# ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ МЕТОДОВ ИЗБЫТОЧНОГО КОДИРОВАНИЯ В СТЕГАНОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

Урбанович П. П., Плонковски М. Д., Савельева М. Г., Шутько Н. П.
Кафедра информационных систем и технологий,
Белорусский государственный технологический университет
Кафедра прикладной информатики,
Люблинский Католический университет Яна Павла II
Минск, Республика Беларусь; Люблин, Польша
E-mail: {p.urbanovich, saveleva, n.shutko}@belstu.by, marcin.plonkowski@kul.pl

*Проанализированы некоторые важные прикладные особенности совместного использования методов помехоустойчивого кодирования данных и стеганографии. Стеганографические преобразования основаны на цветовых моделях RGB и HSL, а также на использовании метода наименее значащих битов (LSB). Комбинация двух видов преобразования позволяет тайно передавать или хранить информацию, а также повышает ее защищенность при конвертациях стеганоконтейнера.*

## Введение

В последнее время особенно остро встал вопрос о защите электронных документов, которые передаются по сети Интернет. Это обусловлено, в первую очередь, тем, что многие учреждения и компании перешли на удаленный режим работы, основной объем информации (в том числе текстовой) передается онлайн. Один из инструментов решения задачи связан с использованием стеганографии.

Стеганографические алгоритмы позволяют скрывать конфиденциальные сообщения ($M$) в других сообщениях (контейнерах, $C$). При этом могут преследоваться две основные цели: тайная передача сообщения и размещение невидимого цифрового водяного знака для защиты авторских прав на контент (контейнер). Злоумышленник должен иметь минимальные возможности для того, чтобы выявить сам факт такого сокрытия и/или извлечь тайное сообщение из стеганоконтейнера (контейнера со скрытым сообщением). При этом необходимо обеспечить сохранение целостности осажденной информация при случайных, намеренных или преднамеренных модификациях (конвертациях) стеганоконтейнера. Для решения такой комплексной задачи стеганоалгоритмы («чистая стеганография») дополняются средствами избыточного кодирования. Использование избыточного (помехоустойчивого) кодирования размещаемой информации обеспечивает контроль ошибок в этой информации при ее извлечении, а также повышает стойкость стеганоконтейнера к атакам [1].

## I. Зависимость целостности осажденной в контейнер информации от используемого формата его конвертации

Если стеганоканал (стеганоконтейнер, $S$) создается на основе электронных документов, то модифицировать можно как отдельные пространственно-цветовые параметры текста, так и отдельные атрибуты файла-контейнера [2-4].

В основе многих преобразований лежит цветовая модель RGB и метод наименее значащих битов (LSB). При разработке контента на основе технологии web и CSS 3 можно использовать наряду с RGB также модель HSL (Hue–Saturation–Lightness – тон–насыщенность (цвета)–светлота (цвета) или визуальная оценка яркости) – это альтернативная цветовая модель, разработанная для более полного соответствия тому, как человеческое зрение воспринимает цветообразующие свойства. В связи с тем, что документ-контейнер с внедренной в него тайной информацией М может подвергаться анализу или обработке в различной среде, представляет интерес оценить, в какой степени осажденная информация на основе использования одной цветовой модели сохраняется при переходе на другую модель: RGB – в HSL или HSL – в RGB.

Отметим, что модель HSL является представлением модели RGB в цилиндрической системе координат. HSL представляет цвета более интуитивным и понятным для восприятия образом, чем RGB. Модель часто используется в графических приложениях, в палитрах цветов и для анализа изображений. HSL имеет цилиндрическую геометрию. Для того чтобы определить тон (Hue, H) нужно указать градус поворота (от 0° до 360°) цветового спектра замкнутого в цветовой круг: радуга, замкнутая в круг, в котором красный цвет всегда ориентирован на север, и угол равен 0°, 120° – это зелёный, 240°– синий. Между этими основными цветами расположены все остальные оттенки цветового спектра.

Использование в качестве контейнера текстового (word) документа характеризуются необходимостью учета ряда специфических особенностей. К основным из таких особенностей относятся: стандартная кодировка символов текста в принятой цветовой модели – 0, 0, 0; изменение стандартной кодировки в цветовых каналах (в

одном, в любых двух или в трех одновременно) в диапазоне от 1 до 4 младших битов (от 1 до 15 из 255) визуально обнаружить практически нельзя; конвертация файла-контейнера по схеме doc(docx) – pdf – doc(docx) уменьшает цветовой код символа в каждом канале на одну единице (на 1 бит). Дополнительно нами для анализа целостности $M$ при конвертации $S$ в различные графические форматы (BMP, GIF, JPG, TIFF) было использовано оригинальное изображение размером 2154×3721 пикселей (1 259 216 байтов). После внедрения сообщения ($M$ = ITS-2022) изображение-контейнер стало занимать 1 261 348 байтов. Были рассмотрены следующие варианты конвертации: PNG–BMP–PNG, PNG–GIF–PNG, PNG–JPG–PNG, PNG–TIFF–PNG. Извлечение сообщения после конвертации происходило из файла, обратно преобразованного в формат PNG.

Конвертация выполнялась с помощью разных сервисов. При использовании Adobe Photoshop сообщение $M$ сохраняется в полном объеме (без ошибок) при конвертации в форматы BMP, JPG, TIFF. При конвертации изображения-контейнера сервисов cloudconvert.com, image.online-convert.com и www.freeconvert.com, как правило, извлеченное сообщение состояло из всех нулей (при конвертации в BMP и TIFF) либо из всех единиц (при конвертации в GIF).

Существуют такие наборы параметров в обеих моделях (RGB и HSL) , которые практически не изменяют при конвертации контейнера цвет модифицированного при стеганографическом преобразовании объекта (символа). Это является положительным фактом, свидетельствующим в пользу стеганографической стойкости рассмотренного метода [5].

## II. Кодирование внедряемого в контейнер сообщения на основе избыточного кода

Модель преобразования исходного сообщения (кодирование/декодирование + стеганография) обычно выполняется двояко: 1) независимое (от содержимого пустого контейнера) избыточное кодирование внедряемого сообщения $M$ с выполнением необходимых последующих операций [6], кодирование с учетом этого содержимого [1]. Можно также объединить оба подхода с учетом вышеприведенных особенностей и результатов конвертации стеганоконтейнера. Каждый mi символ размещаемого текстового сообщения $M$, представленный кодом ASCII ($k = 8$ бит), можно разделить на 2 части по 4 бита каждая: $X_{k1,i} = x_{1i}, x_{2i}, x_{3i}, x_{4i}; X_{k2,i} = x_{5i}, x_{6i}, x_{7i}, x_{8i}$. Далее необходимо сложить по модулю два (XOR) $X_{k1,i}$ и $X_{k2,i} : x_{1i} + x_{5i} = x_{r1,i}, ..., x_{4i} + x_{8i} = x_{r4,i}$. Вычисленные биты четности составят 4-битное избыточное слово, $X_{ri}$. Полубайты некоторого символа mi тайного текста, $X_{k1,i}$ и $X_{k2,i}$, а также избыточного слова $X_{ri}$ записываются по отдельности в каналы, соответствующие трем цветам модели RGB некоторого символа $c_j$ текста-контейнера $C$. Такой модифицированный символ обозначим $c_{jm}$. Следующая модификация $c_{jm}$ ($(c_{jm})$') приведет к тому, что кодовые расстояния между парами векторов ($X_{k1,i}$ и $(X_{k1,i})$', $X_{k2,i}$ и $(X_{k2,i})$', $X_{ri}$ и $X_{ri}$') будут не равны нулю. Это предопределяет реализацию дальнейших шагов по восстановлению исходных слов $X_{k1,i}$ и $X_{k2,i}$. С другой стороны, это может использоваться для доказательства нарушения прав интеллектуальной собственности.

## III. Список литературы


1. Bierbrauer, J., Fridrich J. Constructing Good Covering Codes for Applications in Steganography. In: Shi, Y.Q. (eds) Transactions on Data Hiding and Multimedia Security III. Lecture Notes in Computer Science, vol. 4920. – Berlin, Heidelberg: Springer, 2008. – P. 1–22.
2. Савельева, М. Г. Метод стеганографического преобразования web-документов на основе растровой графики модели RGB / М. Г. Савельева, П. П. Урбанович // Труды БГТУ. Сер.3. Физико-математические науки и информатика. – 2022. – № 2 (260). – С. 90–107.
3. Shutko, N. Method of syntactic text steganography based on modification of the document-container aprosh / N. Shutko, P. Urbanovich, P. Zukowski // Przegląd Elektrotechniczny. – 2018. –Vol. 6. – P. 82–85.
4. Урбанович, П. П. Использование системных свойств и параметров текстовых файлов в стеганографических приложениях / П. П. Урбанович, Д. Э.Юрашевич // Теоретическая и прикладная криптография : материалы международной научной конференции, Минск, 20-21 октября 2020 г. – Минск : БГУ, 2020. – С. 68-73.
5. 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): Международная молодёжная научная конференция, 10–11 ноября 2021 года: Материалы конференции. Сборник докладов. – В 6 т.; Т. 5. – Казань: Изд-во ИП Сагиева А.Р., 2021. С. 748–752.
6. Урбанович, П. П. Коррекция одиночных и двойных парных ошибок в стеганографических каналах передачи информации / П. П. Урбанович // Информационные системы и технологии = Information Systems and Technologies [Электронный ресурс] : материалы междунар. науч. конгресса по информатике. В 3 ч. Ч. 1, Респ. Беларусь, Минск, 27–28 окт. 2022 г. / Белорус. гос. ун-т ; редкол.: С. В. Абламейко (гл. ред.) [и др.]. – Минск: БГУ, 2022. – С. 113–119.