УДК 003.26

А.Н. Николайчук, маг.; П.П. Урбанович, проф., д-р. техн. наук
(БГТУ, г. Минск)

АНАЛИЗ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ НА ОСНОВЕ КОНТЕЙНЕРОВ SVG-ФОРМАТА

Стеганография изображений играет важную роль для передачи секретных данных по компьютерным сетям и каналам связи [1]. Существует большое количество методов для конкретных контейнеров, в которые скрытно помещается информация. Формат SVG предоставляет разнообразный набор таких методов, благодаря структуре его файла.

SVG (Scalable Vector Graphics) – это язык описания двумерной графики в формате XML. SVG может использовать три вида графических объектов: фигуры векторной графики (могут описываться как прямыми, так и кривыми линиями), изображения и текст.

Основу SVG составляют базовые геометрические фигуры: прямоугольники, эллипсы, ломаные линии и т. д. Для таких фигур существуют свои теги и задаются при помощи атрибутов для обозначения начальных координат и размеров. Для создания сложных графических объектов можно использовать общий элемент path, который определяется одним атрибутом *d*. Атрибут *d* содержит серию команд и параметров, используемых этими командами. Команды обозначаются специальными буквами. Например, команда *Переместиться к*, обозначается буквой *M*. В качестве параметров она принимает координаты точки, к которой перемещается; или команда *Линия к*, вызываемая буквой *L*, принимает два параметра – координаты точки *x* и *y*, и рисует линию от текущего положения к этой точке.

С помощью SVG мы можно использовать добавление и отображение текста в изображении. Для этого используется отдельный тег <*text*>. Для того чтобы выровнять текст по задаваемому пути используют тег <*textPath*>. SVG тег <*image*> позволяет выводить растровые изображения внутри SVG-объектов.

Стеганография изображений может быть представлена с помощью растровых и векторных изображений. Методы для растровых изображений можно разделить на два класса: методы пространственной области и методы частотной области. Для пространственной области основные процедуры внедряют скрытое сообщение в младшие биты цифрового кода пикселей изображения (например, на основе известного метода LSB). Для частотных процедур осаждаемое сообщение вставляется в частотную характеристику изображения.

Пространственные процедуры включают методы внедрения цифрового кода сообщения в изображение и замены:

– метод наименее значащего бита (LSB) – незначащий или малозначащий младший бит цвета или палитры изображения заменяется битом вставляемого сообщения;

– псевдослучайные перестановки – биты сообщения распределены по изображению случайным образом. Этот подход увеличивает трудоемкость выявления скрытого сообщения, особенно если псевдослучайный датчик генерирует последовательность сложным алгоритмом.

Частотные процедуры состоят в замене малозначащих частотных характеристик изображения, например, в замене некоторых коэффициентов в дискретном косинус-преобразовании, а также дискретное вейвлет-преобразование. Эти и некоторые другие методы обычно применяются в патчах и методах расширения спектра:

– метод с использованием патчей – статистическое кодирование информации путем изменения некоторых статистических свойств контейнера (добавление избыточных данных к скрытому сообщению и затем размытие его по изображению с применением гауссового распределения) и использует проверку гипотез при извлечении сообщения;

– метод расширения спектра – комбинирует расширение спектра, кодирование с исправлением ошибок и обработку изображений для скрытия вставляемого сообщения [2].

В отличие от растровых изображений, представленных совокупностью бит, векторные используют описание расположение геометрических фигур, а стеганометоды основываются на их преобразовании:

– механизм модификации дробных частей констант геометрических фигур аналогичен LSB для растровых изображений, путем добавления информации в значения координат, будет происходить незначительное изменение элементов фигур, не заметное человеческому глазу, в виду того, что значения крайне малы;

– встраивание дополнительных точек в ребра состоит в использовании расстояний между точками для передачи информации; так как точки лежат на самой фигуре, они не меняют ее внешний вид, а лишь меняют ее внутреннее представление [3–4];

– внедрение дополнительных вершин в описание геометрических фигур.

Существует большое количество методов для преобразования текста, как например метод конечных пробелов и табуляций, где «0» представлен одним пробелом, а «1» двумя. Для SVG допустимыми

будут методы для языков разметки, где преобразования производятся с тегами и их атрибутами:

– представление сообщения битовой последовательностью и замена в файле «0» одинарными кавычками, а «1» – двойными;

– использование специальных кодов для пробела; пробел может быть закодирован разной последовательностью символов, таким образом можно принять за «0» и «1» разные значения последовательностей;

– изменение значений атрибутов тегов;

– изменение регистра букв тегов; представление верхнего регистра тега для «1», нижнего – для «0».

Все методы сокрытия сообщений имеют свои сильные и слабые стороны. Выбирая метод встраивания информации необходимо опираться на множество факторов. Файлы SVG чаще всего используются для графического представления объектов, поэтому даже при допустимой возможности размещения текстовой информации ее объем будет слишком мал для того, чтобы использовать текст в роли контейнера. В таких файлах объекты в основном создаются с помощью команд тега <*path*>, количество тегов также будет недостаточно для внедрения тайной информации в разметку. Так как формат не предоставляет никаких дополнительных возможностей для растровых изображений, то нет оснований для того, чтобы использовать их как контейнер внутри файла SVG. Поэтому для этого формата наиболее разумно скрывать информацию в дополнительных преобразованиях фигур векторной графики, представленных с помощью тега <*path*>.

ЛИТЕРАТУРА

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

2. Сейеди, С.А. Сравнение методов стеганографии в изображениях/ С.А. Сейеди, Р.Х. Садыхов // Информатика. – 2013. – № 1(37). – С. 66–75.

3. Блинова, Е.А. Стеганографический метод на основе встраивания дополнительных значений координат в изображения формата SVG / Е.А. Блинова, П.П. Урбанович // Труды БГТУ. Серия 3. – 2018. – № 1. – С. 104–109.

4. Blinova, E.A. Steganographic method based on hidden messages embedding into Bezier curves of SVG images / E. A. Blinova, P. P. Urbanovich // Journal of the Belarusian State University. Mathematics and Informatics. – 2021. – № 3. – P. 68–83.