УДК [004.056+003.26](075.8)

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ И РЕАЛИЗАЦИИ КОМБИНИРОВАННОГО МЕТОДА ТЕКСТОВОЙ СТЕГАНОГРАФИИ

Н. П. Шутько

Белорусский государственный технологический университет, Минск
e-mail: shutko_bstu@mail.ru

Стеганография становится одним из важнейших направлений решения задач в области тайной передачи данных и защиты авторских прав на электронный контент [1].

В статье [2] рассмотрено понятие одноключевой стеганографической системы $\sum^{o}$, которая состоит из совокупности сообщений M, контейнеров C, ключей K^{o}, стегоконтейнеров (заполненных контейнеров) S и преобразований (прямого F и обратного F^{-1}), которые их связывают:

$$\sum^{o} = (M, C, K^{o}, S, F, F^{-1}).$$

При этом предполагалось, что по аналогии с криптографической системой стеганосистема основана на использовании одного ключа, который отождествляется с методом осаждения или извлечения информации.

Развитием одноключевой модели стала многоключевая, анализ которой проводился, например, в [2]. Это было обусловлено тем, что множество ключей, входящих в математическую модель стеганосистемы, можно представить в виде некоторого количества подмножеств ключей.

Многоключевая стеганосистема позволяет внедрять скрытую информацию в носитель с использованием нескольких ключей. В отличие от обычных стеганосистем многоключевая стеганосистема позволяет создавать различные комбинации ключей, управляющих процессом встраивания и извлечения тайного сообщения, что повышает уровень безопасности и стойкости стеганографической системы.

Следуя упомянутой выше аналогии между криптографической и стеганографической системами, стойкая к атакам стеганосистема должна также строиться согласно известному постулату Керкхоффса [1]: безопасность системы должна основываться не только на секретности самого алгоритма осаждения или извлечения тайной информации, но и главным образом на секретности ключа.

В рамках представляемого в настоящей статье исследования концепцию многоключевой стеганосистемы предлагается реализовать в виде сочетания двух методов текстовой стеганографии. Первым из них является метод, основанный на встраивании секретной информации за счет изменения цветовых координат символов текста, созданного с помощью текстового процессора MS Word в цветовой модели RGB [3].

Математически модель RGB удобнее всего представлять в виде куба. В этом случае каждая его пространственная точка однозначно определяется значениями координат X, Y и Z. Для анализа можно воспользоваться математическим описанием цветового пространства, изложенным в фундаментальном научном исследовании М. Гуревича [4]. Автор этой работы связывает произвольный цвет Φ с определенной точкой цветового пространства и, наоборот, каждую точку цветового пространства связывает с определенным цветом. При использовании такой модели цвет Φ может быть представлен в цветовом пространстве с помощью вектора, описываемого уравнением:

$$\Phi = r\mathrm{R} + g\mathrm{G} + b\mathrm{B},$$

где R, G, B – постоянные, линейно независимые (основные) цвета: красный, зеленый и синий; r, g, b – количественные (весовые) коэффициенты в выбранной шкале, которые указывают число единиц каждого из трех составляющих цветов в составе цвета Φ. Такой подход позволяет формализовать применение и описание известного метода наименее значащих битов (LSB) [1].

Другим методом из указанной комбинации стеганопреобразования будет выступать метод, основанный на изменении такого пространственно-геометрического параметра символа текста, как кернинг или апрош [5]. Отметим, что, например, изменение величины апроша между двумя определенными символами текста относительно базового значения a_o на небольшое расстояние (пункты (пт) или доли пункта) Δa формально можно представить в следующем виде: $a' = a_o + \Delta a$.

Такое изменение не должно вызывать визуально заметного уплотнения ($\Delta a < 0$) или разрежения ($\Delta a > 0$) групп символов. В MS Word апрош может принимать значения в диапазоне от 0 до 1584 пт. Столь широкий диапазон гарантирует достаточно высокую емкость метода, под которой понимается количество тайной информации в расчете на единицу объема контейнера.

Для того чтобы использовать одновременно два метода текстовой стеганографии, предлагается разделить объем осаждаемой информации на две части, причем части будут не равнозначные по объему.

Необходимо определить, в какие символы будет производиться встраивание с помощью метода изменения цвета символа, а в какие – с помощью метода изменения апроша или кернинга. В работе [6] приведен сравнительный анализ отмеченных выше методов для оценивания их стойкости. Опытным путем было установлено, что метод изменения цветовых координат обладает достаточной стойкостью при условии, что стегоконтейнер с зашифрованным сообщением будет храниться и передаваться в электронном виде. Кроме того, цвет символов сохраняется при условии конвертации документов в формат *.pdf и обратно.

Однако если проанализировать возможные манипуляции потенциального пользователя с документом-контейнером, то можно определить, что наиболее часто изменяются такие параметры форматирования, как выравнивание, кегль и семейство шрифтов, апрош и цвет. В связи с этим осаждать стегосообщение предлагается следующим образом. Встраивание в буквы и цифры документа-контейнера будет производиться с помощью метода изменения кернинга (ввиду редкого использования данного параметра), а в знаки пунктуации и пробельные элементы – с помощью метода изменения цветовых координат.

Таким образом, встраивание секретной информации будет осуществляться в разные типы символов, что позволит повысить стойкость стегоконтейнера ко взлому. При извлечении информации необходимо применить соответствующие методы стеганографии, чтобы получить обе части секретной информации и объединить их вместе.

Список литературы

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

2. Urbanovich, P. Theoretical Model of a Multi-Key Steganography System / P. Urbanovich, N. Shutko // Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science. – Vol. 2, Ch. 11. – Lublin : KUL, 2016. – P. 181–202.

3. Шутько, Н. П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста / Н. П. Шутько, Д. М. Романенко, П. П. Урбанович // Труды БГТУ. Сер. VI: Физ.-мат. науки и информатика. – 2015. – № 6. – С. 152–156.

4. Гуревич, М. М. Цвет и его измерение / М. М. Гуревич. – М.-Л.: Изд-во АН СССР, 1950. – 267 с.

5. Shutko, N. The use of aprosh and kerning in text steganography / N. Shutko // Electrical Review (Przeglad elektrotechniczny). – 2016. – № 10. – P. 222–225.

6. Шутько, Н. П. Стойкость стеганографических документов-контейнеров при их конвертации на основе цветовых моделей RGB И HSL / Н. П. Шутько // XXV Туполевские чтения (Школа молодых ученых) : Междунар. молодежная науч. конф., Казань, 10–11 нояб. 2021 г. – Т. 5. – Казань, 2021. – С. 748–752.