АВТОМАТИЗИРОВАННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ МЕТОДАМИ СТЕГАНОГРАФИИ

А.В.Киселева, М.А. Кудрина

Самарский государственный аэрокосмический университет им. академика С.П. Королёва (национально исследовательский университет)

Разработана автоматизированная система защиты информации, реализующая следующие методы стеганографии: LSB, метод Коха-Жао, метод Куттера-Джордана-Боссена и метод сокрытия цветных изображений bmp. Исследована зависимость качества восстановленного секретного изображения и заполненных контейнеров от количества изменяемых бит в цветовой составляющей пикселя.

Введение

В настоящее время, проблема обеспечения конфиденциальности хранимых и, особенно, пересылаемых данных стала чрезвычайно острой. Одним из способов защиты информации является стеганография.

Стеганография – это метод организации связи, который скрывает само наличие связи.

В связи с возрастанием роли глобальных компьютерных сетей становится все более важным значение стеганографии. В настоящее время стеганографические системы активно используются для решения следующих основных задач [1]:

1) защита конфиденциальной информации от несанкционированного доступа;
2) преодоление систем мониторинга и управления сетевыми ресурсами;
3) камуфлирование программного обеспечения;
4) защита авторского права на некоторые виды интеллектуальной собственности.

Теоретическая часть

Стеганографическая система или стегосистема – совокупность средств и методов, которые используются для формирования скрытого канала передачи информации [2]. В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п.

Контейнер – любая информация, предназначенная для сокрытия тайных сообщений.

По используемому принципу скрытия методы компьютерной стеганографии делятся на два основных класса: методы непосредственной замены и спектральные методы. Если первые, используя избыток информационной среды, заключаются в замене малозначительной части контейнера битами секретного сообщения, то другие для скрытия данных используют спектральные представления элементов среды, в которую встраиваются скрываемые данные.

LSB-метод

В настоящее время наиболее распространенным является метод замены наименьших значащих битов или LSB-метод. Суть метода заключается в изменении последних битов изображения, кодирующих цвет, на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека [3]. Схема работы метода показана на рисунке 1.

Метод Куттера-Джордана-Боссена

Для встраивания информации в контейнер используется одно из свойств зрительной системы человека. Это свойство заключается в том, что восприимчивость человека к изменениям яркости синего цвета по сравнению с красным и зелёным – меньше всего.

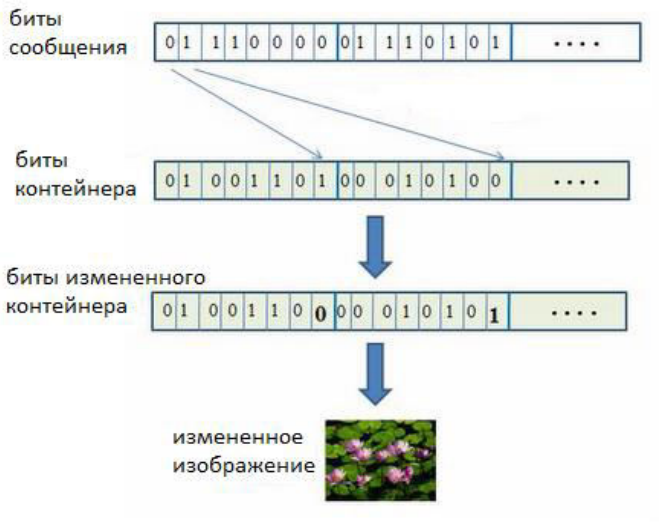

Рисунок 1– Схема работы метода LSB

Один бит сообщения записывается в один пиксель контейнера, при этом яркости красного и зелёного цветов пикселя остаются без изменений, а яркость синего изменяется по следующей формуле [4]:

$$B^*_{x,y} = \begin{cases} B_{x,\,y} + \lambda Y_{x,\,y}, \text{ при } m_i = 1 \\ B_{x,\,y} - \lambda Y_{x,\,y}, \text{ при } m_i = 0 \end{cases},$$

где Bx,y – яркость синего цвета пикселя с координатами (x,y);

$B^*_{x,y}$ – изменённая яркость синего цвета пикселя;

$Yx,y = 0{,}3Rx,y+0{,}59Gx,y+0{,}11Bx,y$ – яркость пикселя;

Rx,y – яркость красного цвета пикселя с координатами (x,y);

Gx,y – яркость зеленого цвета пикселя с координатами (x,y);

mi – i-ый бит сообщения, которое мы хотим встроить;

$\lambda = 0{,}1$ – коэффициент, задающий энергию встраиваемого бита данных (задаётся исходя из функционального назначения и особенности стегосистемы). Чем больше λ, тем сообщение заметнее, но при этом более устойчиво к искажениям.

Так как на принимающей стороне нет оригинального изображения, то гарантированно узнать, в какую сторону изменилась яркость синего цвета, мы не можем. Поэтому для извлечения прогнозируется значение яркости синего цвета:

$$\overline{B}_{x,\,y} = \frac{\sum_{i=1}^{\sigma} (B_{x,\,y+i} + B_{x,\,y-i} + B_{x+i,\,y} + B_{x-i,\,y})}{4\sigma},$$

где $\sigma = 1 \div 3$ – размер области, по которой будет прогнозироваться яркость.

На рисунке 2 показан пример для $\sigma = 2$.Пиксель в центре – это пиксель, яркость синего цвета которого мы должны спрогнозировать, опираясь на пиксели, которые обозначены светло-серым цветом [5].

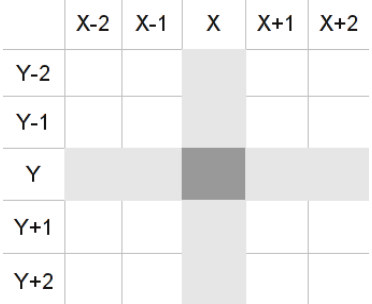

Рисунок 2 – Метод Куттера-Джордана-Боссена

Для извлечения скрытого сообщения используется формула:

$$m_i = \begin{cases} 1, \text{при } B^*_{x,y} > \overline{B}_{x,y}, \\ 0, \text{при } B^*_{x,y} < \overline{B}_{x,y}. \end{cases}$$

Метод Коха-Жао

Алгоритм Коха-Жао для встраивания информации использует частотную область контейнера и заключается в относительной замене величин коэффициентов дискретного косинусного преобразования (ДКП). Изображение разбивается на блоки размерностью 8×8 пикселей и к каждому блоку применяется ДКП. Каждый блок пригоден для записи одного бита информации [6]. Метод является достаточно устойчивым к искажению изображения, даже к его существенному изменению, но для скрытия больших объемов данных неприменим.

Скрытая передача цветных изображений bmp

В качестве входных изображений используются 24-разрядные bitmap-рисунки, в которых на каждый цвет приходится по 8 бит информации. Данные скрываются с помощью метода LSB. Суть алгоритма заключается в том, что секретное изображение разбивается на три цветовых примитива (то есть на оттенки красного, зеленого и синего), а затем каждый примитив записывается в младшие биты одного из изображений-контейнеров. Таким образом, после зашифровки каждый контейнер будет содержать в себе одну цветовую составляющую секретного изображения [7].

Далее из каждого цветового примитива берется два старших бита и записывается в младшие биты соответствующего цвета у соответствующего контейнера. Два младших бита в двух оставшихся цветах обнуляются. Операция повторяется для каждого пикселя.

Для восстановления изображения берется первый пиксель из каждого изображения-контейнера. Два младших бита каждого цвета в этих пикселях становятся старшими битами и складываются соответствующие цветовые составляющие. Эта операция повторяется для всех пикселей и получается восстановленное секретное изображение [7].

Реализация системы

В процессе выполнения выпускной квалификационной работы бакалавра была разработана автоматизированная система, осуществляющая скрытие информации с использованием стеганографических методов, которая позволит выбрать контейнер для встраивания информации, выбрать метод встраивания и ввести секретное сообщение и восстановить информацию из контейнера.

Система реализует следующие функции:

1) встраивание текстовой информации;
2) встраивание изображения;
3) извлечение текстовой информации;
4) извлечение изображения.

После запуска системы отображается окно для встраивания сообщения. В меню пользователь может выбрать пункт «Загрузить контейнер» и выбрать файл для загрузки. Выбранное изображение отобразится на экране. После этого пользователь должен выбрать метод встраивания, например LSB, и нажав на кнопку «Записать» ввести секретное сообщение. После встраивания пользователь может сохранить заполненный контейнер. Для извлечения сообщения переходим на вкладку «Прочитать сообщение». После нажатия на кнопку «Прочитать» выбираем файл, и искомое сообщение появляется в текстовом поле.

Чтобы спрятать изображение пользователь должен перейти на вкладку «Спрятать картинку» (см. рисунок 4), загрузить три контейнера и секретное изображение. Все изображения будут отображены на форме. Чтобы спрятать картинку пользователь должен выбрать количество заменяемых бит. Оно влияет на качество полученных контейнеров и извлекаемого потом сообщения.

Выберем количество заменяемых бит, равное 1, нажмем кнопку «Записать» и сохраним все контейнеры.

Чтобы восстановить картинку нужно перейти на вкладку «Восстановить картинку, загрузить контейнеры и нажать на кнопку «Восстановить».

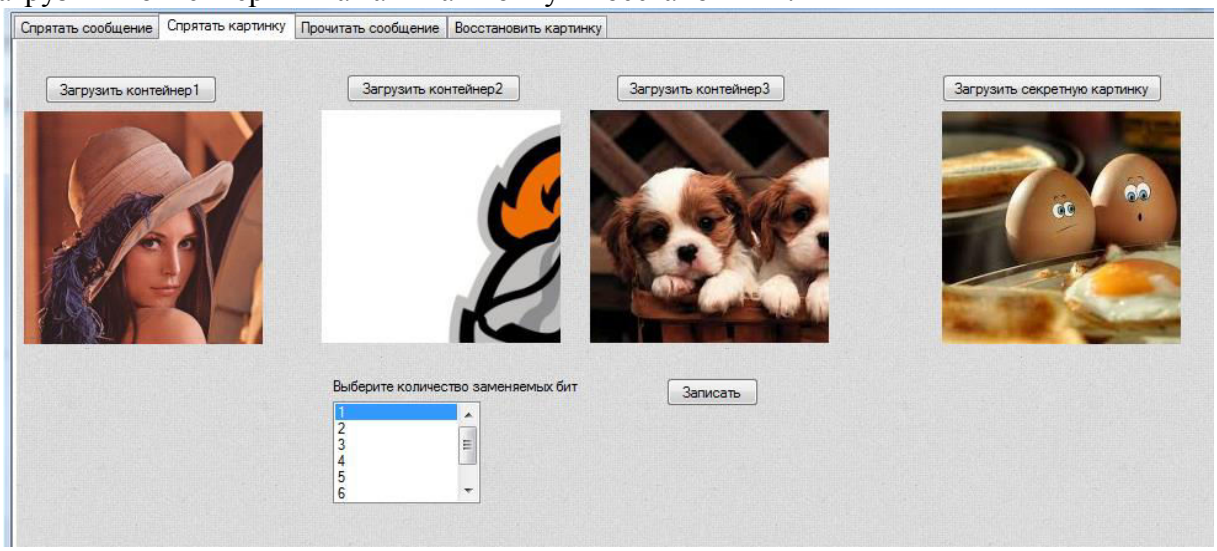

Рисунок 4 – Встраивание изображение с использованием 1 бита цвета контейнера

Экспериментальная часть

Было проведено исследование влияния количества заменяемых бит в байте цветовой составляющей пикселя на качество скрываемого сообщения и контейнеров.

На рисунках 5 – 7 представлены результаты работы программы при 1, 4 и 8 заменяемых битах соответственно.

Из полученных результатов видно, что при использовании одного бита для записи секретное изображение очень сильно искажается, но при этом изменение контейнеров незаметно. При использовании 4 бит, секретное сообщение искажается незначительно, но следы встраивания видны на контейнерах. При использовании 8 бит незаметно передать изображение невозможно, так как контейнеры сильно изменяются и представляют собой RGB составляющие секретной картинки. Кроме того, при одном и том же количестве измененных бит (например, 4), на светлом контейнере искажения видны лучше, чем на темном.

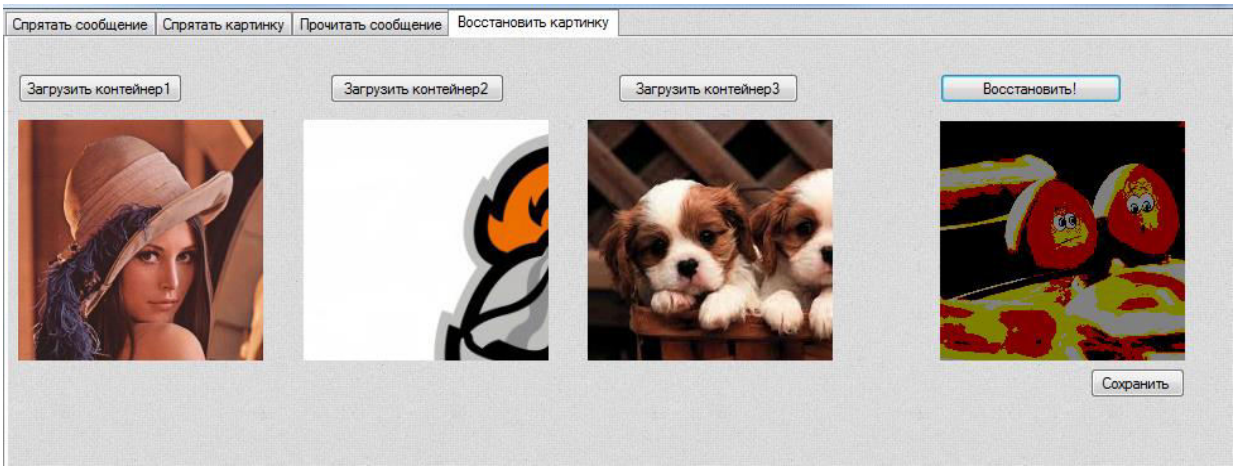

Рисунок 5 – Восстановление изображения при 1 замененном бите

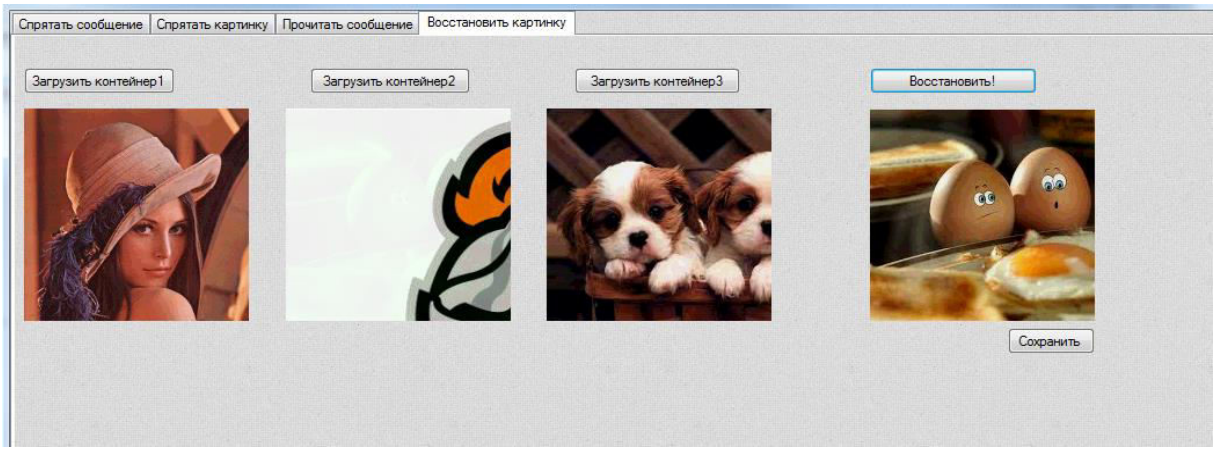

Рисунок 6 – Восстановление изображения с использованием 4 бит

Рисунок 7 – Восстановление изображения с использованием 8 бит

Таким образом, можно сделать вывод, что в качестве контейнеров лучше выбирать темные изображения, содержащие как можно меньше белого цвета, и использовать для записи не более 3-4 бит. Соблюдение этих рекомендаций поможет добиться оптимального баланса между качеством передаваемого изображения и степенью искажения контейнеров.

Заключение

В процессе выполнения выпускной квалификационной работы бакалавра были изучены методы стеганографии и разработана автоматизированная система защиты информации, реализующая сокрытие информации следующие методы стеганографии: метод LSB, метод Коха-Жао, метод Куттера-Джордана-Боссена и метод сокрытия цветных изображений bmp. Даны рекомендации по выбору контейнеров и количеству используемых бит в байте цвета пикселя контейнера.

Литература

1. Стеганография вчера, сегодня, завтра [Электронный ресурс] - http://www.ess.ru/sites/default/files/files/articles/1998/0405/1998_0405_03.pdf

2. Основные положения стеганографии [Электронный ресурс] - http://citforum.ru/internet/securities/stegano.shtml

3. Замена наименее значащего бита или LSB [Электронный ресурс] - http://www.nestego.ru/2012/07/lsb.html

4. Модификация метода скрытия информации Куттера-Джордана-Боссена [Электронный ресурс] - http://www.amursu.ru/attachments/article/11563/11.pdf

5. Стеганографический метод Куттера-Джордана-Боссена [Электронный ресурс] - http://habrahabr.ru/post/115287/

6. Стеганографического метод Коха-Жао [Электронный ресурс] - http://habrahabr.ru/post/216207/

7. Визуальная криптография для цветных изображений [Электронный ресурс] - http://habrahabr.ru/post/121878/