ИСПОЛЬЗОВАНИЕ ДИСКРЕТНОГО КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ В СТЕГАНОГРАФИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Солонович Е. И.

Ярмолик В. Н. – д-р. техн. наук, профессор

Стеганография — это наука о скрытой передачи информации путём сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок или письмо. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

Основными требованиями к стеганографическому преобразованию являются незаметность вложения и устойчивость к различным изменениям контейнера.

В большинстве методов скрытия данных в изображениях используется та или иная декомпозиция изображения-контейнера. Среди всех линейных ортогональных преобразований наибольшую популярность в стеганографии получили вейвлет-преобразование и дискретное косинусное преобразование, что отчасти объясняется их успешным применением при сжатии изображений. Кроме того, желательно применять для скрытия данных то же преобразование изображения, как и то, которому оно подвергнется при возможном дальнейшем сжатии.

Таким образом, учитывая то, что наиболее вероятным методом сжатия изображения является JPEG то вполне обосновано при сокрытии данных, использовать именно дискретное косинусное преобразование, так как оно используется этим методом сжатия.

В общем, метод сжатия JPEG выглядит следующим образом: изображение преобразуется в цветовую схему YCbCr, при необходимости выполняется прореживание. Далее яркостный компонент Y и отвечающие за цвет компоненты Cb и Cr разбиваются на блоки 8x8 пикселов. Каждый такой блок подвергается дискретному косинусному преобразованию. Полученные коэффициенты квантуются (для Y, Cb и Cr в общем случае используются разные матрицы квантования) и пакуются с использованием кодирования серий и кодов Хаффмана.

Одним из наиболее распространенных стеганографических алгоритмов использующих дискретное косинусное преобразование является алгоритм описанный E. Koch.

В данном алгоритме в блок размером 8x8 осуществляется встраивание 1 бита информации. К блоку применяется ДКП и псевдослучайно выбираются два коэффициента. Встраивание информации осуществляется следующим образом: для передачи бита 0 добиваются того, чтобы разность абсолютных значений коэффициентов была бы больше некоторой положительной величины, а для передачи бита 1 эта разность делается меньше некоторой отрицательной величины.

$$\left| c_b\left(j_{i,j},k_{i,1}\right)\right| - \left| c_b\left(j_{i,2},k_{i,2}\right)\right| > \varepsilon, \quad \text{если } s_i = 0,$$
$$\left| c_b\left(j_{i,j},k_{i,1}\right)\right| - \left| c_b\left(j_{i,2},k_{i,2}\right)\right| < -\varepsilon, \quad \text{если } s_i = 1.$$

Где b - номер блока, (j,k) - позиция коэффициента внутри блока, ε - порог вложения, S_i - встраиваемый бит.

После встраивания информации выполняется обратное дискретное косинусное преобразование.

Существуют возможности для улучшения этого алгоритма. Можно определить блоки, которые по определенным признакам наиболее подходят для встраивания информации. Например, было установлено, что наиболее подходящими являются блоки, не являющиеся слишком гладкими, а также не содержащие малого числа контуров. Для первого типа блоков характерно равенство нулю высокочастотных коэффициентов, для второго типа – очень большие значения нескольких низкочастотных коэффициентов. Также возможно изменение алгоритма, уменьшающее искажения контейнера, а именно: использование трех вместо двух ДКП коэффициентов. При этом для встраивания бита изменяется один из трех коэффициентов таким образом, чтобы он был больше или меньше остальных двух (в зависимости от встраиваемого бита). В том случае, если такая модификация приведет к слишком большой деградации изображения, коэффициенты не изменяются, и этот блок просто не используется либо выбираются другие коэффициенты.

Изменение трех коэффициентов вместо двух, а тем более отказ от изменений в случае неприемлемых искажений уменьшает вносимые погрешности. Декодер всегда сможет определить блоки, в которые информация не встроена, повторив анализ, выполненный в кодере.

Таким образом, использование ДКП в стеганографии более чем оправдано. Исключается наиболее распространённый вид искажений контейнера и существенно уменьшается заметность вложений.