НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ», № 2, 2006

УДК: 621.391.7

В. В. Корпінець, Ю. Є. Яремчук

ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ЗОБРАЖЕННЯХ НА ОСНОВІ СПЕЦИФІЧНИХ ОСОБЛИВОСТЕЙ ФОРМАТУ ФАЙЛУ

Приховування інформації в зображеннях є досить поширеним стеганографічним методом. При цьому приховується факт наявності секретної інформації в зображенні. Актуальною проблемою приховування інформації в зображеннях є забезпечення відсутності ознак, які б вказували на наявність інформації в файлі зображення, основною з яких є помітне для людського ока зниження якості зображення [1].

Методи, що вирішують цю проблему, поділяють на такі групи [2]:

1. Прямі методи, що використовують модифікацію зображення в просторовій області.
2. Методи, що модифікують зображення, попередньо перетворене в іншу форму.
3. Методи, що використовують фрактальне кодування зображень.

З точки зору оцінювання цих методів важливими є такі характеристики :

1. Ступінь зміни якості зображення внаслідок приховування інформації;
2. Стійкість прихованої інформації при зміні файлу-контейнера (зсув, обрізка та ін);
3. Стійкість до компресії файлу-контейнера;
4. Кількість інформації, яку можна приховати без суттєвої зміни файлу-контейнера.

Серед наведених характеристик перша є чи не найважливішою тому, що основною задачею стеганографії є приховування самого факту присутності вбудованої інформації у файлі. Більшість методів, за своєю природою, напряму пов'язані зі зміною самого зображення. Розмір інформації, яку ми хочемо приховати, обернено пропорційний до якості вихідного файлу зображення. Кількість приховуваної інформації з непомітним для людського ока погіршенням якості зображення сягає до 20% від розміру файлу-контейнера. Також недоліком більшості методів є чутливість до компресії зображення, наприклад у форматі JPEG [3]. Таким чином, актуальними залишаються дослідження, спрямовані на збільшення розміру приховуваної інформації при відносно непомітному погіршенні якості зображення.

Аналіз формату файлу JPEG з точки зору приховування інформації

Згідно специфікації JPEG [4], файли складаються з маркерів, які вказують на початок певної секції нових даних, наприклад – секція таблиць квантування. Кожен маркер починається з байту, що містить 8 двійкових одиниць (FFh). Після цього обов'язково слідує код маркеру, який вказує на спосіб інтерпретації наступних даних, якщо вони передбачені цим типом маркера. Програми, які аналізують вміст файлів JPEG пропускають послідовність байт FFh, а якщо після байту FFh розміщений байт 00h, то останній байт вилучається з подальшого розгляду, а сам байт FFh уже не розглядається, як початок маркера. Такий підхід дозволяє однозначно ідентифікувати початок певної секції.

Структуру файлу JPEG складають вісім таких частин [5]:

1. Початок малюнку(SOI).
2. Маркер APP0.
3. Необов'язкові маркери APPn, де n – ціле число від 1 до 15.
4. Одна чи кілька таблиць квантування (DQT).
5. Початок фрейму (SOF).
6. Одна чи кілька таблиць Хафмена (DHT).
7. Початок сканування (SOS).
8. Кінець малюнка(EOI).

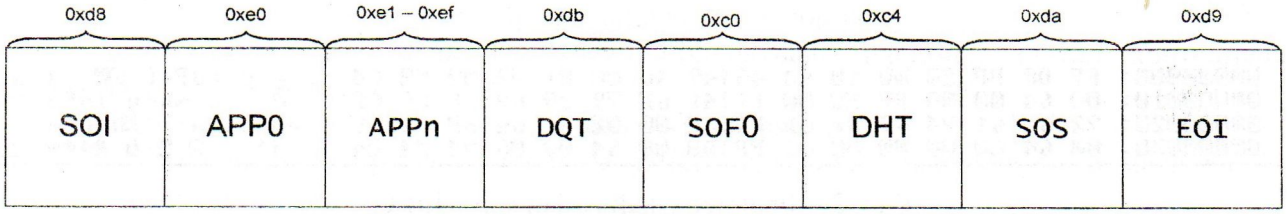

Рис. 1 – Структура файлу JPEG формату

Розглянемо призначення та формат маркерів перших трьох типів.

Кожен файл формату JPEG починається з маркера початку малюнку (SOI), який записаний двома байтами з фіксованими значеннями – FFh D8h.

Слідом за ними розміщені байти FFh E0h – маркер APP0. На відміну від маркерів APPn він має фіксований формат та зберігає основну інформацію про малюнок та версію формату (так званий номер ревізії), в якому його збережено. Типова довжина секції маркера APP0 – 16 байт (10h).

Крім обов'язкових маркерів, довжина яких в сумі складає 20 байт можуть бути присутні додаткові маркери [6], в яких може міститися додаткова інформація. Під додатковою інформацією розуміються дані, які, як правило записують програми, в яких створюється малюнок. Це можуть бути дані найрізноманітнішого змісту, які є доцільними з точки зору розробників програмного продукту, який було використано для створення даного файлу. Проте ця інформація є доступною виключно тільки для самої програми, а не для користувача.

Маркери типу APPn призначені для зберігання додаткової інформації в файлі JPEG-формату. Формат заголовку секції, що починається маркером APPn є достатньо простим і має такий вигляд:

- два байти вказують тип маркера (FFh Enh);
- наступні два байти визначають кількість байт секції (включно з цими двома байтами);
- далі розміщуються необхідні дані, які можуть бути в подальшому використані на розсуд розробників програмного забезпечення.

Виходячи з вищесказаного видно, що додаткова інформація може бути присутньою в зображенні JPEG завдяки зарезервованому простору в об'ємі файлу. Враховуючи те, що будь-який файл JPEG містить зашифровану інформацію програм чи пристроїв [7], за допомогою яких він був створений, можна припустити, що розміщена власна інформація в цій області зображення не викличе підозри.

Аналіз структури формату JPEG показує, що можна використати частину файлу JPEG, яка розмічена додатковими маркерами APPn, для запису своєї інформації, не порушуючи структури файлу та якості зображення.

Метод приховування інформації в зображеннях на основі формату JPEG

Суть даного методу полягає в приховуванні інформації в області додаткової службової інформації, тобто за допомогою маркерів APP1..APP15 чи маркера коментарію. Інформація записується у JPEG-файл послідовно після кожного створеного додаткового маркеру APPn. Для цього вибирається один з 15 можливих маркерів FFh E0h-FhEFh і записується стільки разів підряд (разом з блоком інформації), скільки потрібно для того, щоб помістити всю приховувану інформацію. При цьому, розміщені таким чином дані абсолютно не впливають на будь-які параметри малюнка.

Таким чином, ми можемо розмістити в файлі JPEG, починаючи зі зміщення 20 байт (або 14h), довільну інформацію, яка може нам знадобитись в майбутньому. Приклад такої інформації наведений на рисунку 2.

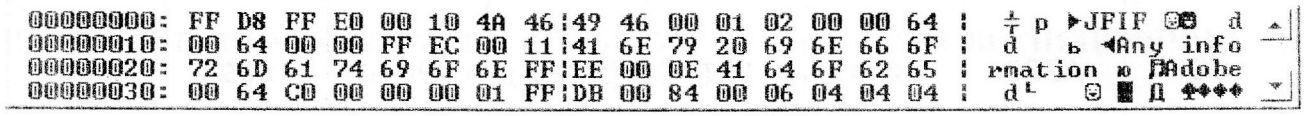

Рис. 2 - Фрагмент файлу формату JPEG

В цьому прикладі в JPEG-файлі міститься текст *Any information*, який було розміщено за допомогою маркера FFh ECh. Довжина тексту на 2 байти менша від значення в полі довжини відповідної секції APPn (як того вимагає специфікація формату JPEG) і складає 11h – 2h = 0Fh, тобто 15 байт.

Максимальний об'єм даних, який може бути розміщений в одному маркері типу APPn сягає $(2^{16}-1)-2=65533$ байт.

На рис. 3 представлено структуру процесу приховування інформації за допомогою даного методу.

Рис. 3 - Процес приховування інформації

Алгоритм процесу приховування інформації згідно запропонованого методу такий:

1. Вибір зображення формату JPEG.
2. Вибір приховуваної інформації .
3. ZIP-ущільнення приховуваної інформації.
4. Вибір секретного ключа для шифрування інформації.
5. Шифрування інформації шляхом послідовного накладання секретного ключа на ущільнену секретну інформацію за модулем 2.
6. Послідовне визначення існуючих додаткових маркерів APPn в заголовку зображення JPEG з послідовним записуванням в них відповідних блоків приховуваної інформації.
7. Якщо існуючих додаткових маркерів APPn недостатньо для розміщення всієї приховуваної інформації, то створити власні додаткові маркери APPn з послідовним записуванням в них інформації блоками до тих пір, поки вся інформація не буде записана.
8. Збереження файлу зображення з секретною інформацією.

Вилучення інформації, згідно запропонованого методу, відбувається таким чином: сканується файл на наявність даного маркеру, після чого збирається інформація про їх кількість і відповідно розмір прихованої інформації, як показано на рис. 4. Далі вона послідовно зчитується.

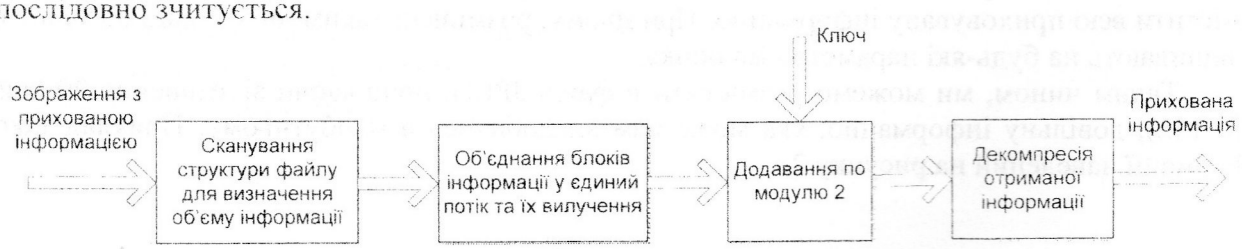

Рис. 4 - Процес вилучення інформації

Детальний алгоритм процесу вилучення приховуваної інформації з файлу-контейнера описується такою послідовністю дій:

1. Вибір JPEG - зображення з прихованою інформацією.
2. Сканування структури файлу на вміст додаткових маркерів та визначення їх кількості.
3. Визначення об'єму приховуваної інформації, шляхом зчитування даних з 3 та 4-го байту заголовку секції кожного додаткового маркеру APPn, яка потім додається.
4. Послідовне зчитування блоків секретної інформації та утворення єдиного потоку.
5. Вибір секретного ключа.
6. Дешифрування прихованої інформації, яке відбувається шляхом накладання секретного ключа на отриману послідовність даних за модулем 2.
7. Декомпресія розшифрованої інформації за допомогою ZIP-алгоритму.
8. Збереження прихованої інформації.

Для покращення характеристик методу було проведено дослідження, задачею якого було визначення кількості додаткових маркерів та об'єму додаткової інформації, в зображеннях формату JPEG, які були створені в найрізноманітніших доступних програмних продуктах та пристроях, а також різного розміру, ступеня компресії, гами кольорів. Це допомогло визначити найоптимальніші параметри (кількість маркерів, які можна створювати в файлі та об'єм інформації, яку можна приховати) при реалізації методу для того, щоб звести до мінімуму можливість виявлення наявності прихованої інформації.

Під час дослідження було проаналізовано близько 100 найрізноманітніших файлів зображення. При цьому розглянуто JPEG-файли, які були створені за допомогою 10-и графічних редакторів (MS Paint, Adobe Photoshop 5.0, Adobe Photoshop 8.0, Adobe PhotoDeluxe 3.0, Corel Draw 11, Ulead Photoimpact XL, ACDSee 7.0 та інші), 2-ох цифрових камер (Olympus Camedia C-765UZ , камера телефону Siemens) та 2-ох сканерів.

Згідно проведеної статистики у файлі формату JPEG може міститися від 6 до 225 додаткових маркерів, причому кількість інформації, яку вбудовують різні програми, може бути від 2 до 120% від розміру самого зображення.

Спираючись на дане дослідження було визначено максимально допустимий розмір приховуваної інформації, що складає не більше 100% від розміру файлу-контейнера.

Кількість маркерів обмежувати недоцільно, оскільки навіть, якщо максимальна кількість маркерів буде 225, то можна приховати інформацію в ущільненому вигляді об'ємом близько 14 Мбайт, що не є коректним з точки зору приховування самого факту наявності вбудованої інформації.

Можливим недоліком запропонованого методу можна вважати насамперед пряму залежність розміру вихідного зображення від розміру приховуваної інформації, що досить збільшує шанси виявити її наявність при великому розмірі файлу. Крім того слід зазначити нестійкість до умисної прямої зміни області JPEG-файлу, де прихована інформація.

Запропонований метод дозволяє зберігати в JPEG-файлі дані будь-якого змісту, навіть інші секретні малюнки. При чому, ці дані спочатку ущільнюються за допомогою методів архівації, що застосовують словники.

Архівування даних використовується з подвійною метою: по-перше, зменшується розмір результуючого файлу; по-друге, усувається надлишковість, характерна для текстових фрагментів, оскільки в подальшому такий архів буде складено з секретним ключем.

Для ущільнення даних пропонується застосувати ZIP-архівування. ZIP-формат є одним з найкращих з точки зору швидкості архівування та степеня ущільнення. ZIP-архівування дозволяє використовувати в кодах програм вільно доступний для розробників програм ZIP-алгоритм, а не додаткові програми – архіватори, тим більше, що цей алгоритм підтримує більшість операційних систем та середовищ розробки програмного забезпечення.

Після ZIP-архівування наступним етапом приховування інформації є шифрування, яке відбувається шляхом накладання на отриману послідовність секретного ключа за модулем 2.

Комбінування методів архівування та шифрування з секретним ключем досить ефективне з точки зору криптостійкості.

Розроблене програмне забезпечення, яке виконує аналіз вмісту JPEG-файлів, дозволяє швидко та зручно зберігати та архівувати дані й розміщувати їх у відповідних JPEG-секціях. Програмну реалізацію запропонованого методу було створено в середовищі Borland Delphi 7 з використанням мови програмування Object Pascal.

Аналіз запропонованого методу

Головним чинником, що впливає на швидкість роботи методу є процес архівування. Оскільки під час ущільнення головним є формат файлу, то швидкість архівування буде залежати тільки від типу інформації.

Найкраще і найшвидше ущільнюються файли з текстовою структурою (*.doc, *.xls,*.html та ін.), при цьому швидкість архівування може досягати до 1,2 Мбайт/с. Практично не ущільнюються архіви та вже ущільнені згідно формату файлу дані – звук, відео, зображення.

Аналіз запропонованого методу з точки зору швидкодії показує, що метод не використовує складних математичних обчислень, а лише використовує специфічні особливості формату файлу. Тому швидкість процесу приховування інформації майже дорівнює швидкості її ущільнення.

Даний метод рекомендовано використовувати для зберігання досить великих, порівняно з іншими методами, об'ємів конфіденційної інформації на локальних носіях інформації. Для найкращого результату файлом-контейнером слід вибирати унікальні зображення – власні шедеври, скановані фотографії чи знімки, зроблені цифровою камерою.

Цей метод також ефективний і при використанні зображень з прихованою інформацією при передаванні через відкритий канал при відносно невеликому розмірі вбудованої інформації (до 30%).

Висновки

Таким чином запропоновано метод приховування інформації в зображеннях формату JPEG, який базується на специфічних особливостях формату файлу, а саме – використання додаткових маркерів, які дозволяють записати секретну інформацію не пошкоджуючи зображення.

Даний метод забезпечує:

- можливість приховувати інформацію, яка не впливає на якість вихідного зображення.
- можливий розмір вбудованої інформації до 100% без втрати якості вихідного зображення;
- захист приховуваної інформації завдяки використанню методів ущільнення та шифрування;
- простоту структури та високу швидкість роботи.

Список літератури

1.В.О. □онфіде, О.Д. Азаров, М.Є. Шелест, Ю.Є. □онфіде. Основи комп'ютерної стеганографії. Навчальний посібник. – Вінниця: ВДТУ, 2003. – 143 с.

2.Воробьев В.И., Грибунин В.Г.Цифровая стеганография.СПб.:ВУС, 2002.

3.Журнал «□онфідент Защита», №3, 2000.

4.Д.С. Ватолин. Алгоритмы сжатия изображений. Методические материалы к спецкурсу ВмиК МГУ "Машинная графика-2". Под руководством Ю.М. Баяковского. Издательский отдел факультета Вычислительной Математики и Кибернетики МГУ им. М.В.Ломоносова, 1999 р., 76 с.

5.Taubman D., Ordentlich E., Weinberger M., Seroussi G. Embedded block coding in JPEG 2000 // Signal Processing: Image Communication. 2002. №17. P. 49-72

6.Shoham Y., Gersho A. Efficient bit allocation for an arbitrary set of quantizers // IEEE Trans. Acoustics, Speech, and Signal Processing. 2000. № 9. P. 1445-1453.

7.Darmstaedter V., Delaigle J.-F., Quisquater J., Macq B. Low cost spatial watermarking // Computers and Graphics. 1998. Vol. 5. P. 417-423.

8.Langelaar G., Lagendijk R., Biemond J. Robust labeling methods for copy protection of images // Proc. Of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. Vol. 3022.

УДК 004-681

Е.А..Кулагин

ОСОБЕННОСТИ ОРГАНИЗАЦИИ СТЕГАНОГРАФИЧЕСКИХ КАНАЛОВ В ПРОВОДНЫХ ТЕЛЕФОННЫХ ЛИНИЯХ

Что такое стеганографический канал? Это канал, который обеспечивает невидимую для сторонних наблюдателей передачу сообщений между отправителем и получателем.

Что такое невидимость? Это неспособность контролирующей системы осознать факт передачи сообщения между отправителем и получателем.

Невидимой может быть информация:

1) которая не вызывает осознаваемую контролирующей системой потерю информации в открытых сообщениях;

2) которая не может быть обнаружена по причине отсутствия у контролирующей системы методик или параметров необходимых для обнаружения;

3) которая в случае обнаружения не осознается контролирующей системой как нелегальная информация.

В какой степени необходимо обеспечить невидимость стеганографического канала? Достаточно ли будет обеспечить только первый из трех видов невидимости или необходимо совмещать два или все три вида невидимости информации? Все это зависит от способности контролирующей системы обнаруживать стеганографические каналы.

Что определяет способность контролирующей системы обнаруживать стеганографические каналы? Как доказывается в [1], способность системы видеть или не видеть оказываемое на нее воздействие определяется доминирующей в ней целью. Таким образом, определив пространство целей систем контроля, присутствующих на участке линии связи межу отправителем и получателем, можно определить некоторые особенности построения стеганографического канала для данного участка линии связи.

Структура стеганографического канала

В общем виде структура стеганографического канала описывается в многочисленной литературе, посвященной данной тематике, например [2].

В нашем случае необходимо рассмотреть особенности построения стеганографического канала при использовании различных точек подключения отправителя и получателя скрытого сообщения к телефонной линии связи.

Как известно, к телефонным линиям относятся абонентские линии и линии первичной сети [3]. Линии первичной сети должны хорошо охраняться, и подключение к ним связано с большими техническими трудностями, поэтому в данной статье этот участок не рассматривается.

Рассмотрим упрощенную структуру проводной телефонной линии связи (рис.1).