электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 04, апрель 2016

УДК 004.056.53

Экспериментальные исследования реализации метода Куттера при решении задач стеганографии

***Волкович Е.К.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность автоматизированных систем»

***Данилова Е.С.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность автоматизированных систем»

Научный руководитель: Чичварин Н.В., к.т.н, доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность автоматизированных систем»
volkovichek@student.bmstu.ru

Введение

Наиболее актуальная задача в области информационной безопасности (ИБ) на сегодняшний день – задача защиты данных от несанкционированного доступа (НСД). Исторически, в ходе поиска решения данной задачи сформировались два основных подхода к защите данных от НСД: криптографический и стеганографический. Криптография защищает содержимое сообщения, шифруя его, а стеганография скрывает сам факт существования секретного сообщения [[1]]. В рамках стеганографии существуют три основных направления: классическая, компьютерная и цифровая стеганография. Как известно, цифровая стеганография основана на сокрытии или внедрении дополнительных данных в цифровые объекты, вызывая при этом незначительные искажения этих объектов. В данной работе рассмотрены результаты исследования метода цифровой стеганографии на примере сокрытия данных в изображении.

Среди стеганографических методов, применяемых к файлам-изображениям, стоит обратить внимание на метод Куттера, так как он обладает высокой пропускной способностью, устойчивостью к искажениям и к основным видам атак. Благодаря своим характеристикам, данный метод позволяет передавать сообщение в файлах формата *JPEG* и быть устойчивым к разрушению младших бит контейнера. Как известно [[2]], метод

Куттера основывается на том, что зрение среднестатистического человека наименее чувствительно к синему цвету. Соответственно, метод предлагает встраивание сообщения в синий канал изображения-контейнера цветовой модели *RGB*.

1. Цель и решаемая задача

Целью работы было провести экспериментальные исследования качества стеганографического сокрытия цифровых Фурье-голограмм. Как известно, такие голограммы избыточны и весьма устойчивы к частичному разрушению. А стеганорафическое сокрытие данных в виде голограмм обеспечивает дополнительное сжатие сообщений и повышает криптоустойчивость.

Основной задачей явилась запись голограмм чертежей в произвольно выбранном контейнере в виде файла управляемого объема методом Куттера.

2. Основные результаты эксперимента

В качестве контейнера, в котором прячется сообщение, выбрано изображение, представленное на рис. 1. Секретное сообщение, которое необходимо передать – цифровая голограмма чертежа, представлено на рис. 3. Используя цифровую голограмму, а не сам чертеж, мы получаем еще одну степень защиты, где ключом является угол падения опорного пучка.

Рис. 1. Контейнер для встраивания секретного сообщения

Изображение чертежа, который требуется передать, приведено на рис. 2.

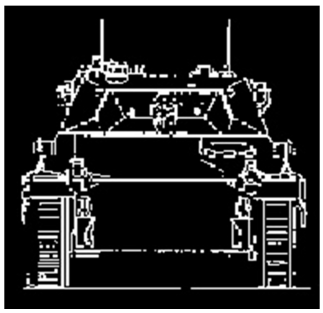

Рис. 2. Секретное сообщение

Тестовый объект, в данном случае - изображение, подсвечивается параллельным пучком виртуального монохроматического излучения. В задней фокальной плоскости виртуального Фурье-объектива располагается виртуальная регистрирующая среда, на которой записывается голограмма.

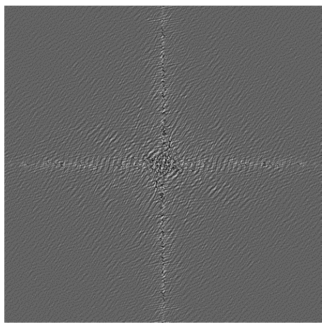

Рис. 3. Голограмма чертежа

Процедура формирования стегосообщения:

1. Получим Фурье-голограмму чертежа (см. рис. 3) и приведем значения голограммы к формату, необходимому для дальнейших вычислений.
2. Представляем голограмму в виде массива битов.
3. Загружаем контейнер для сообщения и определяем матрицы для каждой цветовой компоненты изображения.
4. Задаем параметры встраивания:

– энергия встраиваемого сигнала – $\gamma = 0.05$;

– размерность дифракционно эффективной голограммы – $\sigma = 3$.

5. Определяем функцию, задающую новое значение синей компоненты пикселя после встраивания бита сообщения:

$$SV(x, y, b) = B_{x,y} + (2b - 1) \times \gamma \times \lambda(x, y),$$

где x, y – координаты пикселя, B – матрица синей компоненты, b – значение бита, $\lambda(x,y)$– функция яркости пикселя.

6. Делаем сортировку, необходимую для задания расположения пикселей, в которые будут встраиваться биты сообщения.

Исследования показали, что оптимальной плотности встраивания можно достигнуть, расположив биты, как указано на рис. 4:

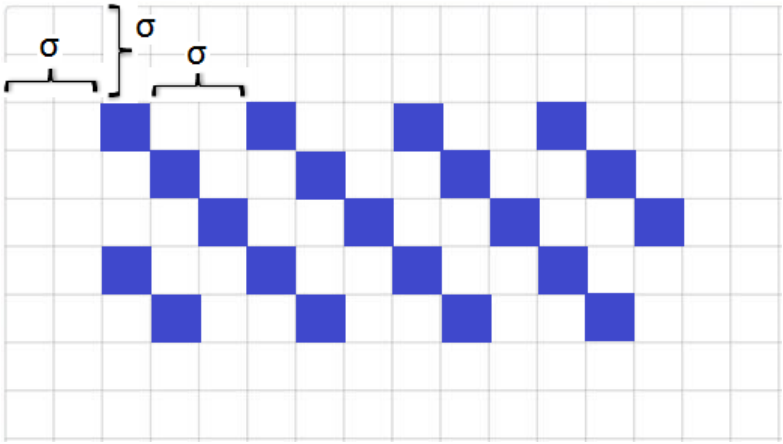

Рис. 4. Расположение бит

При уменьшении энергии встраиваемого сигнала уменьшается вероятность корректного восстановления, а при увеличении данного параметра повышается вероятность обнаружения сокрытия информации.

Коэффициент σ – это количество пикселей слева/справа/сверху/снизу, по которым будет восстанавливаться бит сообщения (см. рис. 4). При уменьшении данного параметра, уменьшается вероятность верного восстановления бита, но повышается объем изображения, которое можно встроить в заданный контейнер.

В зависимости от соотношения размеров контейнера и сообщения, встраивание будет проводиться с некоторым шагом для равномерного расположения встраиваемых битов.

Под ключом понимается секретный элемент, который определяет порядок занесения сообщения в контейнер. Для восстановления сообщения используется секретный ключ, который должен знать получатель: коэффициент σ и размеры изображения.

Процедура извлечения записанного сообщения:

1. Загрузим контейнер с сообщением и определим матрицы для каждой цветовой компоненты изображения.

2. Зададим параметры, необходимые для восстановления сообщения: коэффициент σ и размеры изображения.

3. Извлечем массив бит на основании значений синей составляющей пикселей вокруг тех пикселей, в которые встроены биты сообщения.

4. Полученный массив бит преобразуем к формату голограммы.

5. Выполним обратные преобразования голограммы, чтобы получить изображение – сообщение.

На рис. 5 представлен результат работы программы для нескольких тестовых образцов.

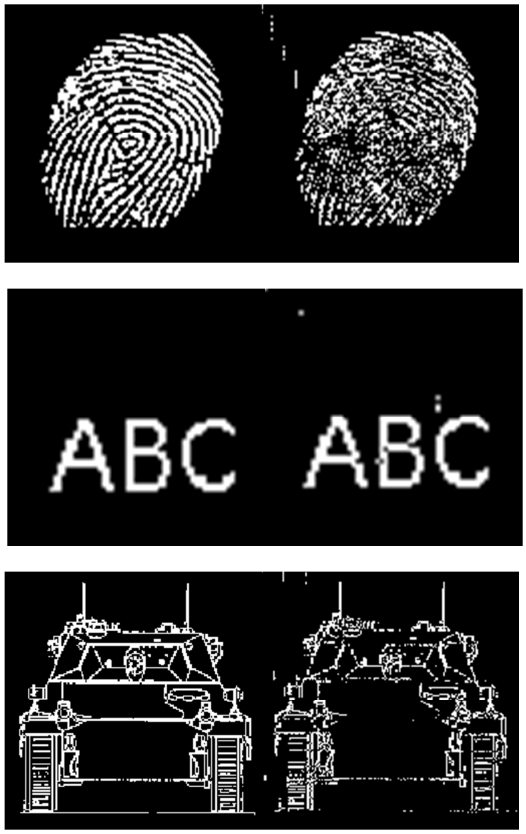

Рис. 5. Тестовые образцы до и после восстановления

Сравнение контейнера и поведение синей цветовой компоненты до и после встраивания секретного сообщения показаны на рис. 6-7.

Рис. 6. Контейнер до и после встраивания сообщения

Рис. 7. Синяя цветовая компонента до и после встраивания сообщения

В процессе исследований промоделирована дефокусировка путем фильтрации изображения контейнера со стего пространственным фильтром с импульсным откликом:

$$h(x,y) = \mathrm{e}^{-\frac{x^2+y^2}{r^2}}.$$

Восстановление дефокусированных и смазанных изображений осложняется наличием помех и шумов в измененном изображении. После восстановления сообщения потери составили 6%, 16% и 34% соответственно. Результат применения фильтра к контейнеру с сообщением и затем восстановленные сообщения для r=2, 3, 5 представлены на рис. 8-9.

Рис. 8. Контейнер после применения фильтра (r = 2, 3, 5)

Рис. 9. Восстановленное сообщение после применения фильтра (r = 2, 3, 5)

Считается, что наименее значащие биты (НЗБ) изображений не являются случайными и при изменении последнего бита статистические параметры изображения будут изменены. В случае стеганографического встраивания, то есть замены НЗБ на случайную последовательность, количество пикселей в парах выравнивается.

Построим гистограммы для синей цветовой компоненты (синий цвет на графике; красным обозначено усредненной значение, то есть ожидаемой в случае встраивание). На рис. 10 представлена гистограмма для контейнера без встраивания, на рис. 11 – для контейнера со встроенным сообщением.

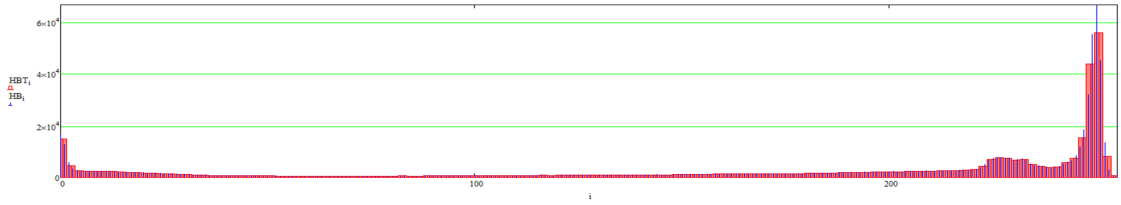

Рис. 10. Гистограмма без встроенного сообщения

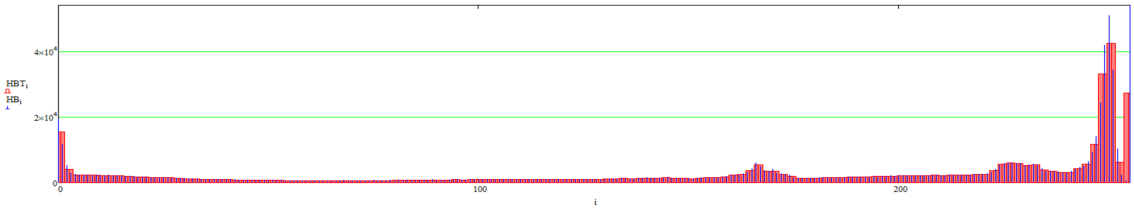

Рис. 11. Гистограмма со встроенным сообщением

В результате полученных данных каких-либо значительных изменений на гистограмме не замечено.

В заключение, был проведен эксперимент, который заключается в наращивании размера стегосообщения при неизменном объеме контейнера. Целью эксперимента было определить зависимость между размером стегосообщения и процентом отклонения синего

в стегосообщении от пустого контейнера в гистограмме. Результат эксперимента представлен на рис. 12.

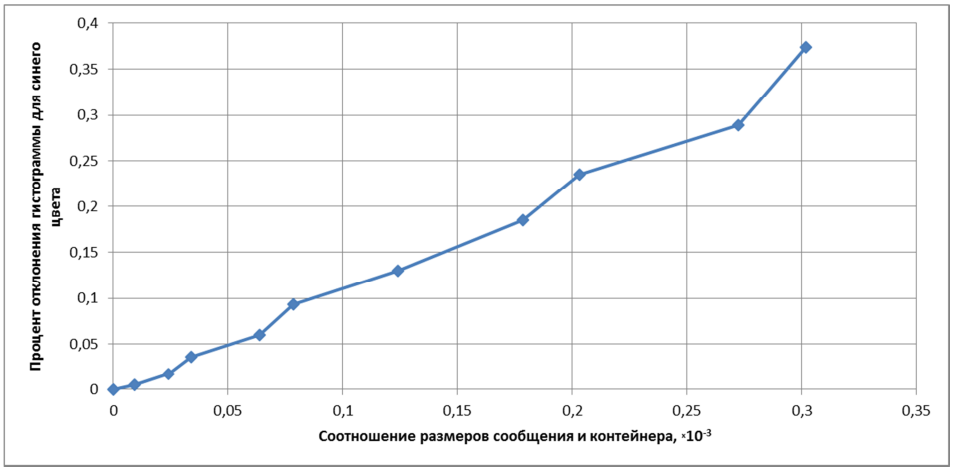

Рис. 12. График зависимости

Из графика видно, что имеет место линейная зависимость между размером стегосообщения и процентом отклонения синего цвета.

Заключение

Проведенные исследования позволили сделать следующие выводы:

1. Сочетание голографирования с сокрытием данных методом Куттера обеспечивает высокую криптостойкость сообщений.
2. Исследованный метод позволяет защищать от НСД проектную документацию, продуцируемую в среде CAD/CAM/CAE/CALS и передаваемую через открытые каналы передачи сообщений.

Список литературы

[1]. Фомин Д.В. Модификация метода скрытия информации Куттера-Джоржана-Боссена. Режим доступа: http://www.amursu.ru/attachments/article/11563/11.pdf (дата обращения 20.09.2015).

[2]. Конахович Г.Ф, Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: МК-Пресс, 2006. 288 с.

[3]. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2009. 265 с.

[4]. Зорин Е.Л., Чичварин Н.В. Стеганография и стегоанализ. М.: Изд-во МГТУ им. Н.Э. Баумана, 2013. 90 с.