УДК 004.056.5

# СТЕГАНОГРАФИЧЕСКИЙ СПОСОБ СКРЫТИЯ ИНФОРМАЦИИ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ОСОБЕННЫХ ТОЧЕК ИЗОБРАЖЕНИЯ

**Лукманова Р.И.,**
**научный руководитель канд. физ.-мат. наук Дмитриев В.Л.**
***Стерлитамакская государственная педагогическая академия им. Зайнаб Биишевой***

В настоящее время, наряду с широким использованием цифровых форматов мультимедиа и существующими проблемами управления цифровыми ресурсами, становятся все более актуальными исследования в области стеганографии [1 – 6]. Решение задачи сокрытия информации также является важной проблематикой в условиях развитой инфраструктуры сетевого общения пользователей глобальных компьютерных сетей, с развитием которых стало возможным быстро и экономически выгодно передавать электронные документы в различные уголки планеты. При этом значительные объемы передаваемых материалов часто сопровождаются незаконным копированием и распространением. Как следствие, это заставляет искать способы сокрытия авторской информации в различных текстовых, графических, аудио, видео, и других типах файлов.

На сегодняшний день существует довольно много программных продуктов, применяемых для целей стеганографии и реализующих методы внедрения конфиденциальных данных в различные типы файлов.

Классическая задача стеганографии состоит в организации передачи секретного сообщения таким образом, чтобы как содержание сообщения, так и сам факт его передачи были скрыты ото всех, кроме заинтересованных лиц. Для решения такой задачи используется некоторое сообщение, называемое контейнером (стего-контейнером), в которое встраивается требуемое для передачи секретное сообщение. При этом разработчики стеганографических методов должны организовать прозрачность передаваемых конфиденциальных данных: изменение определенного числа информационных бит в контейнере не должно привести к особым потерям его качества (должны отсутствовать артефакты визуализации встраивания). В качестве контейнеров наиболее часто выступают файлы, содержащие цифровые фотографии, текст, музыку, видео. Так, например, при использовании в качестве контейнера графических файлов для сторонних наблюдателей процесс передачи сообщений будет восприниматься как обычный обмен цифровыми графическими файлами. Следует при этом помнить о важности соблюдения одного условия: никто не должен иметь доступ одновременно к исходному файлу, выбранному в качестве контейнера, и к файлу, содержащему скрытое сообщение, т.к. в таком случае простое сравнение файлов сразу же выявит наличие сообщения.

Как было отмечено выше, в компьютерной стеганографии в качестве контейнера может выступать практически любой файловый формат, однако наиболее распространенным типом носителя являются файлы изображения формата BMP. Это объясняется тем, что для целей стеганографии наиболее предпочтительны файлы форматов, в которых используются методы сжатия без потерь (такие виды сжатия типичны для изображений формата BMP, TIFF, PNG, TGA, и др.). Также положительной стороной в пользу выбора формата BMP выступает высокое качество изображения и простота формата.

Стоит отметить, что при работе с форматами файлов, использующих сжатие с потерями, таким как JPEG, обычно все равно выполняют преобразование потока

данных JPEG в поток данных BMP [6]. С позиции стеганографии файлы данного формата позволяют скрывать сравнительно большие объемы информации.

В данной работе в качестве контейнера рассматривается 24-битовое растровое изображение в системе цветности RGB. Каждая цветовая комбинация тона (пикселя) представляет собой комбинацию значений яркости трех составляющих цветов – красного (R), зеленого (G) и синего (B), которые занимают каждый по 1 байту (итого по 3 байта на точку). Таким образом, яркость каждой составляющей записывается 8-битным числом и может изменяться в диапазоне от 0 до 255 (комбинация (0, 0, 0) соответствует черному цвету, комбинация (255, 255, 255) – белому). Использование BMP-файлов в настоящей работе обусловлено только лишь простотой их программной обработки, – все полученные результаты с легкостью могут быть перенесены на случай изображений в файлах других форматов.

Самым распространенным на сегодня методом стеганографического скрытия является метод замены наименее значимых бит (LSB). Идея метода заключается в замене от одного до четырех младших битов в байтах цветового представления точек исходного изображения битами скрываемого сообщения. Также известен ряд работ, посвященных вопросам синтеза систем стеганографии, позволяющих увеличить объем скрываемой информации в несколько раз по сравнению с методом LSB.

Традиционно LSB-методы реализуются по следующей схеме: передаваемое сообщение шифруется с использованием секретного ключа, после чего биты зашифрованного сообщения записываются на место младших бит цветовых составляющих изображения. В простейшем случае запись осуществляется последовательно в каждую составляющую цвета точки, но может также производиться и в некотором другом порядке, задаваемом на основе того же секретного ключа. Визуально, в таком изображении не будет заметно никаких искажений (глаз человека, скорее всего, не заметит отличий даже в случае, если имеется исходный файл для сравнения). Однако компьютерные методы стегоанализа смогут определить наличие встроенного сообщения (например, метод стегоанализа, предложенный М.Ю. Жилкиным и относящийся к классу универсальных методов [5]). Поэтому в ряде работ предлагаются варианты LSB-методов, более устойчивых к стегоанализу. Таковым является, например, метод, учитывающий статистику младших бит изображения [3].

В данной работе предлагается метод, использующий распределение в изображении некоторых особенных точек (отсутствующих в исходном изображении оттенков).

На первом этапе необходимо подготовить контейнер к приему скрытого сообщения – в исходном файле изображения, составляющие (оттенки) трех цветов, имеющие значения 255, изменяются на 254. На этом же этапе скрываемое сообщение переводится в двоичную последовательность.

На втором этапе проводится анализ файла-контейнера на наличие точек, удовлетворяющих следующему условию: во всем изображении два оттенка цвета точек (например, синий (B) и зеленый (G)) совпадают, а третий оттенок (в данном случае красный (R) – обозначим его числовое значение через X) таков, что во всем изображении нет точек, для которых значение этого оттенка равно X+1, X-1, или X-2. Среди всех найденных таким образом точек выбирается последовательность точек, имеющая максимальную длину. Такая последовательность и используется для хранения скрытого сообщения: к значению X третьего оттенка прибавляется соответствующее значение из двоичного представления сообщения. При этом первые три байта сообщения содержат информацию о длине сообщения. Первая точка из найденной последовательности должна быть оставлена без изменений.

Очевидно, что для каждого потенциального файла-контейнера распределение точек, удовлетворяющих отмеченному выше требованию по оттенкам, вполне случайно. В связи с этим данный метод не вносит существенных отклонений в статистику распределения младших бит изображения, и должен быть вполне устойчив к методам стегоанализа.

После добавления сообщения в файл-контейнер исходный пустой контейнер уже не требуется и может быть удален. Таким образом, данный метод позволяет использовать для передачи (и последующего восстановления) скрытого сообщения только один файл. Восстановление сообщения основывается на поиске во всем изображении точек, два оттенка цвета которых совпадают, а третий оттенок таков, что во всем изображении нет точек, для которых значение этого оттенка равно X-1 или X-2.

При таком способе сокрытия информации максимальный ее объем, который может быть размещен в файле-контейнере, целиком зависит от файла изображения: какое-то изображение позволит сохранить больше информации – какое-то меньше (или вообще не позволит). Кроме того, само расположение скрытого сообщения в файле-контейнере будет также зависеть от конкретного изображения.

Очевидно, что, если известен метод, использовавшийся для помещения информации в контейнер, то на его основе легко получить скрытое сообщение. Это является недостатком не только описанного здесь метода, но и любого другого. Именно поэтому нужно предусмотреть такое изменение метода, чтобы, даже зная алгоритм его реализации, невозможно было извлечь скрытое сообщение (извлечь сообщение должен только тот, кому оно адресовано). Для этого перед встраиванием в контейнер, в целях повышения безопасности и компактности, секретное сообщение обычно сжимается и шифруется. Для сжатия могут быть использованы различные алгоритмы, например алгоритмы семейства LZ или BWT. Кроме этого, при встраивании сообщения в контейнер можно использовать дополнительный секретный ключ, который будет определять порядок внедрения сообщения.

Описанный метод, конечно же, допускает всевозможные его модификации. Например, для увеличения емкости контейнера можно использовать не только последовательность точек максимальной длины, но и все другие последовательности точек, удовлетворяющие указанному выше условию. Наряду с использованием секретного ключа это позволит повысить стойкость алгоритма к стегоанализу.

## Список литературы


1. Быков С.Ф., Мотуз О.В. Основы стегоанализа.// Защита информации. Конфидент. – СПб.: 2000, № 3. – С. 38-41.
2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
3. Елтышева Е.Ю., Фионов А.Н. Построение стегосистемы на базе растровых изображений с учетом статистики младших бит // Вестник СибГУТИ. – 2009. № 1. – С. 67-84.
4. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
5. Жилкин М. Ю. Стегоанализ графических данных на основе методов сжатия // Вестник СибГУТИ. – 2008. № 2. – С. 62–66.
6. Кувшинов С.С. Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии / Диссертация на соискание ученой степени кандидата технических наук. – Санкт-Петербург. 2010. – 116 с.