УДК 004.056

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ВСТРАИВАНИЯ ИНФОРМАЦИИ В ВЕКТОРНЫЕ ИЗОБРАЖЕНИЯ

Менщиков А. А., Полев А. В.,
научный руководитель канд. техн. наук Шниперов А.Н.
Сибирский федеральный университет

В настоящее время проблема стеганографической защиты информации от несанкционированного доступа является чрезвычайно актуальной. Современные стеганографические методы чаще всего основаны на встраивании секретной информации в мультимедийные контейнеры, информация в которых изначально имеет аналоговую природу. Однако существует проблема изученности стеганографических алгоритмов. Для них существуют отработанные методики стеганографического анализа.

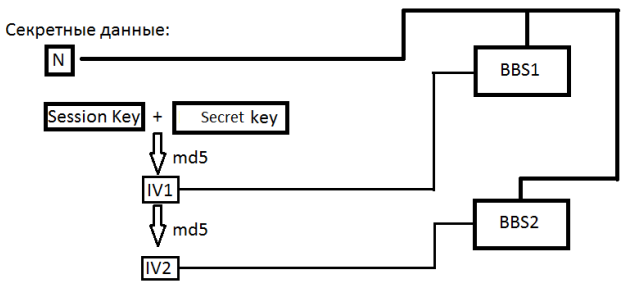
В процессе изучения данной проблемы, нами была выявлена резко возросшая популярность векторных форматов изображений, которые сейчас поддерживаются всеми современными интернет браузерами и активно внедряются на веб-ресурсах, что является прекрасным стеганографическим каналом.

Предлагаемая нами стеганосистема использует методику встраивания информации в векторные изображения форматов, которые основаны на десятичном представлении чисел. Самым популярным форматом такого типа является формат SVG. SVGбазируется на языке разметки XML. Он поддерживает различные виды графики, в том числе анимацию. В данный момент активно внедряется на веб-ресурсах вместо растровых изображений. Разработанный нами стеганографическим метод базируется на встраивании информации в векторные изображения формата SVG на основе избыточности данных.

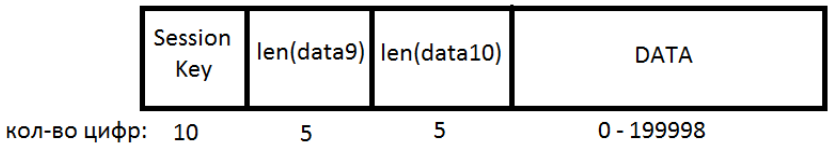
Схема передачи секретного сообщения выглядит следующим образом:

1. Отправитель имеет секретные данные. Он переводит их в десятичную (девятичную)систему счисления, назовем полученное число M.
2. Отправитель находит контейнер C, для которого выполняется len(M) < |C|.
3. Отправитель встраивает M→C и публикует полученный файл в сети.
4. Получатель скачивает файл, автоматически получая последовательность Cm.
5. Получатель, зная алгоритм и операцию «→», извлекает M.

Секретное сообщение после предварительной обработки внедряется в координаты SVG, которые представлены десятичными дробями. Для первичной защиты данных и выравнивания статистических показателей, мы используем гаммирование на основе алгоритма Blum Blum Shub (BBS).Для инициализации генератора используются секретные данные, которыми отправитель и получатель обменялись по безопасному каналу, а также сессионные одноразовые ключи.



Сообщение разделяется на блоки, которые после операции сложения по модулю 2 (XOR) с результатом работы BBS переводятся частично в десятичную, частично в девятичную систему счисления и познаково встраиваются в контейнер.



Примечания:
SessionKey – сессионныйключ.
Len(data9) – длина девятичной части данных.
Len(data10) – длина десятичной части данных.
DATA – сами данные.

Стойкость обеспечивается наличием секретного и сессионного ключей. Векторы инициализации для BBS получаются путем последовательного применения алгоритмов хеширования над конкатенацией ключей.

Разработанный стеганографический метод позволяет встраивать любые данные, а модульная структура – наращивать возможности.

Объем скрываемых данных с приемлемой надежностью скрытия имеет порядок 7% от объема контейнера. Причем количество знаков, используемых для встраивания, поддается регулированию. Таким образом, имеется возможность оптимально подобрать соотношение объема скрываемых данных и надежности скрытия.

На данный момент нами разработана модель стеганосистемы, программное обеспечение и проведены статистические тесты, которые подтверждают приемлемые стеганографические свойства по отношению к пассивному противнику.