изменяется.

На рисунке 2 представлены результаты экспериментальных сравнений обычной и эффективной реализаций алгоритма HMAC.

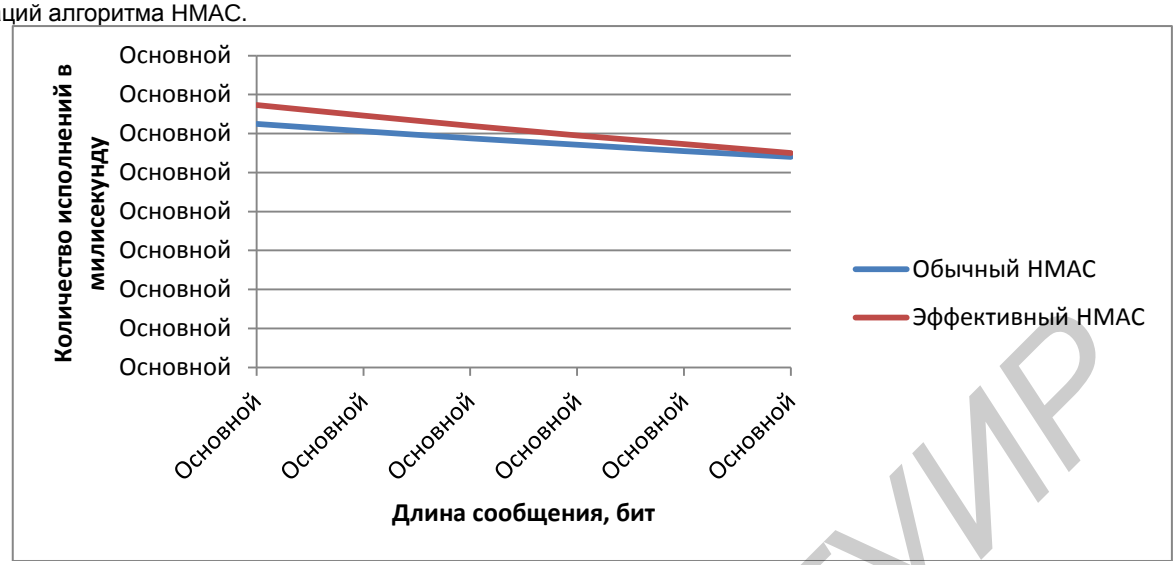

Рис. 2 – Сравнение производительности обычной и эффективной реализаций алгоритма аутентификации сообщений HMAC

Экспериментальное сравнение алгоритмов показало, что предлагаемая реализация HMAC действительно превосходит в эффективности обычную реализацию алгоритма. Данное превосходство наблюдается для коротких сообщений с длиной до 400 байт. Для сообщений большей длины разница в производительности сглаживается, т.к. количество хеш-преобразований при генерировании кодов аутентичности намного больше числа преобразований, удавшееся сократить в эффективной версии алгоритма.

Список использованных источников:

1. Stallings, W. Cryptography and Network Security Principles and Practices, Fourth Edition / W. Stallings. – Prentice Hall, Ca, 2005.
2. Ярмолик, В. Н. Теория информации / В. Н. Ярмолик // Уч. метод. пособие для студентов специальности I – 40 01 01 "Программное обеспечение информационных технологий" дневной и дистанционной форм обучения. – Минск: БГУИР, 2004. – 118 с.: ил.
3. Занкович, А. П. Защита информации: практикум для студентов специальности I – 40 01 01 «Программное обеспечение информационных технологий» дневной и дистанционной форм обучения / А. П. Занкович. – Мн.: БГУИР, 2006. – 39 с.: ил.

ВНЕДРЕНИЕ СТЕГАНОГРАФИЧЕСКОГО СООБЩЕНИЯ В ИЗОБРАЖЕНИЯ ФОРМАТА JPEG

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

Герман Н. В.

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

В современном обществе очень популярен обмен изображениями, гигабайты графической информации ежедневно проходят через социальные сети и средства личного общения. Таким образом, с использованием стеганографии можно передавать значительное количество информации, факт передачи которой является предметом сокрытия.

Стеганографические системы предназначены для передачи по открытым каналам связи таким образом, что сторонний наблюдатель не может обнаружить передачу секретной информации помимо открытой информации. Безусловно, наибольшую вместимость будут иметь форматы сжатия без потерь, однако их применение на сегодняшний день крайне ограничено, в то время как обмен изображениями в формате JPEG распространён довольно широко. Это делает JPEG изображения логичным выбором в качестве стеганографического контейнера.

Существует возможность помещения секретного сообщения в области, предназначенные для метаинформации и неиспользуемые при декодировании изображения области. Однако, такие техники не заслуживают внимания в связи с тем, что их применение легко обнаружить. Другие техники внедрения секретного сообщения связаны с алгоритмом сжатия формата JPEG. Преобразование изображения в формат JPEG происходит в несколько этапов:

1. Преобразование представления цветов к формату YCbCr
2. Децимация (сокращение количества пикселей)
3. Разбиение изображения на блоки размером 8x8 пикселей.
4. Применение к блокам дискретного косинусного преобразования (DCT). [1]
6. Квантизация значений, полученных на предыдущем шаге. Точность определяется коэффициентом качества.
7. Энтропийное кодирование (RLE и код Хаффмана). На этом шаге потери данных не происходит.

Внедрение секретного сообщения, как правило, происходит путём манипуляции коэффициентами DCT после квантизации, между шагами 5 и 6.

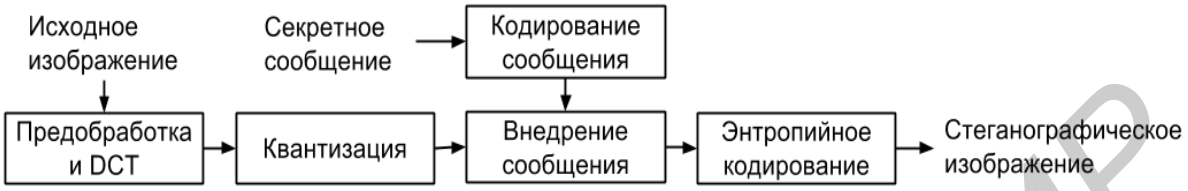

Рис. 1 – Структурная схема формирования сигнала

Сообщение может внедряться различными способами. В простейшем случае младшие биты DCT коэффициентов заменяются битами секретного сообщения (классический LSB метод). Очевидно, что без дополнительных мер по сокрытию внедрения такой метод неприменим, зачастую в связке с ним используют также предварительное шифрование внедряемого сообщения для предотвращения внесения отслеживаемых статистических характеристик , а также использование псевдослучайных последовательностей для вычисления позиций внедрения бит для более равномерного влияния на статистические характеристики изображения.

Метод Jsteg базируется на LSB, но пропускает все нулевые и единичные байты, так как обычно первых значительно больше, чем вторых и факт внедрения очень легко определить по размытию пика на диаграмме распределения значений коэффициентов. В оригинальной реализации не производит предварительного шифрования сообщения, однако существуют реализации с его поддержкой.

Метод F5 [2] так же основывается на LSB. В нём используется псевдослучайная последовательность для выбора позиции записи, матричное кодирование внедряемого сообщения (n бит кодируется в 2^n-1 путём изменения одного бита). В случае необходимости изменения бита абсолютное значение соответствующего коэффициента уменьшается на единицу. Менее подверженная обнаружению версия F5 - nsF5 использует “wet paper codes”.

Метод J2 использует топологический подход к графической стеганографии: информация внедряется в пространственную составляющую (яркость пиксела), хотя изменения производятся над частотными коэффициентами (после DCT): коэффициенты подбираются таким образом, чтобы младшие биты значений яркостей пикселов совпадали с битами сообщения. Предусмотрен пропуск блоков со сликом большим количеством нулевых коэффициентов, в которые невозможно внедрить очередной блок секретного сообщения.

J2 существенно уменьшает число нулей и увеличивает число единиц среди коэффициентов DCT. Поэтому ему на смену был разработан метод J3. Метод J3 нацелен на сохранение распределения значений коэффициентов DCT. Достигается это следующим образом: все возможные значения коэффициентов разбиты на пары (2n, 2n+1) (по модулю); (-1, 1) составляют особую пару, 0 не входит ни в одну пару. Все изменения значений происходят в рамках этих пар. По мере внедрения секретного сообщения учитываются все изменения. Как только достигается ситуация, при которой восстановление баланса в паре потребует изменения всех оставшихся коэффициентов одного из значений этой пары внедрение прекращается, баланс восстанавливается, а позиция в которой возникла ситуация сохраняется вместе с идентификатором пары как “стоп-точка”. По выполнении алгоритма все стоп-точки помещаются в область метаданных изображения. Ключевым недостатком данного метода является необходимость использования области метаданных.

В результате проведенного анализа можно заключить, что внедрение стеганографического сообщения в изображение формата JPEG целесообразно производить согласно методу nsF5. Представляется возможной также модификация метода J3, не использующая область метаданных, обнаружение применения которой будет являться также крайне затруднительным. Использование метода F5 позволяет несколько повысить вместимость контейнера, но при этом уменьшает скрытность. Использование методов Jsteg и LSB нецелесообразно в связи с неустойчивостью получаемого изображения к стегоанализу.

Список использованных источников:

1. ISO/IEC 10918-1 : 2011 “Information technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines”
2. A. Westfeld. F5—A Steganographic Algorithm. High Capacity Despite Better Steganalysis (https://f5-steganography.googlecode.com/files/F5%20Steganography.pdf)