**2. Стеганографические методы защиты мультимедиа информации**

1. Реализуйте стеганографическое внедрение сообщений с помощью метода LSB в контейнеры заданного формата (графический или аудио). Количество внедряемых в каждую позицию контейнера битов 2 или 3.
2. Реализуйте стеганографическую систему постановки и проверки цифрового водяного знака с помощью метода Patchwork. Параметры контейнера и метода: контейнер графический или аудио, = 3, 4 или 5, *n* = 10000, 20000 или 30000.

**Метод LSB**

Метод замены наименее значащих битов в байтах или словах мультимедийных контейнеров (Least Significant Bit, LSB) 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. 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 . В случае необходимости можно занять и три разряда, что весьма незначительно скажется на качестве картинки.

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.

**Метод Patchwork**

Данный метод используется для постановки водяных знаков. Он основан на внесении изменений в два участка изображения: на участке *А* яркость изображения незначительно увеличивается, а на участке *В* – 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 *А* и *В*, яркость в которых равна *а* и *b* соответственно. Теперь положим, что

*S* = *a* – *b*.

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

Теперь предположим, что описанная процедура повторяется *п* раз, полагая, что значения *а*, *b* и *S* на *i*-й итерации равны *ai*, *bi* и *Si* соответственно. Тогда *MS* выразится как



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 (*ai*, *bi*).
2. Увеличить яркость изображения в точке *ai* на значение *,* обычно выбираемое в диапазоне от 1 до 5 для изображения с 256 уровнями яркости.
3. Уменьшить яркость изображения в точке *bi* на значение *.*
4. Повторить шаги 1–3 *п* раз (*п* выбирается порядка 10 000).

Модифицированное значение ** может быть выражено как

.

Таким образом, с каждым новым шагом приведенного выше алгоритма накапливается отклонение на величину  (рис. 2).



Рисунок 2 – Сдвиг распределения *MS* 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.