2. Імпорт повідомлення, що будемо приховувати (звичайний текст);
3. Криптографічне кодування цього тексту:
4. Вбудовування секретних міток (вони потрібні будуть при розпакуванні):
5. Розгорнення матриці зображення у вектор;
6. На основі вектора зображення формується новий вектор, що вже міститиме приховане закодоване повідомлення;
7. Вектор зображення згортається в матрицю зображення, що має розмірність первинної матриці зображення;
8. колірні матриці розставляються по своїх місцях, в результаті чого одержується контейнер-результат (зображення з прихованим повідомленням).

Розпакування прихованого повідомлення відбувається наступним чином:

1. Попередньо знаючи, що повідомлення було поміщене в масив колірних компонентів, виділяються відповідні кожному кольору підмасиви, переводячи значення колірних характеристик кожного пікселя зображення, що містить у собі скрите закодоване повідомлення, у числові матриці;
2. Оброблюється кожен елементи отриманого вектора,
3. Розпаковується приховане повідомлення,
4. Знаючи, що текст корисної інформації обмежений мітками виокремлюємо його з видобутого квазіповідомлення,

5. Декодування повідомлення.

Результати дослідження, проведеного автором, виявляють спотворення зображення в залежності від кількості використаних біт кольору зображення bmp файлу. Це зображено на рис.2.

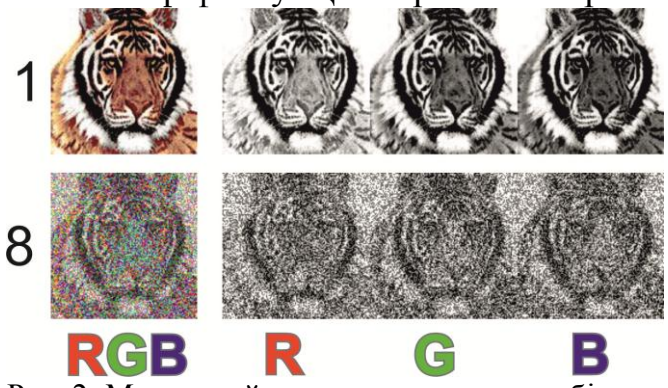

Рис. 2. Метод найменшого значущого біта

Цифри показують кількість залучених біт зображення. Починаючи з 3-4 біту спостерігаємо візуальні спотворення. В стовпчику RGB показано спотворення у зображенні при розміщенні в ньому скритого повідомлення. Справа це саме зображення розкладене на три кольорові складові. Показане спотворення кожного кольору окремо. R – червоний, G - зелений, B - синій.

Метод відносної заміни величини коефіцієнтів ДКП (частотна область) [1].

Запакування прихованого повідомлення відбувається наступним чином:

1. Виділяються масиви колірних компонентів зображення;

2. У зв'язку з низькою чутливістю ЗСЛ до каналу синього кольору, приховуване повідомлення вбудовуватимемо до масиву B (синій колір);

3. Визначається розмірність масиву **B** та задається розмірність сегментів (блоків), на які він розбиватиметься:

4. Кожен сегмент призначено для приховування одного біта секретного повідомлення. Тому необхідно перевірити достатність кількості сегментів для цієї операції.

5. Застосовується до кожного сегменту дискретне косинусне перетворення, одержується відповідна матриця розмірністю $\mathbf{N} \times \mathbf{N}$, кожен елемент якої є коефіцієнтом ДКП.

6. Задаються позиції двох коефіцієнтів ДКП в масиві контейнера B, які використовуватимуться при вбудовуванні і видобуванні повідомлення з контейнера. Ці два коефіцієнти повинні відповідати косинус-функціям із середніми частотами, що забезпечить прихованість інформації в суттєвих областях сигналу, і зробить її стійкішою до JPEG-компресії.

7. Вбудовування інформації проводиться у залежності від контрасту сегмента зображення:

8. Виконується обернене ДКП;

9. Проводиться збирання сегментів до масиву.

Розпакування прихованого повідомлення відбувається наступним чином:

1. До кожного сегмента застосовується пряме ДКП, отримуючи при цьому масив коефіцієнтів ДКП кожного окремого сегмента;

2. Проводиться видобування прихованої інформації. Результат видобування являє собою вектор ASCII-кодів, який можна, наприклад, трансформувати у символьний рядок.

Результати дослідження, проведеного автором, виявляють спотворення зображення в залежності від значення порогу модулів двох коефіцієнтів ДКП. Значення порогу визначає різницю в контрастності між сусідніми сегментами зображення, що використовуються як контейнер приховуваного повідомлення.

Рис. 3. Метод відносної заміни величини коефіцієнтів ДКП

Змінювали тільки синю компоненту зображення, B. Зліва показане кінцеве зображення. Справа синя компонента зображення.

Встановлюємо значення порогу модулів двох коефіцієнтів ДКП в масиві контейнера B, які використовуватимуться при вбудовуванні і видобуванні повідомлення з контейнера. Ці два коефіцієнти повинні відповідати косинус-функціям із середніми частотами, що забезпечить прихованість інформації в суттєвих областях сигналу, і роблять її стійкішою до JPEG-компресії. Дослідження показали, що оптимальне значення порогу P=10. Вбудовування інформації проводилось таким чином: для передачі біта «0» необхідно, щоб різниця модулів коефіцієнтів ДКП була більшою за величину P, а для передачі біта «1» ця різниця повинна бути меншою за –P.

Висновки

Проведене дослідження показало наявність спотворень зображення в залежності від «глибини занурення» стеганографічного методу. Для методу, що приховує повідомлення в просторову частину зображення показником є найменш значущий біт кольору зображення, від 1 до 8. Якщо використовуємо тільки один біт, то спотворення непомітні. Якщо всі біти, тобто 8 для кожного кольору, то зображення втрачає у всіх показниках якості. Максимально можливий біт номер 3. Тобто можна ховати повідомлення в перших трьох бітах зображення.

Для методу, що приховує повідомлення в частотній області зображення показником є найменше порогове значення між модулями двох коефіцієнтів ДКП, від 2 до 65536. Якщо використовувати мале значення порогу, то спотворення непомітні. Але тоді зменшується область де можна приховати

повідомлення. Якщо брати великий поріг, то можна сховати повідомлення більшого розміру, але будуть помітні візуальні спотворення. Максимально можливий поріг 16. Якщо брати більше, то візуальні спотворення стають помітні. Оптимальний варіант 10.

Візуальні спостереження проводились на ЖК моніторі. При роздруковуванні на лазерному принтері, відмінностей теж не було знайдено між зображенням без спотворень і зображенням з прихованим повідомленням, для зазначених параметрів стеганографічного методу.

Література

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: "МК-Пресс", 2006. — 288 с.

2. Мао В. Современная криптография. Теория и практика. – М.: «Вильямс», 2005. – 768с.

3. Steven W. Smith, The scientist and engineer's guide to digital signal processing. — «California Technical Publishing San Diego», (USA), 1997. — P. 625.

4. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: Солон-Пресс, 2002.–265 с.

5. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. — Запоріжжя: Просвіта, 2001. — С.198-201.

Навроцький Д.О. ***Дослідження результатів стеганографічного приховування повідомлень у файлах зображення, як засобу забезпечення захисту інформації.*** *У цій статті представлено синергетику стеганографічних та криптографічних алгоритмів шифрування, які забезпечують надійну основу безпеки. А також порівнюються і досліджуються автором системи приховування повідомлення у просторовій і частотній областях зображення. У статті розглядаються наступні питання: Процес стиснення за схемою JPEG; Структура JPEG – перетворень; Практичні рекомендації вбудовування даних в файли зображень; Метод найменшого значущого біта (просторова область) і метод відносної заміни величини коефіцієнтів ДКП (частотна область); Запакування і розпакування прихованого повідомлення; Зображення візуальних спотворень при зміні параметрів системи.*

Ключові слова: *Стеганографія, криптографія, компресія, дискретне косинусне перетворення Фур'є, графічна адаптація.*

Навроцкий Д.А. ***Исследование результатов стеганографического сокрытия сообщений в файлах изображения, как средства обеспечения защиты информации.*** *В этой статье представлена синергетика стеганографических и криптографических алгоритмов шифрования, которые обеспечивают надежную основу безопасности. А также сравниваются и исследуются автором системы сокрытия сообщения в пространственной и частотной областях изображения. В статье рассматриваются следующие вопросы: Процесс сжатия по схеме JPEG; Структура JPEG - преобразований; Практические рекомендации встраивания данных в файлы изображений; Метод наименьшего значащего бита (пространственная область) и метод относительной замены величины коэффициентов ДКП (частотная область); Упаковка и распаковка скрытого сообщения; Изображение визуальных искажений при изменении параметров системы.*

Ключевые слова: *Стеганография, криптография, компрессия, дискретного косинусного преобразования Фурье, графическая адаптация.*

Navrotskyi D.O. ***The study results steganography hiding messages in image files as vehicle security software.*** *Synergetics of steganographic and cryptographic encryption algorithms, which provide a solid security foundation, is presented in this paper. Hiding messages systems in spatial and frequency domain image are compared and studied by the author. The following questions: Compression scheme JPEG , JPEG – transformation structure, Practical recommendations for hiding data to image files, The method of least significant bits (spatial domain) and the DCT coefficients values relative replacement method (frequency domain), Packing and unpacking the hidden message, Visual distortion image changing system parameters are considered.*

Keywords: *steganography, cryptography, compression, discrete cosine Fourier, graphic adaptation.*