УДК 004.56+003.26

М.Г. Савельева, асп.
(БГТУ, г. Минск)

МЕТОД СТЕГАНОГРАФИЧЕСКОГО ВНЕДРЕНИЯ ТАЙНОЙ ИНФОРМАЦИИ В WEB-ДОКУМЕНТЫ НА ОСНОВЕ РАСТРОВОЙ ГРАФИКИ

Актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации. Современные компьютерные технологии, прогресс в области глобальных компьютерных сетей и средств мультимедиа обеспечивают возможность разработки и реализации новых методов, предназначенных для обеспечения компьютерной информационной безопасности. Одна из самых новых горячих точек в исследованиях безопасности – это сокрытие информации. Она обусловлена двумя важнейшими политическими проблемами информационной эпохи – защитой авторских прав и государственным надзором.

Стеганография является эффективным программно-техническим методом сокрытия данных и защиты их от несанкционированного доступа. Использование стеганографии совместно с другими методами защиты информации обеспечивает многоуровневую безопасность [1].

Методы текстовой стеганографии можно разделить на три основные категории: основанные на формате, или синтаксические методы, лингвистические, или основанные на обработке естественного языка, методы, а также основанные на случайной и статистической генерации.

Работа с текстовыми документами подразумевает, что содержимое документа должно быть абсолютно точно передано при обратном преобразовании.

Формально модель задается следующим выражением:

$$\sum = (M, L, K, E, F, F^{-1})$$

Зафиксируем множество возможных сообщений $M = \{M_1, M_2, \ldots, M_m\}$, множество возможных контейнеров $L = \{L_1, L_2, \ldots, L_l\}$, и множество возможных заполненных контейнеров (стеганограмм) $E = \{E_1, E_2, \ldots, En\}$.

Зафиксируем множество отображений:

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}, \quad (1)$$

где

$$\varphi_i: (M, L) \to E, i = 1, 2, \ldots, k. \quad (2)$$

Определим обратное отображение:

$$\varphi_i^{-1}: E \to (M, L), \quad (3)$$

которое каждому элементу множества E ставит в соответствие элемент множества M и элемент множества L.

Зафиксируем множество ключей $K = \{K_1, K_2, \ldots, K_k\}$ так, что для всех $i = 1, 2, \ldots, k$ отображение $\varphi_i \in \varphi$ однозначно задается ключом K_i. Каждое конкретное отображение φ_i из множества φ соответствует способу встраивания сообщения из множества M в контейнер из множества L при помощи конкретного ключа K_i [2].

Данный метод подразумевает рассмотрение текстового документа как графического объекта растровой графики.

В качестве базового элемента контейнера, свойства которого модифицируются при осаждении информации, выступает пиксель изображения, входящего в массив пикселей служащих для отображения символа текста, не включая непечатные символы.

Используется цветовая модель RGB. RGB – цветовая модель, представление цвета которой задается совокупностью трех цветовых каналов: красного, зеленого и синего. Каждый из каналов имеет размер в один байт, из чего следует, что цвет одного пикселя представляется в виде трех байт. Каждый цветовой канал задается 8-разрядным двоичным вектором либо соответствующим десятичным числом:

$$R, G, B \in \{0, 1\} \text{ либо } R, G, B \in \{0, 1, \ldots, 255\}.$$

Во втором случае часто говорят об интенсивности трех составляющих цвета.

Предлагается следующий метод для внедрения тайной информации в web-документы. Начальным этапом является преобразование web-документа в файл растровой графики формата без сжатия, например, PNG, и выбор секретного сообщения. Зафиксируем документ-контейнер как L, сообщение как M. Длина внедряемого сообщения N_M. Выбранное секретное сообщение необходимо преобразовать в двоичный вид, на данном этапе используется кодировку ASCII, в которой один символ представлен 8 битами. Следовательно, $N_M = length(M) \times 8$.

Для внедрения информации необходимо выбрать набор пикселей, где совпадает значение одного или нескольких цветовых каналов. Из массива выбирается базовый пиксель. Дальнейшее внедрение будет происходить в цветовой канал, который не использовался при выборе массива пикселей, при сравнительном анализе пикселя для внедрения с базовым.

Если значение цветового канала пикселя для внедрения значительно отчается от значения того же цветового канала базового пикселя (5 и более), то значение цветового канала, который использовал-

ся при выборе пикселей изменить на 1. Таким образом, этот пиксель перестанет попадать в массив пикселей для внедрения, так как значительное изменение цветового канала будет очевидно для человеческого глаза.

Если значение цветового канала базового пикселя больше чем пикселя для внедрения, то бит внедряемого сообщения равен 0.

Если значение цветового канала базового пикселя меньше чем пикселя для внедрения, то бит внедряемого сообщения равен 1.

Если полученный бит не совпадает с битом внедряемого сообщения, то значение цветового канала пикселя для внедрения нужно изменить на 5 единиц в необходимую сторону.

В качестве ключей может использоваться информация какой канал или несколько каналов используется для выбора пикселей для внедрения, номер базового пикселя в массиве.

Для внедрения сообщения необходимо $N_M + 1$ пикселей при условии внедрения в каждый пиксель. Исходя из того, что в среднем из 100 пикселей 5 будут подходить для внедрения, то для внедрения сообщения длиной 8 бит необходимо изображение 15×15 пикселей, для внедрения сообщения длиной 80 бит – 45×45 пикселей.

Данный метод можно использовать и для форматов изображений с незначительным сжатием, изменяя значения каналов более значительно.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Кузнецов, А. А. Математическая модель и структурная схема стеганографической системы / А. А. Кузнецов, А. А. Смирнов, Е. В. Мелешко // Збірник наукових праць Кірово-градського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: КНТУ, 2012. – Вип. 25, ч. 1. – С. 273-281.

3. Савельева М. Г. Метод стеганографического внедрения тайной информации в web-документы на основе растровой графики.