Лабораторная работа № 6. Стеганографические методы защиты информации (4 часа)

6.1 ЦЕЛЬ РАБОТЫ

Изучение стеганографических методов защиты информации.

6.2 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Стеганография занимается разработкой методов передачи секретной информации, в которых скрывается само наличие передачи. 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.

Стеганографическая система, или стегосистема, – совокупность средств и методов, которые используются для формирования скрытого канала передачи информации (см. Рисунок 1).

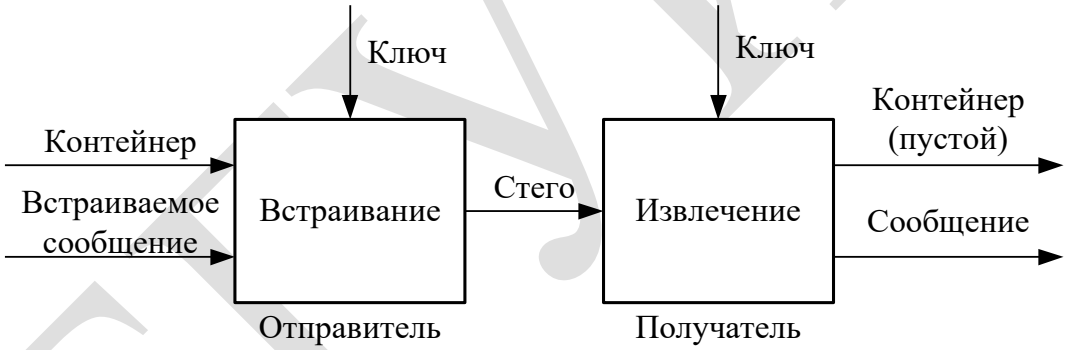

Рисунок 1. Обобщенная модель стегосистемы

В настоящее время можно выделить три тесно связанных между собой направления стеганографии: непосредственное сокрытие данных (сообщений), цифровые водяные знаки (watermark) и цифровые отпечатки (fingerprint). Цифровой водяной знак представляет собой некоторую информацию, которая добавляется к цифровому материалу и может быть позднее обнаружена или извлечена для предъявления прав на этот материал. Цифровой отпечаток представляет собой вариацию цифрового водяного знака с тем отличием, что каждая копия защищаемого материала имеет свою собственную уникальную метку, что позволяет впоследствии идентифицировать покупателя, через которого произошло нелицензионное копирование.

6.2.1 Метод LSB

Большинство существующих стеганографических систем использует для сокрытия информации метод замены наименее значащих битов в байтах или словах мультимедийных контейнеров (так называемый LSB-метод, от LSB – Least Significant Bit). Данный метод основан на том факте, что при оцифровке изображения или звука всегда присутствует погрешность дискретизации, равная наименьшему значащему разряду числа, определяющему величину цветовой составляющей элемента изображения или амплитуды звукового сигнала. Поэтому замена наименее значащих битов скрытым сообщением в большинстве случаев не вызывает значительной трансформации сигнала и не обнаруживается визуально или аудиально.

Рассмотрим использование данного 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: красного (Red), зеленого (Green) и синего (Blue). Интенсивность каждой составляющей лежит в пределах от 0 до 255, то есть каждая составляющая имеет 256 оттенков. Младшие разряды 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 пиксела, что зритель просто не заметит изменения (см. Рисунок 2). Максимальное количество возможных цветов для этого формата составляет более 16 миллионов. Однако следует иметь в виду, что глаз человека способен различать только около 4 тысяч цветов. Для кодирования этого количества цветов достаточно всего четырех битов $\left(\left\lceil \log_2 \sqrt[3]{4000} \right\rceil = 4\right)$. Как показывает практика, замена одного или двух младших битов не воспринимается человеческим глазом. В случае необходимости можно занять и три разряда, что весьма незначительно скажется на качестве картинки.

а)

R	1	1	0	0	0	0	1	1	195
G	0	0	1	0	0	0	0	0	32
B	0	1	1	0	0	1	1	0	102

б)

R	1	1	0	0	0	0	1	**0**	194
G	0	0	1	0	0	0	**1**	**1**	35
B	0	1	1	0	0	1	**0**	0	100

Рисунок 2. Внедрение последовательности из шести битов 101100 в младшие два бита цветовых составляющих одного пиксела RGB-изображения по методу LSB: *а*) – до внедрения; *б*) – после внедрения

Давайте подсчитаем 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 пиксела изображения, что соответствует 25 % объема картинки. Таким образом, имея файл

изображения размером 200 Кбайт, мы можем скрыть в нем до 50 Кбайт произвольных данных так, что невооруженному глазу эти изменения не будут заметны.

6.2.2 Метод Patchwork

Данный метод используется для постановки водяных знаков. Он основан на внесении изменений в два участка изображения: на участке A яркость изображения незначительно увеличивается, а на участке B – уменьшается. Рассмотрим основную идею Patchwork на примере изображения, в котором для простоты примем, что все возможные значения яркости пикселей распределены равномерно в диапазоне от 0 до 255.

Выберем на изображении случайным образом две точки A и B, яркость в которых равна a и b соответственно. Теперь положим, что

$$S = a - b.$$

Среднее значение разницы S (обозначим его M_S) после многократного повторения данной процедуры будет равно 0.

Теперь предположим, что описанная процедура повторяется n раз, полагая, что значения a, b и S на i-й итерации равны a_i, b_i и S_i соответственно. Тогда M_S выразится как

$$M_S = \sum_{i=1}^{n} S_i = \sum_{i=1}^{n} (a_i - b_i) = nS \approx 0.$$

Учитывая приведенные выше рассуждения, общий алгоритм встраивания метки может быть представлен следующим образом:

1. Используя оговоренный заранее секретный ключ как начальное значение для криптостойкого генератора псевдослучайных чисел, сгенерировать координаты пары точек (a_i, b_i).
2. Увеличить яркость изображения в точке a_i на значение δ, обычно выбираемое в диапазоне от 1 до 5 для изображения с 256 уровнями яркости.
3. Уменьшить яркость изображения в точке b_i на значение δ.
4. Повторить шаги 1–3 n раз (n выбирается порядка 10 000).

Модифицированное значение M_S^* может быть выражено как

$$M_S^* = \sum_{i=1}^{n} \left((a_i + \delta) - (b_i - \delta) \right) = 2\delta n + \sum_{i=1}^{n} (a_i - b_i) = 2\delta n + M_S.$$

Таким образом, с каждым новым шагом приведенного выше алгоритма накапливается отклонение на величину 2δ (см. Рисунок 3).

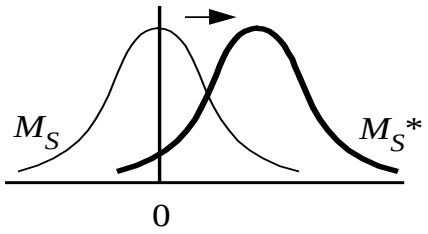

Рисунок 3. Сдвиг распределения M_S после внедрения водяного знака

Наличие подобного отклонения от ожидаемого значения свидетельствует о наличии встроенной в изображение метки. Таким образом, владелец может доказать свои интеллектуальные права на изображение, предъявив секретный ключ, который использовался для встраивания метки в изображения.

6.3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить теоретический материал по лабораторной работе.
2. Реализуйте стеганографическое внедрение сообщений с помощью метода LSB в контейнеры заданного формата (табл. 6.1, колонка 2). Количество внедряемых в каждую позицию контейнера битов задано в колонке 3.
3. (*) Реализуйте стеганографическую систему постановки и проверки цифрового водяного знака с помощью метода Patchwork. Параметры контейнера и метода заданы в колонках 4–6 таблицы 6.1.

Пояснение по выбору варианта:
Ваш_Номер_Варианта=(Номер_Вашей_зачетной_книжки) mod 8+1
Например №=123456
Выполнить задание согласно своему варианту (см. табл. 6.1).
(123456) mod 8 +1 = 0 + 1 = 1

Таблица 6.1.

№ варианта	Формат контейнера LSB	Количество заменяемых битов	Формат контейнера Patchwork	δ	n
1	2	3	4	5	6
1	графический	1	аудио	3	10000
2	аудио	2	графический	4	20000
3	графический	3	аудио	5	30000
4	аудио	1	графический	3	10000
5	графический	2	аудио	4	20000
6	аудио	3	графический	5	30000
7	графический	1	аудио	4	20000
8	аудио	2	графический	5	30000