Лабораторная работа №4: **Методы встраивания информации в изображения**

Цель работы: разработка программы, реализующей один из методов встраивания информации в изображение.

1. Стеганография

Стеганография - это метод организации связи, который собственно скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания. Слово "стеганография" в переводе с греческого буквально означает "тайнопись" (steganos - секрет, тайна; graphy - запись). К ней относится огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные каналы и средства связи на плавающих частотах и т.д. Стеганография занимает свою нишу в обеспечении безопасности: она не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты. В настоящее время в связи с бурным развитием вычислительной техники и новых каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т. п. Это дает нам возможность говорить о становлении нового направления - компьютерной стеганографии. Из цифровой стеганографии вышло наиболее востребованное легальное направление - встраивание цифровых водяных знаков, являющееся основой для систем защиты авторских прав. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера (атакам). В результате необходимо встраивать информацию не только не заметно, но и так чтобы она была устойчива к различным видам атак. В общем случае типичная схема ЦВЗ выглядит следующим образом:

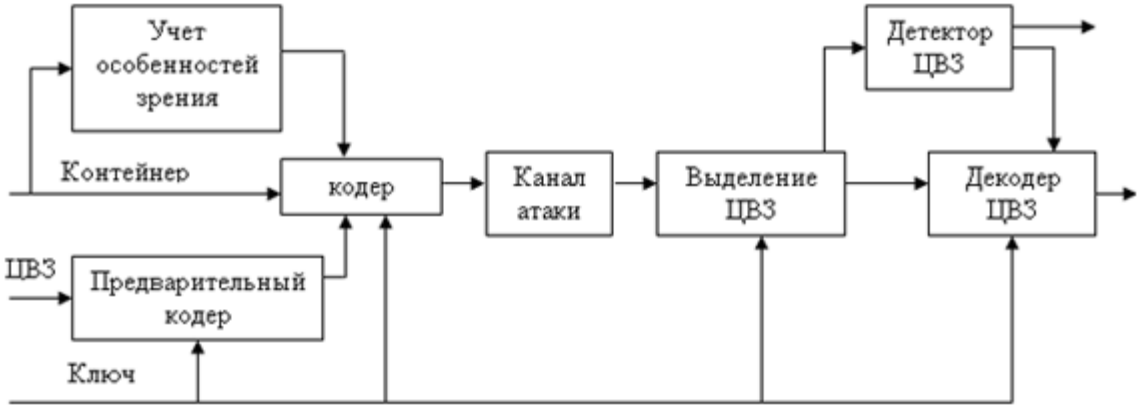

Рис. 1. Типичная стегосистема

- прекодер - устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в сигнал-контейнер (контейнером называется информационная последовательность, в которой прячется сообщение);
- стегокодер - устройство, предназначенное для осуществления вложения скрытого сообщения в другие данные с учетом их модели;
- устройство выделения встроенного сообщения;
- стегодетектор - устройство, предназначенное для определения наличия стегосообщения;
- декодер - устройство, восстанавливающее скрытое сообщение.

2. Алгоритм LSB

LSB (Least Significant Bit, наименьший значащий бит) — суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.

В нашем случае контейнером будет выступать картинка в формате BMP. Для начала рассмотрим структуру этого файла. Файл условно можно разбить на 4 части: заголовок файла, заголовок изображения, палитру и само изображение. Для наших целей надо знать только то, что записано в заголовке.

Первые два байта заголовка – это сигнатура BM, далее в двойном слове записан размер файла в байтах, следующие 4 байта зарезервированы и должны содержать нули и, наконец, в ещё одном двойном слове записано смещение от начала файла, до собственно байтов изображения. В 24-битном bmp-файле каждый пиксель кодируется тремя байтами RGB.

Воспользуемся методом LSB. Допустим, если очередной байт нашего секретного сообщения – 11001011, а байты в изображении –…11101100 01001110 01111100 0101100111…, то кодирование будет выглядеть так. Мы разобьём байт секретного сообщения на 4 двухбитовые части: 11, 00, 10, 11, и заменим полученными фрагментами младшие биты изображения: …11101**11** 01001**00** 01111**10** 0101100**11**…. Такая замена в общем случае не заметна человеческому глазу. Более того, многие старые устройства вывода, даже не смогут отобразить такие незначительные перемены.

Для простоты описания покажем принцип работы этого метода на примере 24-битного растрового RGB-изображения. Одна точка изображения в этом формате кодируется тремя байтами, каждый из которых отвечает за интенсивность одного из трех составляющих цветов (рис. 2) [1].

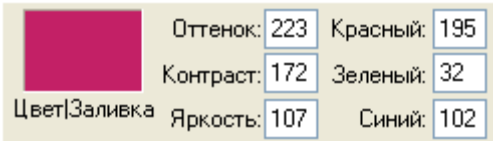

Рис. 2. Компоненты, составляющие исходное изображение

В результате смешения цветов из красного (R), зеленого (G) и синего (B) каналов пиксель получает нужный оттенок. Чтобы нагляднее увидеть принцип действия метода LSB, распишем каждый из трех байтов в битовом виде (рис. 3). Младшие разряды (на рисунке они расположены справа) в меньшей степени влияют на итоговое изображение, чем старшие. Из этого можно сделать вывод, что замена одного или двух младших, наименее значащих битов, на другие произвольные биты настолько незначительно исказит оттенок пикселя, что зритель просто не заметит изменения.

Допустим, нам нужно скрыть в данной точке изображения шесть бит: 101100. Для этого разобьем их на три пары (рис. 4) и заместим ими по два младших бита в каждом канале (рис. 5).

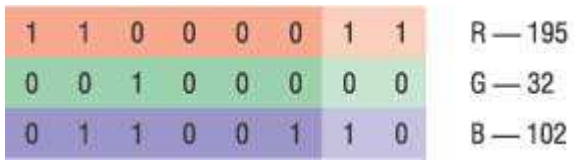

Рис. 3. Битовый вид исходного изображения (пикселя)

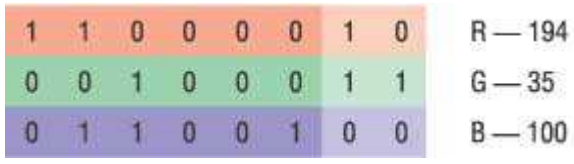

Рис. 4. Битовый вид измененного изображения (пикселя)

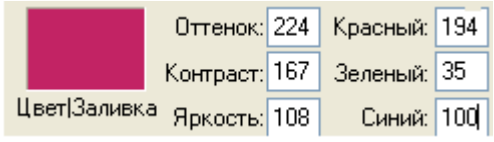

Рис. 5. Компоненты, составляющие измененное изображение

В результате мы получим новый оттенок, очень похожий на исходный. Эти цвета трудно различить даже на большой по площади заливке, хотя разница будет заметна по одной отдельной точке (рис. 6). Как показывает практика, замена двух младших битов не воспринимается человеческим глазом. В случае необходимости можно занять и три разряда, что весьма незначительно скажется на качестве картинки.

Рис. 6. Слева — оригинальный цвет, справа — цвет после модификации

Определим полезный объем такого RGB-контейнера. Занимая два бита из восьми на каждый канал, мы будем иметь возможность спрятать три байта полезной информации на каждые четыре пикселя изображения, что соответствует 25% объема картинки. Таким образом, имея файл изображения размером 400 Кбайт, мы можем скрыть в нем до 100 Кбайт произвольных данных так, что невооруженному глазу эти изменения не будут заметны.

Понятно, что можно менять не только 2 младших бита, но и любое их количество. Тут есть следующая закономерность: чем большее количество бит мы меняем, тем больший объём информации мы можем спрятать, и тем большие помехи в исходном изображении это вызовет.

Методы LSB являются неустойчивыми ко всем видам атак и могут быть использованы только при отсутствии шума в канале передачи данных. Обнаружение LSB-кодированного стего осуществляется по аномальным характеристикам распределения значений диапазона младших битов отсчётов цифрового сигнала.

3. 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.

И так, для встраивания информации будет использоваться синий цвет заданного контейнера-изображения.

Обозначения

$B_{x,y}$ — яркость синего цвета пикселя с координатами (x,y);

$B_{x,y}$* — изменённая яркость синего цвета пикселя;

$Y_{x,y}$ — яркость пикселя;

m_i — i-ый бит сообщения, которое мы хотим встроить;

λ — коэффициент, задающий энергию встраиваемого бита данных (задаётся исходя из функционального назначения и особенности стеганосистемы);

σ — размер области, по которой будет прогнозироваться яркость.

Встраивание

Встраивание информации будет производиться 1 бит сообщения в 1 пиксель контейнера. Секретный ключ задаёт координаты пикселей, в которые будет производиться встраивание.

При встраивании яркости красного и зелёного цветов остаются без изменений, а яркость синего — изменяется по следующей формуле:

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

где λ = 0.1, $Y_{x,y} = 0.3*R_{x,y}+0.59*G_{x,y}+0.11*B_{x,y}$

Извлечение

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 σ = 1÷3.Проиллюстрирую на примере (σ = 2):

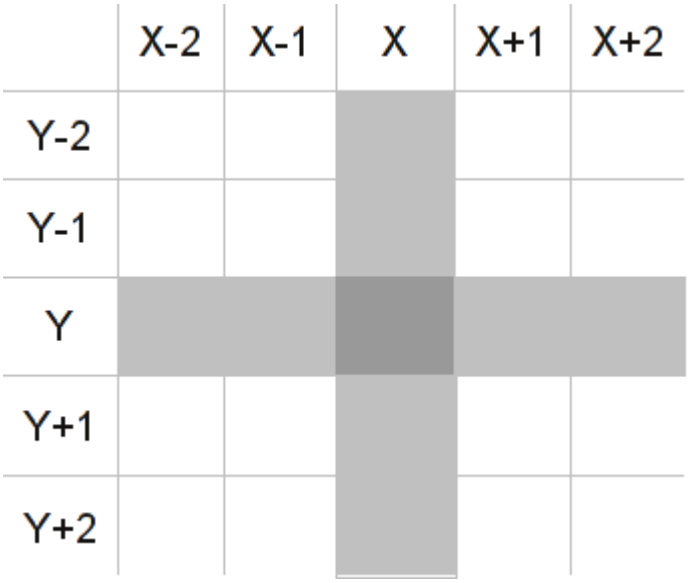

Рис. 7. Прогнозирование значения яркости

Пиксель в центре — это пиксель, яркость синего цвета которого мы должны спрогнозировать, опираясь на пиксели, которые обозначены светло серым цветом. И наконец, для извлечения скрытого сообщения используется формула:

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

Достоинства метода:

- Высокая пропускная способность;
- Высокая устойчивость к несанкционированному ознакомлению;
- Высокая устойчивость к частотному детектированию;
- Высокая устойчивость к разрушению младших бит контейнера;
- Устойчивость к атаке сжатия.

К недостаткам можно отнести то, что извлечение носит вероятностный характер.

Задание: реализовать один из двух рассмотренных алгоритмов.

Контрольные вопросы:

1. Основные понятия стеганографии?
2. Схема ЦВЗ?
3. Суть алгоритма LSB?
4. Особенности метода Куттера-Джордана-Боссена?

Список литературы:

1. Кузнецов А. Двоичная тайнопись. Компьютер Пресс 4`2004.
2. Конахович Г.Ф., Пузыренко А.Ю. «Компьютерная стеганография. Теория и практика». МК-Пресс, 2006. 288 с.
3. Грибунин В.Г., Оков И.Н., Туринцев И.В. «Цифровая стеганография», Солон-Пресс, 2002. 265 с.