ний при прочих равных условиях и демонстрирует явное преимущество над последним по всем показателям.

Литература

1. Тявловский, А.К. Анализ дефектов поверхности исходных подложек алюминия и его сплавов методом сканирующего зонда Кельвина / А.К. Тявловский, А.Л. Жарин, О.К. Гусев, Р.И. Воробей, Н.И. Мухуров, Г.В. Шаронов, К.В. Пантелеев // Приборы и методы измерений. – 2017. – Т. 8, № 1. – С. 61–72. DOI:10.21122/2220-9506-2017-8-1-61-72

2. Пантелеев, К.В. Цифровой измеритель контактной разности потенциалов / К.В. Пантелеев, А.И. Свистун, А.К. Тявловский, А.Л. Жарин // Приборы и методы измерений. 2016. – Т. 7, № 2. – С. 136–144.

УДК 621.391

ОЦЕНКА ПРИМЕНЕНИЯ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ С ИСПОЛЬЗОВАНИЕМ ИЗОБРАЖЕНИЯ В КАЧЕСТВЕ КОНТЕЙНЕРА

Ковынёв Н.В.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Использование стеганографии с контейнером в виде изображения относится к процессам сокрытия данных в файлах цифровых изображений различных типов.

Цифровое изображение можно представить в виде конечного набора цифровых значений, которые называются пикселями. Пиксель – наименьший отдельный неделимый элемент изображения, который содержит значения, представляющие яркость определенного цвета в конкретной точке. Исходя из данных определений, можно представить изображение в виде матрицы или двумерного массива, содержащих фиксированное количество строк и столбцов.

Рассматривая термин «цифровое изображение», используют понятие «растровая графика». Растровая графика представляет структуру данных с точечной матрицей, которая предстает в виде сетки пикселей, которая может храниться в файлах изображений при различных форматах.

Исходя из определения термина «пиксель», можно утверждать, что каждый пиксель – образец исходного изображения. Отсюда следует вывод: чем больше представлено образцов, тем лучше и точнее представляется оригинальное изображение. Каждый пиксель имеет определенную интенсивность, которая переменна. Обычно цвет представляют тремя или четырьмя интенсивностями компонентов в системах цветовой визуализации, для систем из трех компонентов чаще всего используются следующие цвета: красный, зеленый, синий. Для систем из четырёх компонентов чаще всего используют: черный, желтый, голубой, пурпурный.

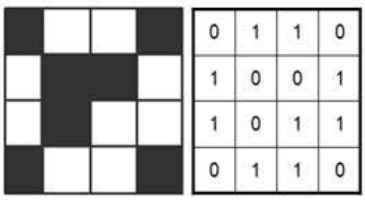

Рисунок 1 – Пример кодирования цветов пикселя

Каждый пиксель имеет определенные значения, которые можно представить в виде двоичного кода, работая с которым можно наблюдать более значимые и менее значимые биты пикселей изображения.

Рисунок 2 – Пример представления числа в виде массива бит

Изменение наиболее значимого бита изображения оказывает огромное влияние на конечное значение изображения. Например, если изменить значение наиболее значимого бита с 1 но 0 (в двоичном виде замена будет выглядеть следующим образом: с 11111111 на 01111111), то десятичное значение данного битам изменится с 255 на 127. Обратная данной замене – замена наименее значимого бита, которая оказывает меньшее влияние на конечное значение изображения. Например, если значение наименее значимого бита изменить с 1 на 0 (в двоичном виде замена будет выглядеть следующим образом: с 11111111 на 11111110), то десятичное значение данного бита изменится с 255 на 254. Исходя из данных замен видно, что наименее значимый бит меняется только на 1, что меньше 1 %, так как полный диапазон состоит из 256.

Исходя из данных, использованных при заменах пикселей, можно сделать вывод, что каждый пиксель имеет три значения: красный, зеленый и синий (RGB: Red, Green, Blue). Каждое значение цветов (RGB) восьмиразрядное, может хранить восемь двоичных значений. Соответственно, если изменить наименее значимые биты, то можно получить незначительное влияние на конечное изображение. Данное незначительное влияние –

стеганографический ключ, скрывающий информацию внутри изображения. Для наиболее успешного стеганографического преобразования изображения нужно изменить наименее значимые биты исходного изображения, включив в них наиболее значимые биты из другого (секретного или передаваемого) изображения. Данные преобразования характерны для метода младшего значащего бита или LSB (Least Significant Bit). Данный метод наиболее распространен в стеганографии с использованием изображений.

Остальные стеганографические алгоритмы, которые используют изображение в качестве контейнера, используют в своих реализациях воздействие на яркость в каких-либо определенных участках изображения, которые незначительно влияют на исходное изображение (контейнер). Стоит отметить, что изменения яркости контейнера не нарушают скрытность передачи стеганографического сообщения.

Стеганографические контейнеры в виде изображений на данный момент очень сильно распространены, их применяют в сферах защиты авторских прав, сферах идентификации и подлинности документов, сокрытия передаваемых сообщений, защита от контрафактного использования товаров и услуг. Также стеганографию в изображениях применяют и авторы вредоносного или шпионского программного обеспечения. Использование данного метода актуально среди злоумышленников, так как антивирусные средства и средства защиты мало что могут сделать с заполненными контейнерами, потому что их трудно обнаружить, так как они выглядят как обычные графические файлы.

Рассмотрим положительные и отрицательные стороны применения данных методов стеганографии с изображениями. К положительным сторонам можно отнести следующее:

– неизменность размера файла контейнера;

– замены битов в канале трудно заметить визуально;

– возможность варьирования пропускной способностью, при помощи изменения количества заменяемых бит;

– при использовании изображений с большим разрешением, можно получить контейнер большой емкости;

– методы не требуют дополнительной предобработки (в частности шифрования) исходного изображения;

– возможность скрытой передачи большого объема информации;

– многие методы просты в использовании и легки в реализации (например, методы, связанные с особенностями форматов файлов).

Несмотря на большое количество достоинств данных методов, стеганография в изображениях имеет ряд недостатков, такие как:

– слабая устойчивость к статистическому стегоанализу;

– высока вероятность нарушения порядка бит в цветовых векторах изображения, что приведет к разрушению стегоконтейнера;

– слабая устойчивость к перекодировкам изображения, ввиду чего скрытое сообщение может быть утеряно (пересылка по электронной почте или мессенджерам);

– легкое детектирование наличия стегосообщения;

– низкая защищенность;

– неустойчивость методов к обработкам файла-контейнера;

– сообщение трудно восстановить, если изображение подвергается атаке (например, сдвиг или поворот).

Рассмотрев все достоинства и недостатки стеганографии в изображения можно сделать вывод, что использование графических изображений в виде контейнеров для стеганографической передачи информации имеет широкое распространение как при передаче информации по открытым каналам, так и для ведения вредоносной или шпионской деятельности. Также стеганография в изображениях используется для подтверждения авторства, проверки подлинности документов. Исходя из преимуществ и недостатков каждого алгоритма сокрытия, можно выбрать для использования подходящий алгоритм.

В заключении можно сказать, что при передаче информации, скрываемой в файле изображения, необходимо отдавать предпочтения методам кодирования и расширения спектра сигнала. Кроме того, само сообщение необходимо зашифровать стойким криптоалгоритмом, чтобы при перехвате сообщения, было сложнее получить передаваемую информацию. В тоже время графические изображения вызывают много подозрений при передачи их по открытым каналам, ввиду чего скрытая передача информации стеганографическими методами переходит к текстовым файлам, так как на данный момент текстовые файлы вызывают меньше подозрений при передаче по открытым каналам.

Литература

1. Коробейников А.Г, Кувшинов С.С., Блинов С.Ю., Лейман А.В., Кутузов И.М. Цифровые водяные знаки в графических файлах / Научно-технический вестник информационных технологий, механики, оптики. – 2013. – № 1. – С. 152–157.

2. Конахович Г.Ф., Пузыренко А.Ю., Компьютерная стеганография. Теория и практика. – К. «МК-Пресс». – 2006. – 288 с.

3. Васина Т.С. Обзор современных алгоритмов стеганографии / Электронное научно-техническое издание «Наука и образование» МГТУ им. Н.Э. Баумана. – 2012. – С. 1–8.