

ОБРАБОТКА И ПЕРЕДАЧА ИНФОРМАЦИИ PROCESSING AND TRANSMISSION OF INFORMATION

УДК 004.56+003.26

М. Г. Савельева, П. П. Урбанович

Белорусский государственный технологический университет

РАСТРИРОВАНИЕ WEB-ДОКУМЕНТОВ И ИСПОЛЬЗОВАНИЕ ЕГО ХАРАКТЕРИСТИК ДЛЯ СТЕГАНОГРАФИЧЕСКОЙ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ЭЛЕКТРОННЫЙ КОНТЕНТ

Электронный документ-контейнер, защищаемый от несанкционированного использования или модификации на основе стеганографии, может изначально создаваться как на основе растровой, так и векторной графики. Оригинальный контент при этом может конвертироваться из форматов одной графики в другую. При конвертации или преобразовании текстовых документов-контейнеров одной из важных проблем является растривание текста: контуры букв начинают расплываться, цвет по контуру переходит в градиент. Однако можно воспользоваться этим обстоятельством для внедрения в защищаемый контент тайной информации (цифрового водяного знака, ЦВЗ). Для повышения пропускной способности создаваемого таким образом тайного канала можно использовать преобладающие оттенки среди переходных оттенков растриванных символов. В статье описаны и проанализированы результаты, характеризующие распределения пикселей, составляющих документ-контейнер, по частоте встречаемости различных оттенков из градации серого при конвертации PDF-документов в формат PNG. Это может использоваться как важная входная информация для разработки стеганографических методов защиты электронного контента от несанкционированного использования или модификации (защиты авторского права). Выбор соответствующего цветового оттенка для размещения тайной информации (ЦВЗ) позволяет повышать пропускную способность тайного стеганографического канала, снижать эффективность визуальных или иных атак на стеганоcontainer.

Ключевые слова: стеганография, авторское право, осаждение, растривание.

Для цитирования: Савельева М. Г., Урбанович П. П. Растривание web-документов и использование его характеристик для стеганографической защиты авторских прав на электронный контент // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2023. № 1 (266). С. 54–63. DOI: 10.52065/2520-6141-2023-266-1-10.

M. G. Saveleva, P. P. Urbanovich

Belarusian State Technological University

RASTERIZATION OF WEB DOCUMENTS AND THE USE OF ITS CHARACTERISTICS FOR STEGANOGRAPHIC COPYRIGHT PROTECTION OF ELECTRONIC CONTENT

An electronic document container, protected from unauthorized use or modification based on steganography can initially be created both on the basis of raster and vector graphics. At the same time, the original content can be converted from the formats of one graphic to another. When conversion or transformation of the text container-documents, one of the important problems is the text rasterization: the contours of the letters begin to blur, the color along the contour turns into a gradient. However, it is possible to use this circumstance to embed secret information (digital watermark) into the protected content. To increase the bandwidth of the secret channel created in this way, you can use the prevailing shades among the transitional shades of rasterized characters. The article describes and analyzes the results characterizing the distribution of pixels that make up a certain container document by the frequency of occurrence of various shades of grayscale when converting PDF documents to PNG format. This can be used as the most important input information for the development of stenographic methods

for protecting electronic content from unauthorized use or modification (copyright protection). The choice of the appropriate color shade for the placement of secret information allows you to increase the bandwidth of the secret steganographic channel, reduce the effectiveness of visual or other attacks on the steganocointainer.

Keywords: steganography, copyright, deposition, rasterization.

For citation: Saveleva M. G., Urbanovich P. P. Rasterization of web documents and the use of its characteristics for steganographic copyright protection of electronic content. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*, 2023, no. 1 (266), pp. 54–63. DOI: 10.52065/2520-6141-2023-266-1-10 (In Russian).

Введение. Следует признать тот факт, что развитие Интернет-технологий характеризуется более высокими темпами по сравнению с развитием законодательной и регламентирующей базы, управляющей деятельностью в Интернете. В соответствии с современными законодательными нормами об авторском праве формальности регистрации и уведомления об авторских правах не требуются [1]. В сфере образования создано много интернет-материалов, которые можно использовать в качестве учебных пособий или в научных исследованиях. Это играет важную роль в реализации образовательных стандартов на основе дистанционных платформ [2].

Доступность цифрового контента в компьютерных сетях и электронных репозиториях облегчает создание точных копий электронных документов. Закон об авторском праве вступает в силу в случае несанкционированного копирования, публикации, исполнения (с помощью цифровых средств или иным образом), публичного показа или пересмотра (создания производных) любых материалов, защищенных авторским правом. Приведенные особенности и факты вызывают необходимость разработки дополнительных мер, соответствующих методов и инструментальных средств для защиты авторских прав на электронный контент [3–5].

Стеганография является одним из ведущих направлений, развитие которого связано, в основном, как раз с решением анализируемой проблемы путем внедрения в защищаемый контент невидимой информации в виде цифрового водяного знака (ЦВЗ) [5–11].

Защищаемый авторскими правами электронный документ может создаваться как на основе растровой, так и векторной графики. Вместе с тем оригинальный контент может конвертироваться из форматов одной графики в другую. Такое изменение формата (без согласования с авторами) может приводить к необратимым (полностью или частично) модификациям стеганокоинтейнера S (защищаемый документ с ЦВЗ) при обратной конвертации ЦВЗ [5, 7, 10–13].

Растровую графику применяют при разработке электронных и печатных изданий. Иллюстрации, выполнение средствами растровой

графики, изредка создаются вручную с помощью компьютерных программ. Чаще используются отсканированные иллюстрации, подготовленные художником на бумаге, или фотографии. Для ввода растровых изображений в компьютер также используют цифровые фото- и видеокамеры. Основная масса растровых графических редакторов нацелена не столько на создание изображений, сколько на их обработку.

Программные средства для работы с векторной графикой предусмотрены в первую очередь для создания иллюстраций и в меньшей степени – для их обработки. Принципы векторной графики основаны на отличном от пиксельной графики математическом аппарате и имеют целью построение линейных контуров, составленных из элементарных кривых (от геометрических примитивов до кривых Безье), описываемых математическими уравнениями (см., например, [14]).

При редактировании элементов векторной графики изменяются параметры линий, описывающих форму этих элементов. При этом можно переносить элементы, менять их размер, форму и цвет, и это не отразится на качестве их визуального представления. Данный вид графики также не зависит от разрешения выходных устройств [15].

Конвертация документа из растровой графики в векторную возможна только с помощью трассировки (компьютер чертит предполагаемые векторы) или через ручную отрисовку всех элементов изображения. При этом векторная графика легко конвертируется в растровую. В некоторых случаях это происходит автоматически.

В основе многих стеганографических преобразований лежит цветовая модель RGB, представляющая цвета путем объединения трех цветовых каналов: красного, зеленого и синего. Каждый из каналов имеет размер в один байт. Это означает, что цвет одного пикселя представляется в виде трех байтов. Каждый цветовой канал задается 8-разрядным двоичным вектором или его десятичным эквивалентом [5, 6, 8, 16, 17].

Далее проанализируем некоторые выявленные нами важные особенности, которые необходимо учитывать при разработке и реализации

методов текстовой стеганографии на основе векторной и растровой графики.

Основная часть. Электронные текстовые документы, проходя через сеть Интернет, либо целенаправленно подвергаясь конвертациям и модификациям, достаточно легко изменяют свое исходное (оригинальное) состояние. Любой из них можно рассматривать как изображение и, соответственно, часть растровой или векторной графики.

При конвертации или преобразовании текстовых документов-контейнеров S [5, 9, 11] одной из важных проблем является растривание текста. Процесс растривания векторного изображения с заданным разрешением можно представить как наложение на контур растровой сетки с ячейкой и последующим закрасиванием тех ячеек, в которые попадают точки исходной фигуры знака. В зависимости от количества точек, попавших в растровую ячейку, она закрашивается серым цветом с уровнем от 0 до 255. Таким образом, получается полутоновое изображение растрованного знака [18].

Растрованный текст-контейнер (C) имеет некоторые ограничения: его нельзя редактировать, изменять оформление, копировать, удалять и т. д. Однако растриванием можно воспользоваться как преимуществом для внедрения в C тайной информации M (ЦВЗ).

При растривании символов невозможно сохранить их цвет (рис. 1) и размер (рис. 2) в исходном варианте. При конвертации в иной формат контур буквы начинает расплываться, цвет по контуру переходит в градиент (рис. 1). При этом появляются пиксельные элементы для отображения новых оттенков, т. е. общее количество пикселей для отображения буквы увеличивается (рис. 2). Именно в эти новые пиксели можно внедрять информацию M . При этом очень важно обеспечить максимально возможный (или заданный) уровень защиты стегано-контейнера S от различных атак на него, главным образом – визуальных.



Рис. 1. Пример отображения буквы:
а – как объект растровой графики;
б – как объект векторной графики



Рис. 2. Дополнительные пиксели, возникающие при растривании символа

При преобразовании PDF-документов в формат PNG следует учитывать, что часть элементов может перейти из векторной графики в растровую. Чаще всего PDF-файл создается на основе файлов различных расширений, предназначенных для работы с текстом (.docx, .doc и т.д.). При конвертации исходного файла в формат PDF часть документа может быть преобразована в растр. Дело в том, что в PDF-документах данные хранятся в виде глифов – объектов изображения или наборов графических команд, применяемых для визуализации символов. Для глифов нет четкой формализации, они могут представлять как текстовые элементы, так и объекты изображений, а некоторые символы могут быть представлены несколькими глифами [19]. Дополнительные сложности связаны с неоднозначной структурой PDF-файлов: визуально одинаковые документы могут быть представлены разными наборами глифов. Распознавание самих элементов и границ областей, в которые они входят, зависит от их расположения в документе и от типов отдельных символов. Этот процесс основан на актуализации таблиц соответствия глифов символам в базе данных [19]. Текстовые символы определяются с помощью извлечения их Unicod-значений и свойств шрифта, а нетекстовые (знаки, скобки, линии и т. д.) и сложные текстовые элементы – посредством перевода в растровый формат и OCR. После того как все составляющие элементов были извлечены, определяются границы областей каждого символа [19].

К элементам, которые имеют большую вероятность «перехода» в растровый формат, относятся различные формулы, матрицы, таблицы, листинги и им подобные, т. е. элементы документа, имеющие более сложное оформление, чем абзац текста (рис. 3).

Для первичного анализа и конвертации файлов нами использовалось приложение Adobe Photoshop. В его интерфейсе бело-серый узор в виде клеток на шахматной доске обозначает прозрачный фон. При просмотре PDF-документа можно увидеть, что в некоторых частях

страницы имеется белый фон (рис. 3). Наличие этого фона означают, что формулы и часть обрамляющего текста растривались, как и схема, фрагмент которой размещен в нижней части рисунка. Если схема изначально могла быть рисунком, то формулы, очевидно, нет. Текст, имеющий отступ от растровых элементов, остался в векторном формате.

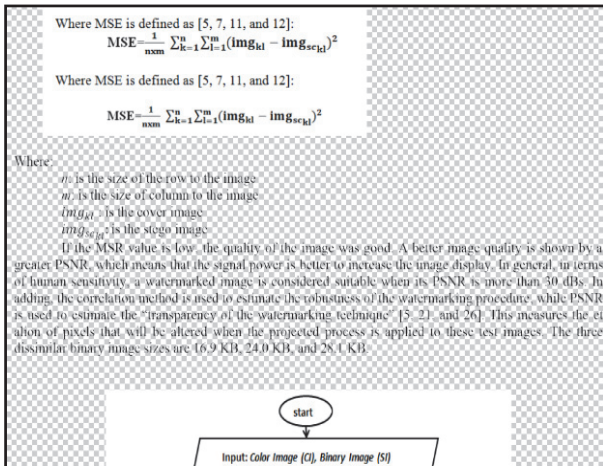


Рис. 3. Фрагмент PDF-документа, содержащий формулу как объект растровой графики

Если на всем документе установился прозрачный фон (рис. 4), то все формулы остались элементами векторной графики, в отличие от рис. 3. Это можно объяснить тем, что при конвертации исходного файла в файл формата PDF, обработчик «не смог» выделить элементы формулы из-за ее сложного оформления (верхний и нижний индексы, наличие индекса у индекса, дроби, структурные операторы, диакритические знаки, крупные операторы с пределами надстрочного (подстрочного) знака и т. д.). Формулы, состоящие из множества различных элементов, с высокой вероятностью будут преобразованы в растр. Простые формулы, в которых четко можно выделить строки и знаки, останутся в векторном формате. Все элементы векторной графики, похожие на рисунок (схема, график, фигуры), растриваются всегда.

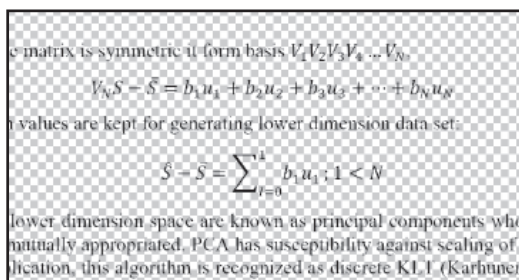


Рис. 4. Фрагмент PDF-документа, содержащий формулу как объект векторной графики

При конвертации PDF-документа в PNG-формат растровые и векторные элементы будут преобразовываться по-разному: растровые сохраняются в таком же виде, а векторные – обрабатываются по группам глифов. Таким образом, сложные элементы фактически будут образованы в окончательном виде при создании PDF-документа из исходного файла иного расширения (.docx, .doc и т. д.). А все остальные – при преобразовании PDF – PNG.

Для повышения пропускной способности стеганоканала, т. е. для внедрения информации M большего объема в расчете на единицу объема контейнера C , следует в элементах переходных отренков растрованных символов выделить преобладающие оттенки.

Нами было проанализировано 50 страниц стандартизированного оформления текстовых документов в формате PNG (преобразованных из PDF): 8 содержали элементы, которые либо обязательно преобразуются в растр при конвертации в PDF (схемы, графики, фигуры), либо уже являются таковыми (рисунки); 17 страниц содержали различные элементы сложного оформления (формулы, таблицы, листинги), которые могут стать растровыми; 25 – содержали только текст. Перечисленные источники разделены условно на 4 группы: 1) все документы; 2) чисто текстовые документы; 3) документы с элементами сложного оформления (формулы, таблицы, листинги); 4) страницы с наличием растровых фрагментов.

На рис. 5–7 представлены полученные усредненные результаты появления пикселей определенного цветового оттенка, соответствующего коду от 0 до 255 для каждого канала модели RGB.

Следует отметить, что на всех проанализированных страницах объем текстовой информации превышает объем информации, представленной в другом виде. Понятно, что на большинстве анализируемых страниц преобладают черно-белые оттенки, за исключением нескольких, имеющих небольшие (до 1% от всего объема) вкрапления иного цвета (рамка, стрелка и т. д.). Так как документы содержат в основном обычный текст, то большинство пикселей окрашены в белый (255, 255, 255) либо в черный (0, 0, 0) цвет.

Для красного канала R (рис. 5) наибольшие относительные частоты отмечены для кодов, соответствующих следующим десятичным значениям данного цвета: 0, 17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255, несколько меньшие – для следующих кодов: 64, 79, 94, 123, 152, 167, 192, 196, 226, 233, 236, 237, 253, 254. Как видно, проявляется некоторая периодическая зависимость между пиковыми значениями частоты.

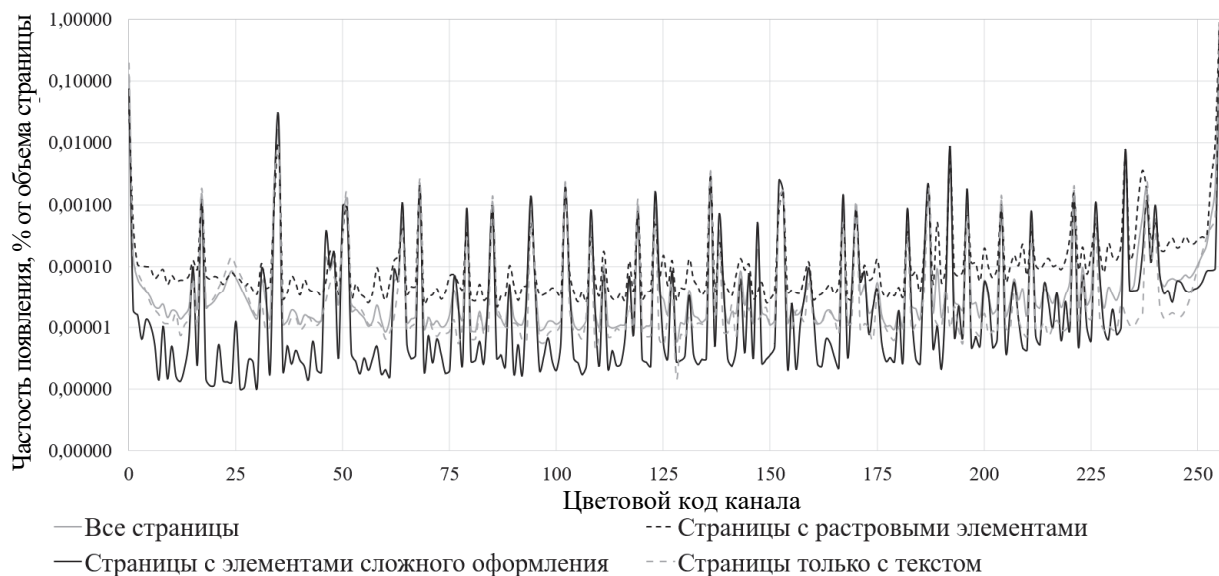


Рис. 5. Распределение пикселей по цветовым оттенкам для канала R

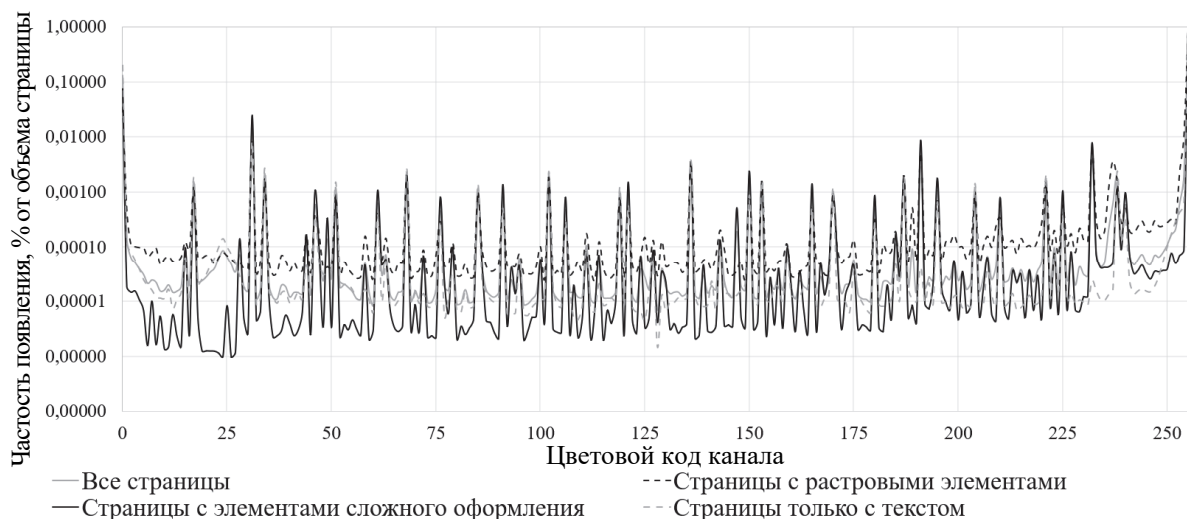


Рис. 6. Распределение пикселей по цветовым оттенкам для канала G

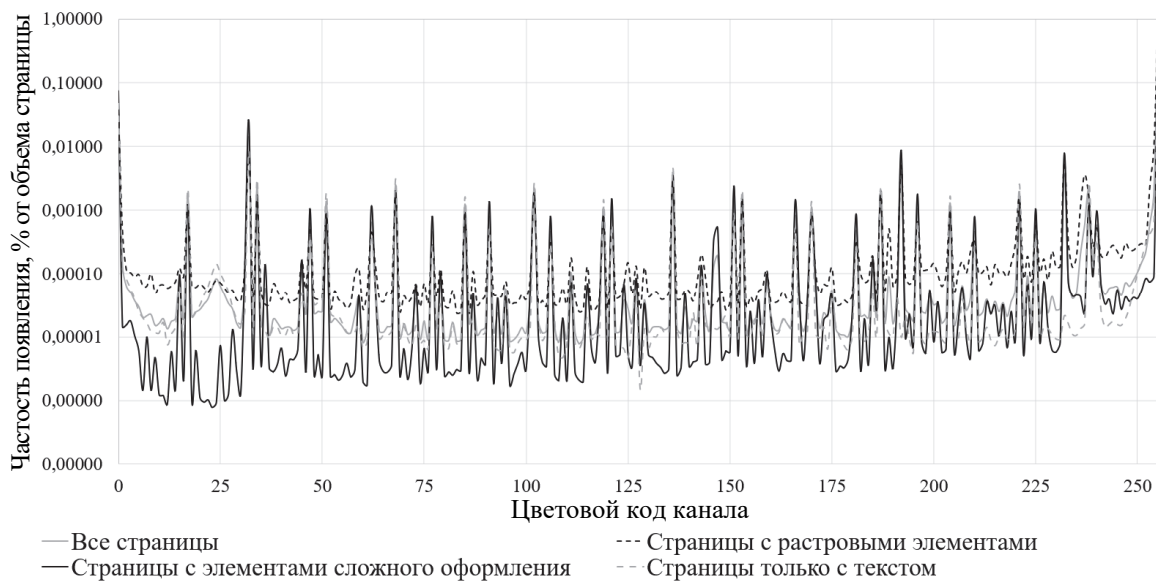


Рис. 7. Распределение пикселей по цветовым оттенкам для канала B

Для канала G (рис. 6) соответственно: 0, 17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255 и 31, 46, 61, 76, 91, 106, 121, 150, 165, 180, 191, 195, 210, 225, 232, 236, 237, 253, 254.

И, наконец, для канала B (рис. 7) соответственно: 0, 17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255 и 32, 46, 62, 77, 91, 106, 121, 147, 151, 166, 181, 192, 196, 210, 225, 232, 236, 237, 253, 254.

Как видно из сравнения полученных распределений, различия между характеристиками каналов практически минимальны.

Пиковые значения для первой из двух рассматриваемых групп (0, 17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255) во всех распределениях соответствуют цвету от черного (0) до белого (255) для 16 различных оттенков: 0 0 0; 17 17 17; ...; 255 255 255) (рис. 8). Так как белый цвет – это фон, то оставшиеся 15 оттенков соответствуют отображениям элементов буквенных символов.



Рис. 8. Градация оттенков серого при растривании символов текста

Такое количество оттенков необходимо для отображения всех растриванных букв с учетом особенностей их строения.

Для форматирования и оформления документов приняты, как известно, определенные правила. В общем виде их можно описать так: для печатных документов – шрифт Times New Roman; для документов, обрабатываемых преимущественно в электронном виде, возможно также применение шрифтов Arial, Helvetica, Verdana; размер 12–14 пт – для основного текста; 10–14 пт – для таблиц и подписей.

Отметим, что Times New Roman – гарнитура на основе засечкового шрифта. Засечка – небольшой узкий штрих, расположенный на конце основного штриха, перпендикулярно ему. Arial, Helvetica, Verdana – гарнитуры, на основе гротеска, рубленого шрифта (шрифт без засечек).

Для выделения преобладающих переходных оттенков, возникающих при растривании из гарнитуры Times New Roman, проанализируем этот шрифт, а из гарнитур Arial, Helvetica, Verdana – шрифт Arial, как наиболее популярные. Так как кириллический алфавит более сложен по сравнению с латинским (из-за наличия шипящих «Ж», «Ч», «Ш», «Щ», «Ц» и йотированных гласных «Я», «Ю»), то проанализируем именно кириллицу, в частности строчные графемы [20].

В источнике [21] приведена классификация букв в зависимости от формы штрихов (строчные и прописные графемы могут относиться к разным группам):

– буквы первой группы, состоящие только из вертикальных и горизонтальных штрихов, – «Г», «Е», «Н» и др. (рис. 9);

– буквы второй группы, состоящие только из вертикальных и горизонтальных и наклонных линий, – «А», «Ж», «И» и др. (рис. 10);

– буквы третьей группы, в которых прямые штрихи соединяются с округлыми, – «Б», «В», «Ч» и др. (рис. 11);

буквы четвертой группы (круглые буквы) – «З», «О», «С» и др. (рис. 12).

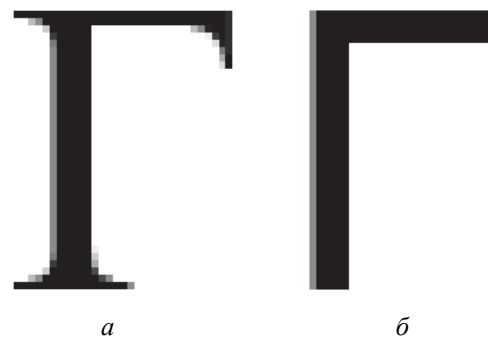


Рис. 9. Пример буквы первой группы: а – шрифт Times New Roman; б – шрифт Arial

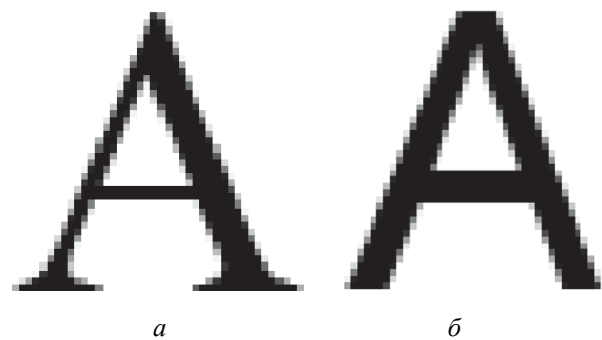


Рис. 10. Пример буквы второй группы: а – шрифт Times New Roman; б – шрифт Arial

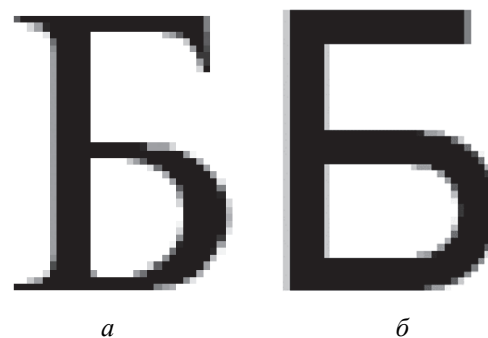


Рис. 11. Пример буквы третьей группы: а – шрифт Times New Roman; б – шрифт Arial

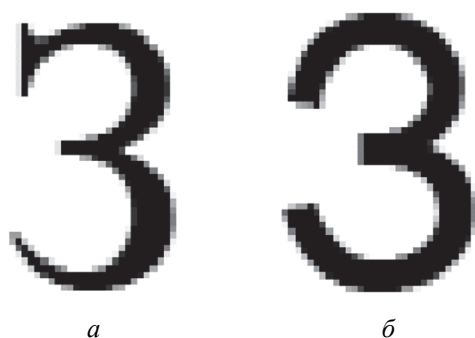


Рис. 12. Пример буквы четвертой группы:
а – шрифт Times New Roman; б – шрифт Arial

Для анализа отображения символов использовалась панграмма (текст, состоящий из всех или почти всех букв алфавита) для русского языка: «Съешь же ещё этих мягких французских булок, да выпей чаю». Результат приведен в таблице.

Количество оттенков для отображения графемы

Графема	Times New Roman			Arial		
	10pt	12pt	14pt	10pt	12pt	14pt
а	17	15	15	15	15	15
б	15	15	15	15	15	15
в	15	14	14	14	15	15
г	14	14	13	4	3	3
д	15	15	15	15	15	15
е	15	15	15	15	15	15
ё	15	15	15	15	15	15
ж	15	15	15	15	15	14
з	14	14	15	15	15	15
и	15	15	14	15	15	15
й	15	15	15	14	15	15
к	15	14	17	14	15	15
л	14	15	15	9	10	11
м	15	14	15	15	15	15
н	13	13	12	4	4	2
о	15	15	15	15	15	15
п	11	10	10	4	3	3
р	14	14	15	15	15	15
с	15	15	15	15	15	15
т	15	13	15	4	4	4
у	15	15	15	15	15	15
ф	15	15	15	15	15	15
х	15	14	15	15	15	15
ц	13	15	14	6	6	5
ч	13	15	15	13	14	14
ш	15	15	15	6	5	5
щ	15	15	15	6	5	6
ъ	15	14	15	12	14	14
ы	15	15	15	12	13	14
ь	13	14	14	13	15	14
э	15	15	15	15	15	15
ю	15	17	15	15	15	15
я	15	15	15	15	15	15

Графемы, имеющие дополнительно иные оттенки, выделены полужирным курсивным начертанием.

Исходя из табличных данных можно сказать, что буквы из первой группы при написании шрифтом Arial имеют в разы меньше оттенков при отображении на экране. Кроме того, остальные буквы хотя и имеют одинаковое или близкое к одинаковому число оттенков при написании шрифтами Arial и Times New Roman, но число пикселей, соответствующих каждому из оттенков, при использовании Arial меньше. Наиболее часто встречаются оттенки: (17, 17, 17), (34, 34, 34), (68, 68, 68), (102, 102, 102), (136, 136, 136), (153, 153, 153), (187, 187, 187).

Среди особенностей шрифта Times New Roman можно выделить пересечение границ букв (слияние букв, рис. 13). Чем меньше кегль, тем больше буквы сливаются друг с другом и имеют больше общих пикселей. В таком случае недостаточно 15 оттенков для отображения символа. Единичные пиксели имеют иные промежуточные оттенки серого.



Рис. 13. Слияние букв при использовании шрифта Times New Roman

К слиянию «склонны» графемы, имеющие такие элементы, как «хвост», «нога», «капля», «ухо», концевой элемент или графемы засечковых шрифтов [19]. Брусковые шрифты имеют заданное расстояние между графемами, что помогает избежать слияния.

Заключение. Проведенный анализ выявил наиболее часто встречающиеся оттенки из градации серого при конвертации PDF-документов в формат PNG.

Установлено, что наименьший разброс значений частоты появления оттенка (с кодом от 0 до 255) свойственен простым текстовым документам. Для них можно выделить следующие оттенки (R, G, B) как наиболее часто проявляющиеся (17, 17, 17), (34, 34, 34), (68, 68, 68), (102, 102, 102), (136, 136, 136), (153, 153, 153), (187,

187, 187). Для остальных элементов отмечается 16 равномерно распределенных оттенков с кодами от 0 до 255: (0, 0, 0), (17, 17, 17), (34, 34, 34), ..., (255, 255, 255). Так как белый цвет (255, 255, 255) – это фон страницы, то только 15 оттенков используются для отображения символов.

Полученные результаты являются важнейшей входной информацией для разработки стеганографических методов защиты электронного контента от несанкционированного использования или модификации (защиты авторского права) при конвертации этого контента в иной формат. Выбор соответствующего цветового оттенка для размещения тайной информации (ЦВЗ) позволяет повышать пропускную способность тайного стеганографического канала, снижать эффективность визуальных или иных атак на стеганоконтентер.

Список литературы

1. Reichman J. H., Okediji R. L. When Copyright Law and Science Collide: Empowering Digitally Integrated Research Methods on a Global Scale // *MinnLawRev.* 2012. Vol. 96 (4). P. 1362–1480.
2. Урбанович П. П., Блинова Е. А., Ржеутская Н. В. Дистанционное обучение: тенденция, естественный процесс или вынужденная мера? // *Информационные технологии в образовании, науке и производстве: VIII Междунар. науч.-техн. интернет-конф.*, 21–22 ноября 2020 года. Минск: БНТУ, 2020. С. 116–122.
3. Kim, M. The creative commons and digital protection in the digital era: uses of Creative Commons licenses // *Journal of Computer-Mediated Communication.* 2008. Vol. 13. P. 187–209.
4. Micunovic M., Balkovich, L. Author's rights in the digital age: how Internet and peer-to-peer file sharing technology shape the perception of copyrights and copywrongs // *Libellarium Journal for the Research of Writing Books and Cultural Heritage Institutions.* 2016. Vol. 8 (2). P. 27–64. DOI: 10.15291/libellarium.v0i0.232.
5. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации. Минск: БГТУ, 2016. 220 с.
6. Шутько Н. П. Защита авторских прав на электронные текстовые документы методами стеганографии // *Труды БГТУ.* 2013. № 6 (162): Физико-математические науки и информатика. С. 131–134.
7. Блинова Е. А., Урбанович П. П. Сравнительные особенности использования стеганографических методов в электронных картах // *Информационные технологии в промышленности, логистике и социальной сфере (ITI-2019): тез. докл. X Междунар. науч.-техн. конф.*, Минск, 23–24 мая 2019 г. Минск: ОИПИ НАН Беларуси, 2019. С. 22–25.
8. Шутько Н. П., Урбанович П. П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста // *Информационные технологии: материалы 83-й науч.-техн. конф. проф.-препод. состава, науч. сотрудников и аспирантов (с междунар. участием), Минск, 4–15 февраля 2019 г.* Минск: БГТУ, 2019. С. 41–43.
9. Шутько Н. П., Листопад Н. И., Урбанович П. П. Моделирование стеганографической системы в задачах по охране авторских прав // *Информационные технологии в промышленности (ITI 2015): тез. докл. Восьмой Междунар. науч.-техн. конф.* Минск, 2015. С. 30–31.
10. Блинова Е. А. Стеганографический метод на основе изменения междустрочного расстояния неотображаемых символов строк электронного текстового документа / Е. А. Блинова // *Труды БГТУ.* 2016. № 6 (188): Физико-математические науки и информатика. С. 166–169.
11. Shutko N., Urbanovich P., Zukowski P. Method of syntactic text steganography based on modification of the document-container aprosh // *Przegląd Elektrotechniczny.* 2018. Vol. 6. P. 82–85. DOI:10.15199/48.2018.06.15.
12. Chang C. S., Nguyen T.-S. A Reversible Data Hiding Scheme for SMVQ Indices // *Informatica.* 2014. Vol. 25, no. 4, pp 523–540. DOI: <http://dx.doi.org/10.15388/Informatica.2014.27>.
13. Almutairi A. A Comparative Study on Steganography Digital Images: A Case Study of Scalable Vector Graphics (SVG) and Portable Network Graphics (PNG) Images Formats // *(IJACSA) International Journal of Advanced Computer Science and Applications.* 2018. Vol. 9, no. 1. P. 170–175.

14. Blinova E. A., Urbanovich P. P. Steganographic method based on hidden messages embedding into Bezier curves of SVG images // *Journal of the Belarusian State University. Mathematics and Informatics*. 2021. No. 3. P. 68–83. DOI: <https://doi.org/10.33581/2520-6508-2021-3-68-83>.

15. Новиков А. Н., Фирсов А. В., Каршакова Л. Б. Развитие традиционных и появление новых художественных стилей под влиянием компьютерной графики // *Вестник славянских культур*. 2021. Т. 60. С. 282–297. URL: <https://doi.org/10.37816/2073-9567-2021-60-282-297> (дата обращения: 12.10.2022).

16. 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. DOI: <https://doi.org/10.52065/2520-6141-2022-260-2-99-107>.

17. Prasad S., Pal A. K. An RGB colour image steganography scheme using overlapping block-based pixel-value differencing // *Royal Society Open Science*. 2017. Vol. 4. 16 p. DOI: 10.1098/rsos.161066.

18. Агеев В. Н., Соломыков В. С. Моделирование процесса растривания векторных шрифтов в выводных устройствах низкого разрешения // *Известия ТулГУ. Технические науки*. 2013. № 3. С. 9–16.

19. Быканова А. С. Методы распознавания математических формул в электронных документах // *Актуальные проблемы авиации и космонавтики*. 2018. № 14. С. 133–134.

20. Рыжанкова А. С. Анатомия буквы: анализ названий элементов // *Труды БГТУ*. 2022. Сер. 4, Принт- и медиатехнологии. 2022. № 1 (255). С. 131–139. DOI: <https://doi.org/10.52065/2520-6729-2022-255-1-131-139>.

21. Тоотс Виллу. Современный шрифт. М.: Книга, 1966. 272 с.

References

1. Reichman J. H., Okediji R. L. When Copyright Law and Science Collide: Empowering Digitally Integrated Research Methods on a Global Scale. *MinnLawRev*, 2012, vol. 96 (4), pp. 1362–1480.

2. Urbanovich P. P., Blinova E. A., Rzhetskaya N. V. Distance learning: a trend, a natural process or a forced measure? *Informatsionnyye tekhnologii v obrazovanii, nauke i proizvodstve: VIII Mezhdunarodnaya nauchno-tekhnicheskaya internet-konferentsiya* [Information Technologies in Education, Science and Production: VIII International Scientific and Technical Internet Conference]. Minsk, 2020, pp. 116–122. (In Russian).

3. Kim, M. The creative commons and digital protection in the digital era: uses of Creative Commons licenses. *Journal of Computer-Mediated Communication*, 2008, vol. 13, pp. 187–209.

4. Micunovic M., Balkovich, L. Author's rights in the digital age: how Internet and peer-to-peer file sharing technology shape the perception of copyrights and copywrongs. *Libellarium Journal for the Research of Writing Books and Cultural Heritage Institutions*, 2016, vol. 8 (2), pp. 27–64. DOI: 10.15291/libellarium.v0i0.232.

5. Urbanovich P. P. *Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii* [The protection of information based on the methods by cryptography, steganography and obfuscation]. Minsk, BGTU Publ., 2016. 220 p. (In Russian).

6. Shutko N. P. Copyright protection for electronic text documents using steganography methods. *Trudy BGTU* [Proceedings of BSTU], 2013, no. 6 (162): Physics and Mathematics. Informatics, pp. 131–134 (In Russian).

7. Blinova E. A., Urbanovich P. P. Comparative features of the use of steganographic methods in electronic maps. *Informatsionnyye tekhnologii v promyshlennosti, logistike i sotsial'noy sfere (ITI-2019): tezisy dokladov X Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii* [Information technologies in industry, logistics and social sphere (ITI-2019): abstracts X International scientific and technical conference]. Minsk, 2019, pp. 22–25 (In Russian).

8. Shutko N., Urbanovich P. Copyright protection for text documents based on steganographic modification of the color of text symbols. *Informatsionnyye tekhnologii: materialy 83-y nauchno-tekhnicheskoy konferentsii professorsko-prepodavatel'skogo sostava, nauchnykh sotrudnikov i aspirantov (s mezhdunarodnym uchastiyem)* [Information technologies: materials of the 83rd scientific and technical conference of the faculty, researchers and graduate students (with international participation)]. Minsk, 2019, pp. 41–43 (In Russian).

9. Shutko N., Listopad N., Urbanovich P. Modeling a steganographic system in problems of copyright protection. *Informatsionnyye tekhnologii v promyshlennosti (ITI'2015): tezisy dokladov Vos'moy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii* [Information Technologies in Industry (ITI'2015): abstracts Eighth International Scientific and Technical Conference]. Minsk, 2015, pp. 30–31 (In Russian).

10. Blinova E. A. Steganographic method based on changing the line spacing of non-displayed characters of lines of an electronic text document. *Trudy BGTU* [Proceedings of BSTU], 2016, no. 6 (188): Physics and Mathematics. Informatics, pp. 166–169 (In Russian).

11. Shutko N., Urbanovich P., Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh. *Przegląd Elektrotechniczny*, 2018, vol. 6, pp. 82–85. DOI: 10.15199/48.2018.06.15.
12. Chang C. C., Nguyen T.-S. A Reversible Data Hiding Scheme for SMVQ Indices. *Informatica*, 2014, vol. 25, no. 4, pp. 523–540. DOI: <http://dx.doi.org/10.15388/Informatica.2014.27>.
13. Almutairi A. A Comparative Study on Steganography Digital Images: A Case Study of Scalable Vector Graphics (SVG) and Portable Network Graphics (PNG) Images Formats (*IJACSA International Journal of Advanced Computer Science and Applications*, 2018, vol. 9, no. 1, pp. 170–175.
14. Blinova E. A., Urbanovich P. P. Steganographic method based on hidden messages embedding into Bezier curves of SVG images. *Journal of the Belarusian State University. Mathematics and Informatics*, 2021, no. 3, pp. 68–83. DOI: <https://doi.org/10.33581/2520-6508-2021-3-68-83>.
15. Novikov A. N., Firsov A. V., Karshakova L. B. The development of traditional and the emergence of new artistic styles under the influence of computer graphics. *Vestnik slavyanskikh kul'tur* [Herald of Slavic Cultures], 2021, vol. 60, pp. 282–297. Available at: <https://doi.org/10.37816/2073-9567-2021-60-282-297> (accessed 12.10.2022). (In Russian).
16. Saveleva M. G., Urbanovich P. P. Method of steganographic transformation of web-documents based on raster graphics and RGB model. *Trudy BGTU* [Proceedings of BSTU], issue 3, Physics and Mathematics. Informatics, 2022, no. 2, pp. 99–107. DOI: <https://doi.org/10.52065/2520-6141-2022-260-2-99-107> (In Russian).
17. Prasad S., Pal A. K. An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society Open Science*, 2017, vol. 4, 16 p. DOI: 10.1098/rsos.161066.
18. Ageyev V. N., Solomykov V. S. Modeling the process of rasterization of vector fonts in low-resolution output devices. *Izvestiya TulGU. Tekhnicheskkiye nauki* [News of TulGU. Technical science], 2013, no. 3, pp. 9–16. (In Russian).
19. Bykanova A. S. Methods for recognizing mathematical formulas in electronic documents. *Aktual'nyye problemy aviatsii i kosmonavtiki* [Actual problems of aviation and astronautics], 2018, no. 14, pp. 133–134. (In Russian).
20. Ryzhankova A. S. Anatomy of a letter: analysis of the names of elements *Trudy BGTU* [Proceedings of BSTU], issue 4, Print- and Mediatechnologies, 2022, no. 1, pp. 131–139. DOI: <https://doi.org/10.52065/2520-6729-2022-255-1-131-139> (In Russian).
21. Toots Willu. *Sovremennyy shrift* [Modern typeface]. Moscow, Kniga Publ., 1966. 272 p. (In Russian).

Информация об авторах

Савельева Маргарита Геннадьевна – аспирант кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: saveleva@belstu.by.

Урбанович Павел Павлович – доктор технических наук, профессор, профессор кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: p.urbanovich@belstu.by.

Information about the authors

Saveleva Margarita Gennadijevna – PhD student, the Department of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: saveleva@belstu.by

Urbanovich Pavel Pavlovich – DSc (Engineering), Professor, Professor, the Department of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: p.urbanovich@belstu.by

Поступила 28.11.2022