Список использованных источников

1. Днепровская Н.В. Формирование инновационной среды цифровой экономики: дис. …д-ра экон. наук. Москва. 2020. 361 с.
2. Шевцова, И. В. Социальные медиа в коммуникации между гражданами и органами государственного управления / И. В. Шевцова, Н. В. Днепровская Н. В. // Государственное управление. Электронный вестник. – 2015. – № 51. – С. 145.
3. Силкина Г.Ю., Шабан А.П. Цифровые инновации: сущностные характеристики и особенности. π-Economy, 2023, 16 (5), 51–62

УДК 004.56+003.26

М.Г. Савельева
Белорусский государственный технологический университет
Минск, Беларусь

ОБЩАЯ КОНЦЕПЦИЯ СТЕГАНОГРАФИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ РАСТРИРОВАННЫХ ИЗОБРАЖЕНИЙ

Аннотация. *Представлена общая концепция стеганографического моделирования для растрированных изображений. Математическая модель стеганографической системы предназначена как для размещения скрытых меток в целях защиты авторского права на электронные документы, выступающих в качестве контейнера, так и для скрытой передачи данных.*

M.G. Saveleva
Belarusian State Technological University
Minsk, Belarus

GENERAL CONCEPT OF STEGANOGRAPHIC MODELING FOR RASTERIZED IMAGES

Abstract. *The general concept of steganographic modeling for rasterized images is presented. The mathematical model of the steganographic system is designed both for placing hidden labels in order to protect copyright on electronic documents acting as a container, and for hidden data transmission.*

Благодаря цифровым сетям и репозиториям доступ к электронным документам стал проще. Но неправомерное копирование, публикация или распространение защищенных авторским правом (в

том числе и цифровым водяным знаком (ЦВЗ)) материалов незаконно. Для защиты авторских прав разрабатываются методы и инструменты, такие как стеганография [1].

При передаче или модификации электронных документов часто происходит изменение их оригинального состояния. Конвертация контента из одного формата в другой может негативно повлиять на стеганоконтейнер *S*. Проблемы могут возникнуть из-за особенностей форматов и алгоритмов сжатия, которые могут нарушить стеганографическую информацию в ЦВЗ. Поэтому при изменении форматов следует быть осторожным и учесть возможные последствия для стеганографической информации.

Стеганоконтейнеры могут быть частью растровой или векторной графики. Форматы, которые представляют растровое изображение, склонны к потере качества и детализации. Векторные форматы, такие как PDF или SVG, сохраняют текст как математические формулы, обеспечивая более точное воспроизведение. При растрировании векторных контейнеров происходит преобразование векторной графики в растровое изображение. Однако, при этом возникают ограничения в разрешении и качестве изображения.

Потеря четкости и создание градиентов оттенков цвета пикселей при растрировании текста могут быть использованы в стеганографии для передачи данных. Внедрение информации в символы контейнера на основе их геометрических параметров может увеличить пропускную способность и стойкость стеганографических каналов. Это позволяет скрыть информацию, используя изменения в градиентах, текстуре или других характеристиках символов. Такие методы полезны в области информационной безопасности и тайной передачи данных.

В [2] были представлены методы и алгоритмы стеганографического преобразования, которые используют элементы web-приложений, основанные на растровой графике, в качестве контейнера. Основной элемент контейнера – пиксель изображения, цветовые параметры которого изменяются в модели RGB при встраивании информации. Внедрение и извлечение информации происходит в пикселях с одинаковыми значениями (одно из 256) в одном или нескольких цветовых каналах. Разработанный метод отличается тем, что внедрение и извлечение информации происходит путем анализа значений одной или двух цветовых координат базового пикселя и пикселя для внедрения. Количество цветовых каналов (R, G, B), используемых для выбора пикселей и встраивания сообщения, зависит от цветовых характеристик изображения и длины сообщения.

Формально процесс встраивания (осаждения) тайных сообщений M, с помощью которого, в частности, можно решать упомянутую задачу защиты авторского права на контент, содержащийся в документах из множества C, можно описать как стеганографическую модель [3].

Модель строится на основе следующих положениях. Полагаем, что $\boldsymbol{M}$ − множество скрываемых сообщений, $\boldsymbol{M} = \{M_1, M_2, \ldots, M_n\}$, $\boldsymbol{C}$ − множество контейнеров (в нашем случае − изображения), $\boldsymbol{C} = \{C_1, C_2, \ldots, C_r\}$ $(r > n)$, $\boldsymbol{K_г}$ − множество ключей для генерации авторской информации (параметры, связанные с выбором способа внедрения сообщения в контейнер, параметры шифрования или сжатия сообщения, уникальные идентификаторы для аутентификации и авторизации доступа к сообщению и т.д.), $\boldsymbol{K_г} = \{K_{г1}, K_{г2}, \ldots, K_{гt}\}$, $\boldsymbol{K_в}$ − множество ключей для методов внедрения авторской информации (параметры для изменения цвета, или других свойств для встраивания информации в контейнер, уровни компрессии или шифрования, применяемые к модифицированному контейнеру, цветовые преобразования или методы, используемые для внедрения информации в изображение и т.д.), $\boldsymbol{K_в} = \{K_{в1}, K_{в2}, \ldots, K_{вg}\}$.

Произвольное тайное сообщение M можно скрыть в контейнере C при использовании ключей $K_г$ и $K_в$, где $M \in \mathbf{M}$, $C \in \mathbf{C}$; $K_г \in \boldsymbol{K_г}$, $K_в \in \boldsymbol{K_в}$. Результатом такого преобразования будет стегоконтейнер S, $S \in \boldsymbol{S}$ $\{(M_1, C_1, K_{г1}, K_{в1}), (M_2, C_2, K_{г2}, K_{в2}), \ldots, (M_x, C_x, K_{гx}, K_{вx})$.

Формально процесс встраивания (осаждения) тайных сообщений $\boldsymbol{M}$, с помощью которого, в частности, можно решать упомянутую задачу защиты авторского права на контент, содержащийся в документах из множества $\boldsymbol{C}$, можно описать как отображение $\boldsymbol{F}$:

$$\boldsymbol{F}: \boldsymbol{M}\times\boldsymbol{C}\times\boldsymbol{K_г}, \boldsymbol{K_в} \rightarrow \boldsymbol{S}. \qquad (1)$$

Процесс извлечения $\boldsymbol{M}$ из стеганоконтейнеров $\boldsymbol{S}$ описывается функцией, обратной к F:

$$\boldsymbol{F^{-1}}: \boldsymbol{S}\times\boldsymbol{K_г}, \boldsymbol{K_в} \rightarrow \boldsymbol{M}, \boldsymbol{C}. \qquad (2)$$

Таким образом стеганографическая модель определяется как:

$$\boldsymbol{SF} = (\boldsymbol{SC}, \boldsymbol{C}, \boldsymbol{M}, \boldsymbol{K_г}, \boldsymbol{K_в}, \boldsymbol{F}, \boldsymbol{F^{-1}}), \qquad (3)$$

где $\boldsymbol{SC}$ – стеганографический канал

$$\boldsymbol{F}: \boldsymbol{C} \rightarrow \boldsymbol{SC}. \qquad (4)$$

Описанная математическая модель стеганографической системы отличается от известных моделей наличием ключей $\boldsymbol{K_г}$ и $\boldsymbol{K_в}$. Модель предназначена как для размещения скрытых меток в целях защиты

авторского права на электронные документы, выступающих в качестве контейнера, так и для скрытой передачи данных.

Список использованных источников

1. Конахович, Г. В. Компьютерная стеганография. Теория и практика / Г. В. Конахович, А. Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

2. Савельева М. Г., Урбанович П. П. Метод стеганографического преобразования web-документов на основе растровой графики и модели RGB // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2022. № 2 (260). С. 99–107.

3. Шутько, Н. П., Листопад Н. И., Урбанович П. П. Моделирование стеганографической системы в задачах по охране авторских прав // Восьмая Междунар. научно-техн. конф. «Информационные технологии в промышленности» (ITI`2015): тезисы докладов. Минск, ОИПИ НАН Беларуси, 2015. С. 30–31.

УДК 61:004.9

Н.Ш. Самедов
Тамбовский государственный университет им. Г.Р. Державина
Тамбов, Россия

ЦИФРОВИЗАЦИЯ В МЕДИЦИНЕ. ПОСТКОВИДНЫЙ СИНДРОМ

Аннотация. *Статья рассматривает влияние процесса цифровизации на сферу медицины с фокусом на постковидный синдром. В статье рассматривается роль цифровых технологий в диагностике постковидного синдр ома и сопровождающей его медицинской помощи, а также в реабилитации пациентов.*

N. Sh. Samedov
Tambov State University named after G.R. Derzhavin
Tambov, Russia

DIGITALIZATION IN MEDICINE. POSTCOVID SYNDROME

Abstract*. This article examines the impact of digitalization on the field of medicine with a focus on postcovid syndrome. The article discusses the role of digital technology*