Рисунок 4 – Главная страница сайта Телесеть (источник – https://teleset.plus/)

В заключение необходимо отметить, что использование актуальных тенденций – только часть успеха для любого веб-проекта. Важно, чтобы проект обладал индивидуальностью, был узнаваемым и отражал концепцию компании или организации. А для этого веб-дизайнеру, как проводнику идей по организации контента и визуализации компонентов сайта необходимо постоянно развиваться, учиться, осваивать новые инструменты дизайна.

ЛИТЕРАТУРА

1 Psychology through Critical Auto-Ethnography: Academic Discipline, Professional Practice and Reflexive History. – Routledge. – 2020.

2 Главные тренды веб-дизайна в 2023 году: [Электронный ресурс] / Сайт CONTENTED. – 2023. – Режим доступа: https://media.contented.ru/. – Дата доступа: 14.02.2023.

УДК 004.056.55

Доц. Н.П. Шутько
(БГТУ, г. Минск)

АНАЛИЗ СТОЙКОСТИ ТЕКСТОВЫХ СТЕГАНОКОНТЕЙНЕРОВ К ИЗМЕНЕНИЮ ТИПА НОСИТЕЛЯ ИНФОРМАЦИИ

Стеганография как наука с каждым годом получает все большее развитие. Во многом это обусловлено широким спектром ее применения в различных областях. Одним из интересных и перспективных направлений является применение методов стеганографии для защиты прав интеллектуальной собственности [1]. То есть, секретные данные, в качестве которых в данном случае будет выступать какая-то авторская информация, например, дата создания произведение, его автор и т. д. встраиваются в документ-контейнер с помощью выбранного стеганографического метода. В данной работе интерес представляют текстовые стеганоконтейнеры, информация в которые была осаждена

с использованием стеганографического метода, основанного на модификации цветовых параметров символов текста [2].

Исследование емкости и устойчивости при конвертации документов с встроенным сообщением с использованием, указанных выше методов в формат *.pdf уже проводились ранее. В данной статье было решено провести анализ стойкости текстовых стеганоконтейнеров к изменению типа носителя информации. То есть исследовать, сохраняется ли секретное сообщение в документе-контейнере после такого рода изменений и можно ли его извлечь без потери содержимого.

Первоначально был выбран текстовый документ в формате *.doc в качестве контейнера, в который будет происходить встраивание. Количество символов с пробелами в данном документе 1233, без пробелов – 1096. Секретным сообщением было слово «секрет».

Для анализа стойкости метода на основе модификации цветовых параметров к изменению типа контейнера предполагалось встроить авторское сообщение в выбранный контейнер с помощью программного обеспечения Sword, определив предварительно последовательность, которая будет выступать в роли ключа (рис. 1). Затем текстовый документ-стегоконтейнер (контейнер со встроенной тайной информацией) необходимо было напечатать, отсканировать и проанализировать устойчивость метода к такого рода деформациям.

Для чистоты эксперимента было принято решение производить печать документа на различных устройствах. Одним из таких было выбрано многофункциональное устройство Canon, другим являлось цветное многофункциональное устройство Konica Minolta bizhub C364.

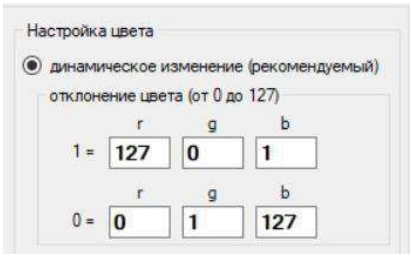

Рисунок 1 – Последовательность ключей

Цвет символов после печати не соответствовал оригиналу. Это объясняется тем, что цвет символов на экране монитора описывается с помощью цветовой модели RGB, тогда как при печати цвета конвертируются в цветовую модель CMYK. Ввиду этой важной особенности цвет символов после сканирования не соответствовал исходным значениям. Таким образом, необходимо отметить, что при использовании метода модификации цветовых координат нужно учитывать форму,

в которой будет хранится в дальнейшем документ с осажденным сообщением для корректной его работы.

Кроме того, в ходе проведения эксперимента была также проанализирована стойкость стеганоконтейнера к искажениям, которые возникают в случае отправки электронного документа по почте. Проведенный анализ показал, что при пересылке по электронной почте изменений в стегоконтейнере не произошло. Искажений не было выявлено, цвета измененных символов соответствуют исходным. Встроенное секретное сообщение также было извлечено с помощью программного обеспечения Sword (рис. 2).

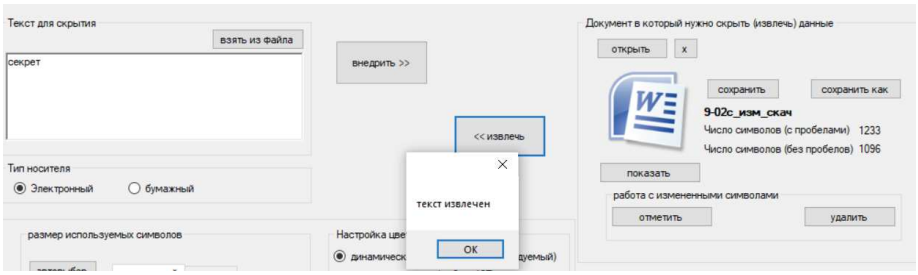

Рисунок 2 – Интерфейс программного средства Sword

Как уже упоминалось выше, печать проводилась не только с помощью МФУ, но и с помощью цифровой печатной машины. Разрешение печати − 1800 × 600 dpi. Разрешение принтера или цифровой печатной машины подразумевает под собой максимальное количество точек на квадратный дюйм, которые печатающее устройство может напечатать за определенное количество проходов печатающей головки. Сам термин «разрешение» используют для описания качества и контрастности отпечатка. Этот показатель напрямую зависит от количества и размера точек. Влияет это и на качество печати. Сканирование проводилось с разрешением 600×600 dpi. Внешний вид отрывка полученного документа представлен на рис. 3.

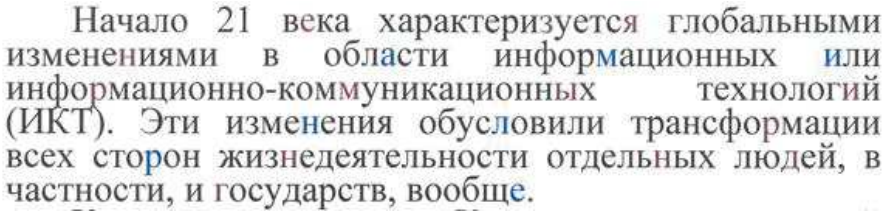
Начало 21 века характеризуется глобальными изменениями в области информационных или информационно-коммуникационных технологий (ИКТ). Эти изменения обусловили трансформации всех сторон жизнедеятельности отдельных людей, в частности, и государств, вообще.

Рисунок 3 – Отсканированный документ

Как видно из рисунка, цвет модифицированных символов сохранился. Чтобы понять, сохранились ли конкретные значения по цветовым каналам, был использован инструмент «Пипетка» в многофункциональном графическом редакторе Adobe Photoshop. Ввиду того, что отсканированный документ представлен в графическом формате *.jpg, цвет символа формируется неоднородно, т. е. цвета со-

седних пикселей, которые формируют цвет символа, могут отличаться (рис. 4).

Рисунок 4 – Пиксельное изображение символа

Результаты, полученные в ходе двух экспериментов, могут отличаться. Это обусловлено значением разрешения при печати и сканировании полученного документа. Помимо этого, для проверки устойчивости метода цветных координат принудительно был изменен цвет одного символа. Символ был определен случайным образом. При этом моделируется ситуация, когда документ с осажденной авторской информацией попадет в руки третьего лица и будет отформатирован. Для наглядности цвет произвольного символа был изменен на желтый (рис. 5).

Начало 21 века характеризуется глобальными изменениями в области информационных или информационно-коммуникационных технологий (ИКТ). Эти изменения обусловили трансформации всех сторон жизнедеятельности отдельных людей, в частности, и государств, вообще.

Рисунок 5 – Вид отформатированного документа

После этого было опытным путем установлено, возможно ли извлечение тайной информации с помощью упомянутой выше программы Sword. Как было выяснено в ходе проведения эксперимента, модификации такого рода не влияют на корректное извлечение встроенного сообщения. Конечно, стоит отметить, что это будет работать лишь в случае частичного форматирования. Таким образом, результат проведения исследований, описанных выше, можно считать удовлетворительным. Интерес для дальнейших исследований представляет вопрос максимально точного сохранения цветов при конвертации из режима RGB в CMYK.

ЛИТЕРАТУРА

1. Шутько, Н. П. Защита авторских прав на электронные текстовые документы методами стеганографии / Н. П. Шутько // Труды БГТУ. − Минск: БГТУ, 2013. − № 6 (162). − С. 131−134.

2. Шутько, Н. П. Стойкость стеганографических документов-контейнеров при их конвертации на основе цветовых моделей RGB и HSL // XXV Туполевские чтения (Школа молодых ученых): Международная молодежная научная конференция. – Т. 5. – Казань, 2021. – С. 748 –752.