УДК 004.056.57

ДОСЛІДЖЕННЯ МЕТОДУ LSB ДЛЯ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ВИГЛЯДІ ЗОБРАЖЕНЬ

В.Ю. Шадхін, О.Л. Грищенко, А.С. Голосков, Д.С. Хижняк

Київський Національний університет технологій та дизайну

У статті розглянуто метод стеганографічного приховування інформації в мультимедійних файлах на основі алгоритму Least Sagnificant Bit (LSB). Досліджуюється та аналізується стегосистема приховування таємного файлу зображення в іншому зображенні. В ролі базового контейнера пропонується використовувати файли BMP-зображень високої роздільності з глибиною кольору 24 та 32 біти, таємне зображення може мати розширення .BMP, .GIF, .PNG, .JPEG.

Ключові слова: *стеганографія, стеганографічний алгоритм, Least Sagnificant Bit, стегосистема, BMP-зображення, приховування даних.*

Цікавість до стеганографії з'явилася в останнє десятиліття й пов'язана з широким розповсюдженням та стрімким розвитком мультимедійних технологій. Стеганографія – наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі [1].

Існуючі алгоритми вбудовування таємної інформації [1] можна поділити на декілька підгруп:

- алгоритми, що працюють з самим цифровим сигналом, наприклад Least Sagnificant Bit (LSB);
- алгоритми, що приєднують таємну інформацію (зображення, звук, текст) поверх оригіналу;
- алгоритми, що використовують особливості форматів файлів, наприклад: запис в метадані, запис в порожні зарезервовані поля файлу.

За способом вбудовування інформації стегоалгоритми поділяють на лінійні (адитивні: A17, A18, L18D, A21, A25), нелінійні та ін. [1].

Головною вимогою до стеганографічної системи є її стійкість до зовнішніх та внутрішніх атак [2]. Під стеганографічною стійкістю розуміють здатність стегосистеми приховувати від противника факт прихованої передачі інформації, можливість протистояти спробам противника до руйнування, викривлення чи видалення прихованих повідомлень [2].

© Київський національний університет технологій та дизайну, 2012

Вибір стеганографічного методу залежить від даних, що представлені у вигляді контейнера секретного повідомлення та цілей стегосистеми загалом, які визначають мінімальну стеганографічну стійкість системи до можливих атак [3].

Постановка завдання

Задачею дослідження є вирішення проблеми приховування таємної інформації (зображення .BMP, .GIF, .PNG, .JPEG чи текст) в файлі-зображення .BMP методом заміни молодшого біту – LSB.

Досліджувана стегосистема повинна бути стійкою, тобто здатна приховувати від кваліфікованого порушника факт прихованої передачі повідомлень, протистояти спробам порушника зруйнувати, спотворити, видалити секретне повідомлення, а також здатна підтвердити або спростувати достовірність таємно переданої інформації. Для забезпечення успішної реалізації стегосистеми необхідно в першу чергу захиститись від візуальних атак, а саме: зображення з секретним вмістом не повинно візуально вказувати на факт існування цього секретного вмісту, тобто зображення повинно бути ідентичним тому, що було на вході. Розмір файла-контейнера до приховування інформації повинен дорівнювати розміру після приховування.

Для досягнення необхідного рівня безпеки та можливості приховування якнайбільше секретної інформації пропонується записувати данні в кожні два-три останні біти кольору, тобто з точки зображення-контейнера брати 2 біта червоного кольору, 3 біта зеленого та 3 біта синього кольорів під секретну інформацію, тобто використовувати 1 байт з трьох та пікселі.

Стегосистема повинна бути реалізована на мові програмування C# в рамках платформи .NET FRAMEWORK 4.0 (OS WINDOWS 7).

Об'єкти та методи дослідження

Об'єктом дослідження виступає стегосистема, що реалізує приховування таємної інформації в мультимедійних файлах (зображень). Базова модель стегосистеми зображена на рисунку 1.

В ролі базового контейнера стегосистеми пропонується використати файли BMP-зображень високої роздільності з глибиною кольору 24 та 32 біти. BMP, зазвичай, не використовує стиснення, що дає можливість для приховування в ньому достатньо великої кількості інформації (33,3 % від загального розміру файла-контейнера).

© Київський національний університет технологій та дизайну, 2012

Секретна інформація представлена у вигляді зображення з можливим розширенням: .BMP, .GIF, .PNG, .JPEG або звичайним текстом.

Рис. 1. **Базова модель стегосистеми**

BMP для представлення кольору використовує модель RGB, тобто колір, який бачить людина отримується в результаті змішування трьох кольорів: червоний, зелений та синій (Red, Green, Blue – RGB). Максимальні розміри для BMP-зображень становлять 65535 x 65535 пікселів [5].

В BMP-файлах з глибиною кольору 24 біта, байти кольору кожного пікселя зберігаються в послідовності BGR (Blue, Green, Red), а в BMP файлах з глубиною кольору 32 біта, байти кольору кожного пікселя зберігаються в послідовності BGRA (Blue, Green, Red, Alpha), де Alpha – альфа-канал (прозорість).

Кожен колір кодується одним байтом (8 біт). В BMP таких кольорів три (червоний, зелений та синій), загалом 3 байта по 8 бітів (BMP з глубиною кольору 24 біта) (рисунок 2).

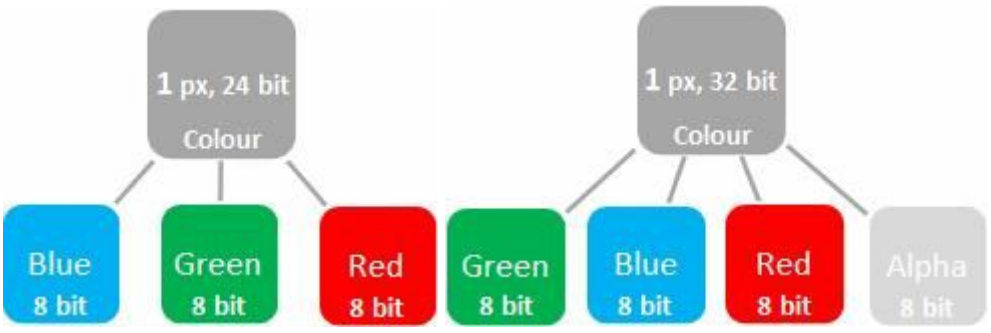

Рис. 2. **Пікселі зображення з глибиною кольору 24 та 32 біти**

Метод дослідження – стеганографічний метод приховування інформації заміною молодшого біту Least Sagnificant Bit (LSB).

© Київський національний університет технологій та дизайну, 2012

Вибір стеганографічного методу залежить від даних, що представлені у вигляді контейнера секретного повідомлення та цілей стегосистеми загалом, які визначають мінімальну стеганографічну стійкість системи до можливих атак.

Метод реалізовується наступним чином. Для того, щоб записати секретну інформацію і при цьому не спотворити зображення-контейнер, необхідно записати дані в молодші біти кольорів зображення, тобто візьмемо один піксель, розділимо його на складові кольори й заміним молодші біти бітами секретної інформації. У випадку використання BMP з глибиною кольору 32 біта, приховування секретної інформації відбувається так само: запис даних в молодші біти перших трьох байтів кольорів зображення.

Метод запису Least Sagnificant Bit можна використовувати й для приховування таємної інформації в відеофайли AVI, так як не стиснутий AVI-файл представляє собою послідовність BMP-зображень [6].

Недоліком методу LSB є чутливість до розміру зображення, тобто чим менший розмір зображення, тим більше будуть відрізнятися два сусідні пікселі, тому пропонується використовувати зображення з великою роздільністю. Також метод «видає себе» при побітовому перегляді зображення, де чітко видно області зображення в які «вбудовано» таємну інформацію. Не дивлячись на це, метод запису Least Sagnificant Bit є досить популярним, стійким та простим в реалізації.

Результати та їх обговорення

З метою дослідження та оптимізації стеганографічного методу LSB для приховування таємної інформації був розроблений програмний додаток для приховування одного зображення в іншому.

Приклад функціонування. Для демонстрації було взято зображення-контейнер «Tree.bmp» з роздільною здатністю 1898x1080 та розміром 6007,55 Кб та зображення-повідомлення «Spider.png» роздільною здатністю 984x738 та розміром 137,15 Кб (рисунок 3). Повідомлення займає 1 байт кожного взятого пікселя. Такий варіант дозволяє зарезервувати в файлі «Tree.bmp» 2001,78 Кб під файл «Spider.png». Візуально (без детального вивчення і порівняння (рисунок 5)) файли «контейнер до» та «контейнер після» різницю не знайти (рисунок 4).

© Київський національний університет технологій та дизайну, 2012

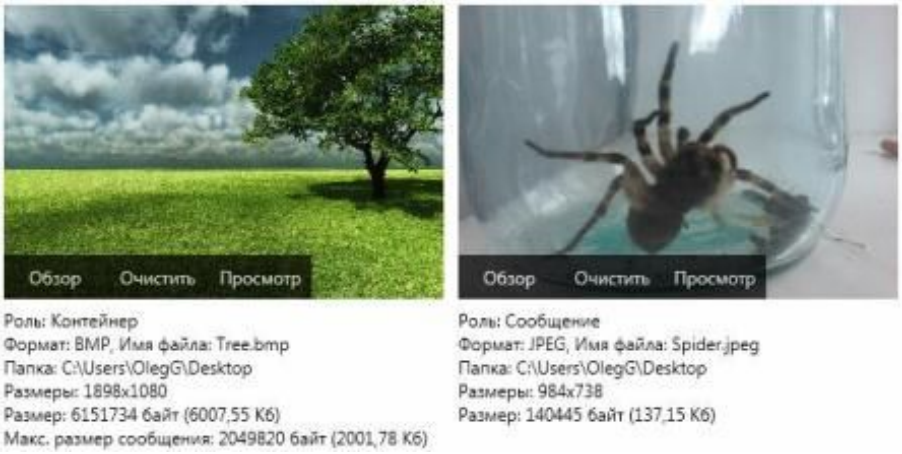

Рис. 3. **Приклад зображення-контейнер та зображення-повідомлення**

Рис. 4. **Зображення-контейнер до та після шифрування**

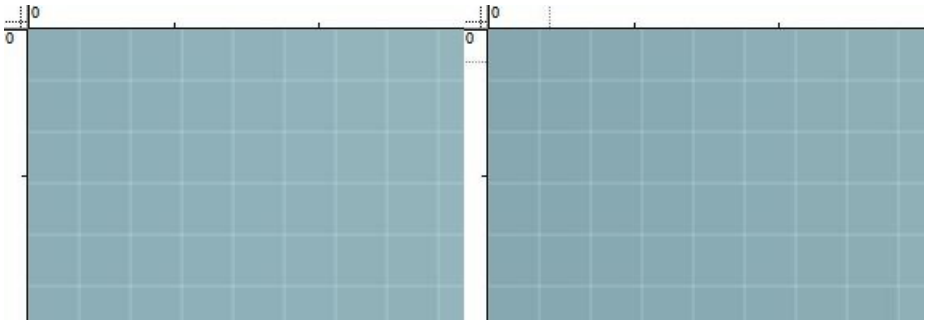

Рис. 5. **Збільшення контейнера до та після шифрування**

Стегосистема працює наступним чином. Вибираються два файли: зображення-контейнер та зображення-повідомлення. Розраховується їхня відповідність (можливість запису інформації). Якщо запис секретного зображення можливий, зображення-повідомлення конвертується в масив байтів byte котрий і записується в зображення-контейнер. При цьому в перший піксель (0,0) зображення-контейнера записується мітка наявності секретного повідомлення (1 бай під символ), в наступні символи записується розмір зображення-повідомлення – пікселі (0,1) – (0,N), далі слідує мітка початку запису – піксель (0,N+1) та сам запис зображення-повідомлення.

© Київський національний університет технологій та дизайну, 2012

Максимальний розмір секретного повідомлення визначається формулою (1).

$$(Width * Height) - Symbol - CountBytes - Start; (байт) \quad (1)$$

Пояснення формули (1):

Width – ширина контейнера в пікселях,

Height – висота контейнера в пікселях,

Symbol – 1 байт під символ наявності секретного повідомлення,

CountBytes – від 1 до N байтів під запис розміру секретного повідомлення,

Start – 1 байт під символ початку запису повідомлення.

Все це реалізується вбудованими методами бібліотеки .NET FRAMEWORK 4.0 [4].

Далі наведено приклад запису (заміни) одного байта прихованого повідомлення: *10 101 010*

RGB пікселя:	Після заміни молодших бітів отримаємо:
R: 11110000	R: 11110*010*
G: 00001000	G: 00001*101*
B: 11001000	B: 11001*010*

Процес зчитування секретного зображення відбувається в оберненому до запису порядку: спочатку виявляються потрібні біти повідомлення (завдяки визначення розміру повідомлення та початку запису), формується масив байтів повідомлення, потім масив байтів конвертується в об'єкт Image що зберігається на жорсткому диску.

Висновки

Таким чином у статті розглянуто метод стеганографічного приховування інформації в мультимедійних файлах на основі алгоритму Least Sagnificant Bit (LSB). Також було досліджено та проаналізовано стегосистему приховування таємного файлу зображення в іншому зображенні.

Заміна 8 бітів з 24 є найбільш оптимальним для приховування досить великої кількості секретної інформації, так як це не вносить в зображення помітних людському оку змін. Для досягнення більшої надійності, таємну інформацію можна записувати та зчитувати за певним алгоритмом обходу пікселів, не рухаючись за піксельними лініями зображення [5]. Наприклад, дані можна записати по краям зображення, залишивши середину без змін. Для створення більш надійної стегосистеми можна застосувати шифрування повідомлення. Також потрібно пам'ятати що чим менше повідомлення, тим важче його виявити.

© Київський національний університет технологій та дизайну, 2012

ЛІТЕРАТУРА

1. Классификация критериев выбора контейнера для LSB-метода: тезисы докладов в 3-х томах 13-ой межд. науч.-техн. конф. студ. и асп. [«Радиоэлектроника, электротехника и энергетика»], Т.1. – М.: МЭИ, 2007. С. 400-401.
2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко – К.: МК-Пресс, 2006. – 288 с.
3. Стеганографія [Електронний ресурс] / Матеріал з Вікіпедії — вільної енциклопедії. Режим доступу: http://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F (Последнее изменение этой страницы: 15:25, 1 июня 2012).
4. Обзор алгоритмов Шифрования [Електронний ресурс] / Rohos Защита данных и контроль доступа // Режим доступу: http://www.rohos.ru/help/crypto_algorithms.htm
5. LSB стеганография [Електронний ресурс] / Режим доступу: http://habrahabr.ru/blogs/algorithm/112976/

В.Ю. Шадхин, О.Л. Грищенко, А.С. Голосков, Д.С. Хижняк

Исследование метода LSB для стеганографического сокрытия информации в представлении изображений.

В статье рассмотрен метод стеганографического скрытия информации в мультимедийных файлах на основе алгоритма Least Sagnificant Bit (LSB). Исследуется и анализируется стегосистема скрытия секретного файла изображения в другом изображении. В роле базового контейнера предлагается использовать файлы BMP-изображений высокого разрешения с глубиной цвета 24 и 32 бита, секретное изображение может иметь расширение .BMP, .GIF, .PNG, .JPEG.

Ключевые слова: *стеганография, стеганографический алгоритм, Least Sagnificant Bit, стегосистема, BMP-изображение, скрытия данных.*

V.Y. Shadhin, O.L. Grischenko, A.S. Goloskov, D.S. Hiznyak

The investigation of LSB method for the steganographic information hiding in presentation of images.

The article reviews a method of steganographic information hiding in multimedia files on the basis of the Least Sagnificant Bit (LSB) algorithm. Investigated and analyzed stegosystem that hiding a secret image file in another image. In the role of the basic container is proposed a BMP-high-resolution images with a color depth of 24 and 32 bits, the secret image can have the extension: .BMP,. GIF,. PNG,. JPEG.

Keywords*: steganography, steganographic algorithm, Least Sagnificant Bit, stegosystem, BMP image, data encapsulation.*

© Київський національний університет технологій та дизайну, 2012