004.056.5

А.Д. Котов, М.С. Потеряев

**Современные методы цифровой стеганографии**

Санкт-Петербург, Государственный университет морского и речного флота имени адмирала С.О. Макарова

Аннотация

В статье рассмотрен и описан ряд современных методов цифровой стеганографии, основанных на сокрытии данных в пространственной области. В качестве примеров используются алгоритмы «LSB+SPIHT», «LSB+1+RSA» и «LSB with Random pixel selection». Также в статье предоставлен более детальный разбор процесса разработки алгоритма «LSB with Random pixel selection» и анализ полученных данных в результате его тестирования.

В любом обществе информация была и остается основным объектом кражи, подмены или уничтожения. Решением этой проблемы занимаются такие науки, как криптография и стеганография.

Криптография–это наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства [8]. Стеганография в свою очередь занимается методами передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения)[7].

Стеганография делится на несколько направлений: классическая, компьютерная и цифровая. Третий тип – наиболее распространенный и используемый, он основан на сокрытии или внедрении дополнительной информации в цифровые объекты, что ведет к искажению этих объектов. Внесение искажений должно находиться ниже порога чувствительности среднестатистического человека, что не приведет к заметным изменениям этих объектов.

Методы сокрытия информации в изображениях делятся на два типа: сокрытие данных в пространственной области и в области преобразования (в частотной области). Сокрытие данных в пространственной области основано на принципе замены бит избыточной и малозначимой информации на биты встраиваемого сообщения. Сокрытие в области преобразования основано на ортогональных преобразованиях, таких как быстрое преобразование Фурье, вейвлет-преобразование и т.д. В данной статье будет рассмотрен только первый тип алгоритмов.

**Рассматриваемые методы стеганографии, предложенные в 2016-2018 гг.**

Огромную нишу стеганографических методов занимают методы семейства LSB (Least Significant Bit). Суть этих методов заключается в замене наименьших значащих бит в изображении на биты встраиваемого сообщения. Эти изменения должны быть внесены таким образом, чтоб человеческий глаз не мог определить их наличие. У LSB существует большое количество модификаций.

**LSB+ SPIHT**

Одним из наиболее распространённых форматов изображений является JPEG, однако прямое применение LSB к нему невозможно. Метод LSB+ SPIHTрешает эту проблему.Данный метод был опубликован в марте 2016 года в International Journal of Computational Engineering Research. Метод предназначен для сокрытия изображения в изображение.

Первоначально к изображению, которое мы хотим спрятать, применяется вейвлет-преобразование. Вейвлет – математическая функция, позволяющая анализировать различные частотные компоненты данных [3]. После к изображению применятся алгоритм SPIHT. SPIHT (Set partitioning in hierarchical trees) был разработан для оптимальной прогрессирующей передачи изображений, а также для их сжатия. Важной особенностью алгоритма является то, что на любом этапе декодирования качество отображаемой картинки будет наилучшим для введенного объема информации о данном образе [1]. В этом методе стеганографии SPIHT разделяет разложенный вейвлет на значимые и незначимые разбиения на основе функции:

(1)

где - значение набора координат *T*

- значение коэффициента в координате (*i, j*).

После сжатия изображение вейвлет-преобразованием и SPIHT-кодированием, сжатые данные внедряются в изображение-контейнер посредством метода LSB. [5]

Как правило, стегоконтейнеры обладают маленькой ёмкостью, что не позволяет встраивать в них изображения больших размеров. Данный алгоритм решает эту проблему и для сокрытия будет достаточно стегоконтейнера того же размера, что и само изображения.

**LSB+1 + RSA**

В октябре 2017 года в International Journal of Computational Engineering Research была опубликована статья с новым предложенным методом стеганографии LSB+1 + RSA[2]. В алгоритме генерируется открытый и закрытый ключ при помощи алгоритма RSA и применяется функция шифрования к сообщению, которое хотим скрыть. Далее встраиваем это сообщение. При процедуре встраивания проверяется самый значимый бит, если он равен «0», то используются 6 младших бит +1, для сокрытия информации, если он равен «1», после этого используются 7 младших бит +1 для сокрытия информации. Генерируем ключ дешифрования с использованием алгоритма RSA. Настроенные сегменты входного текста затем записываются в папку и получаются в выходном изображении. [4]

Алгоритм LSB достаточно прост в обнаружении, поэтому этот метод сочетает в себе криптографическую и стеганографическую составляющие, которые обеспечивают лучшую безопасность при атаках на стегоконтейнер.

**LSB + Random Pixel Selection**

Как правило, стеганографические методы сильно влияют на качество исходного изображения, вследствие чего посредством визуальной атаки злоумышленник легко определит наличие скрытой информации. Частичным решением проблемы является улучшенный метод стеганографии, основанный на LSB и случайном выборе пикселей, опубликованный в 2016 году. Изображение-контейнер преобразуется в три слоя (красный, зеленый и синий). В технике встраивания используется принцип 2-1-2 (т. е. на первой итерации используются два слоя (синий и зеленый), на второй итерации используется только один слой (т. е. синий), и на третьей опять два слоя (синий и зеленый) и так далее. Секретное сообщение внедряется случайным образом в пиксельные местоположения с использованием генераторов псевдослучайных чисел вместо последовательных. Биты сообщения встраиваются в виде 3-2-3. Первые 3 бита из сообщения встроены в первый случайный пиксель (2 бита в синий слой, и 1 бит в зеленый слой), затем 4, 5 биты внедряются во второй случайный пиксель в синий слой, и последние 3 бита сообщения (шестой, седьмой и восьмой биты) встраиваются в третий случайный пиксель (2 бита в синий слой, 1 бит в зеленый слой) и так далее. Метод хорош тем, что благодаря использованию рандомизации выбора пикселей повышается уровень безопасности стегосистемы, а также визуальное качество изображения остается высоким. [6]

**Оценка качества**

Главная цель стеганографической системы – сохранение качества изображения. Для оценки качества изображения используются такие метрики, как PSNR и MSE. PSNR (Peak Signal-to-Noise Ratio) – это пиковое отношение сигнала к шуму, означающим соотношение между максимумом возможного значения сигнала и мощностью шума, искажающего значения сигнала. В нашем случае PSNR используется для определения ухудшения качества изображения после внесения секретного сообщения в сравнении с исходным изображением. MSE(Mean Squared Error) –среднеквадратическое отклонение.

MSE для двух монохромных изображений I и K размера m\*n определяется по формуле:

*MSE* (2)

В случае изображений с тремя цветными компонентами RGB, считается по всем трем компонентам и делится на утроенный размер изображения:

(3)

[dB] (4)

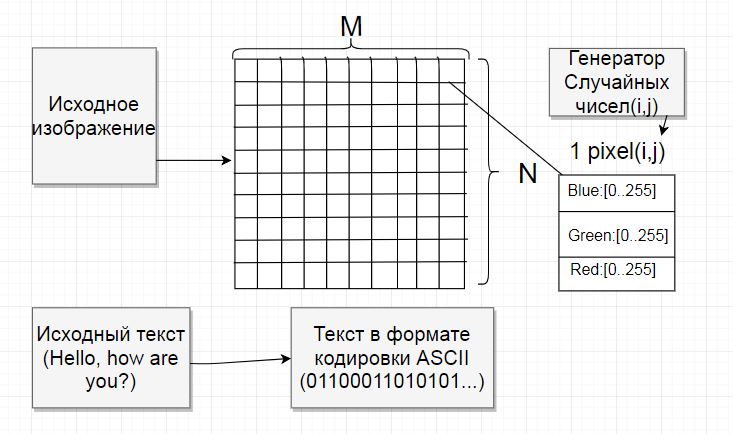
где *MAXI* – максимальное значение, принимаемое пикселем.

В целях углубленного изучения вопроса стеганографических методов было решено подробно разобрать и реализовать метод, основанный на LSB и случайном выборе пикселей.

**Описание реализованного алгоритма «LSB + Random Pixel Selection»**

Алгоритм был реализован в среде Microsoft Visual Studio 2015 на языке программирования С++ на ноутбуке с Intel(R) Core (TM) i3-5005U CPU 2.00 GHz, 8 GB RAM и ОС Windows 7.

Первоначально для простоты понимания и реализации алгоритма была построена схема исходных данных алгоритма, представленная на рис.1.



1Рис.1. Схема исходных данных алгоритма

Входные данные алгоритма: 24-разрядное изображение формата BMP размером M\*N; сообщение, которое хотим закодировать, длинной L. Размер сообщения и размеры изображения определяется в ходе работы программы. Объём памяти в байтах, которое занимает сообщение равно L. Объём памяти в байтах, занимаемое изображением, равно M\*N\*3 (каждый пиксель кодируется 3 байтами). Рассмотрим этапы работы алгоритма:

1. Сообщение преобразуется в двоичную строку с учетом кодировки ASCII.
2. При помощи генератора псевдослучайных чисел формируется два массива: массив индексов строк и массив индексов столбцов. Так как запись битов сообщения в незначащие биты изображения осуществляется по схеме 3-2-3, то для записи 1 байта сообщения нам потребуется 3 пикселя изображения, поэтому размерность массивов равна L\*3. Случайные числа для первого и второго массива генерируются в диапазонах от [0..M],[0..N] соответственно при помощи встроенного генератора случайных чисел языка С++. Объединив попарно значения этих двух массивов получаем набор координат (i,j) случайных пикселей изображения. В пиксели с этими координатами будут записаны биты сообщения.
3. При помощи циклов, программа обрабатывает каждый пиксель изображения. Если координаты очередного пикселя не равны каким-либо координатам из сгенерированных массивов, то этот пиксель просто перезаписывается в новый файл формата \*\*\*.bmp, если же координаты совпадают, то в таком пикселе при помощи поразрядных логических операций языка С++ заменяются младшие значащие биты на биты сообщения, а затем измененный пиксель также записывается в файл. Замена происходит по схеме: 2 бита в синий цвет и 1 бит в зеленый первого пикселя; 2 бита в синий цвет второго пикселя; 2 бита в синий цвет и 1 бит в зеленый третьего пикселя. Файл исходного изображения не изменяется, а перезаписывается в новый файл с целью дальнейшего расчёта метрик MSE и PSNR.

**Результаты работы реализованного алгоритма**

Написанный алгоритм тестировался на 24-разрядных изображениях формата BMP размерами 512\*512 пикселей и 256\*256 пикселей.

Пример работы алгоритма на изображении Lena.bmp: левый рисунок(рис.2) – изображение до обработки алгоритмом, правый рисунок(рис.3) – изображение после встраивания в него сообщения размером 22500 байт.

2 Рис.2. Lena.bmp до применения 3 Рис.3. Lena.bmp после применения

*алгоритма алгоритма*

Полученные результаты оценок PSNR были сравнены с результатами, представленными в первоисточнике этого алгоритма. Результаты представлены в таблице 1.

Таблица 1

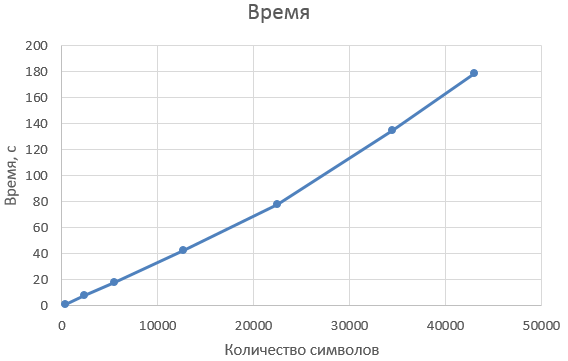
*Результаты работы реализованного алгоритма*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Изображение | Объем сообщения(bytes) | Получившийся PSNR(db) | Время работы алгоритма (сек) | PSNR(db) первоисточника |
| Lena(512\*512) | 43003 | 51,3844 | 179 | 51,8283 |
| 34505 | 52,5412 | 135 | 53,0805 |
| 22427 | 54,4317 | 78 | 54,8254 |
| Baboon(512\*512) | 43003 | 51,4155 | 181 | 51,8436 |
| 34505 | 52,5886 | 135 | 53,1012 |
| 22427 | 54,4557 | 83 | 54,8664 |
| Lena(256\*256) | 12525 | 50,7641 | 16 | - |
| 7705 | 53,0404 | 8 | - |
| 2500 | 57,887 | 1 | - |
| Baboon(256\*256) | 12641 | 50,872 | 15 | - |
| 8500 | 52,8354 | 8 | - |
| 2500 | 57,9117 | 2 | - |

После проведения ряда тестов, был построен график зависимости времени работы алгоритма, от количества символов входного изображения (рис.4).

В данной статье было рассмотрена часть современных методов цифровой стеганографии для изображений, имеющих ряд преимуществ перед устаревшими методами.

Кроме того был детально изучен алгоритм стеганографии, основанный на LSB и случайном выборе пикселей, а также реализован на языке программирования С++ и проверен на тестовых изображениях. Результаты оценок PSNR получились очень близкими с результатами PSNR, представленных статьёй-первоисточником алгоритма, что и подтвердило достоверность представленного метода. Таким образом, выбранный метод стеганографии имеет ряд достоинств: он прост в реализации, за счет рандомизации является более безопасным, чем простой LSB, а также хорошо сохраняет качество изображения. К минусам алгоритма можно отнести длительное время работы программы на сообщениях большого размера.



4Рис.4.График зависимости времени работы алгоритма от количества символов

Анализ других эффективных алгоритмов этого семейства, а также алгоритмов, основанных на сокрытии данных в области преобразования являются предметом наших дальнейших исследований.

**Список использованной литературы:**

1. Д.Сэломон. Сжатие данных, изображений и звука : учеб. пособие / Д.Сэломон -Москва: Техносфера, 2004 – С. 267-274.
2. Свободная энциклопедия Википедия, "RSA" [Электронный ресурс] URL: <https://ru.wikipedia.org/wiki/RSA>
3. Свободная энциклопедия Википедия, "Вейвлет" [Электронный ресурс] URL:

<https://ru.wikipedia.org/wiki/Вейвлет>

1. An Enhanced Steganography Method For Digital Images. Sandeep Kaur, Dr.Akshay Girdhar. [Электронный ресурс]: Journal with Sl. No. 4627 , 2017 - URL: <http://www.ijceronline.com/papers/Vol7_issue10/C07101521.pdf>
2. A New Secure Image Steganography Using Lsb And Spiht Based Compression Method. M.J.Thenmozhi1 , Dr.T.Menakadevi. [Электронный ресурс]: International Journal of Engineering Research & Science (IJOER) , Vol-2, Issue-3 March- 2016 URL: <https://ijoer.com/ICVE2k16-MAR-2016/IJOER-ICVE2k16-MAR-2016-11.pdf>
3. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. Marwa M. Emam, Abdelmgeid A. Aly, Fatma A. Omara. [Электронный ресурс]: (IJACSA) International Journal of Advanced Computer Science and Applications. Vol. 7, No. 3, 2016. URL: <https://www.researchgate.net/publication/299575798_An_Improved_Image_Steganography_Method_Based_on_LSB_Technique_with_Random_Pixel_Selection>
4. Свободная энциклопедия Википедия, " Стеганография" [Электронный ресурс] URL: <https://ru.wikipedia.org/wiki/Стеганография>
5. Российские криптографические стандарты. Кажемский М.А. [Электронный ресурс]   
   URL: <http://dom8a.ru/seminar-ib/05.06.2014/kazemskiy/paper.pdf>