ОБРАБОТКА И ПЕРЕДАЧА ИНФОРМАЦИИ
PROCESSING AND TRANSMISSION OF INFORMATION

УДК 004.56+003.26

М. Г. Савельева[1], П. П. Урбанович[1, 2]
[1]Белорусский государственный технологический университет
[2]Люблинский Католический университет Яна Павла II, Польша

ИСПОЛЬЗОВАНИЕ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК РАСТРИРОВАНИЯ ТЕКСТОВЫХ ДОКУМЕНТОВ В СТЕГАНОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

Цифровой контент может создаваться или преобразовываться с использованием векторной или растровой графики. Растрирование текстовых фрагментов указанного контента приводит к расплыванию контуров букв и переходу цвета в градиент. Этой особенностью векторно-растрового преобразования можно воспользоваться для решения прикладных задач на основе стеганографических методов, создавая тайные каналы с целью хранения или передачи данных. Для увеличения пропускной способности и стеганографической стойкости таких каналов целесообразно внедрять элементы осаждаемого сообщения в символы документа-контейнера, опираясь на определенные пространственно-геометрические параметры и свойства этих символов. В статье представлены результаты анализа и классификации букв русского алфавита по нескольким статистическим признакам. В соответствии с этим все буквы условно разделены на три группы. Результаты анализа распределений пикселей для отображения буквы при конвертации контента по схеме PDF – PNG могут быть использованы для разработки стеганографических методов путем создания тайных каналов для хранения (цифровой водяной знак) или передачи информации. Выбор соответствующих символов, относящихся к различным группам, для размещения тайной информации не только повышает пропускную способность канала и снижает эффективность визуальных или иных атак на стеганоконтейнер, но и позволяет упростить алгоритмы внедрения (извлечения) тайной информации.

Ключевые слова: стеганография, растрирование, текст, шрифт, статистические параметры.

Для цитирования: Савельева М. Г., Урбанович П. П. Использование статистических характеристик растрирования текстовых документов в стеганографических приложениях // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2023. № 2 (272). С. 89–96. DOI: 10.52065/2520-6141-2023-272-2-13.

M. G. Saveleva[1], P. P. Urbanovich[1, 2]
[1]Belarusian State Technological University
[2]The John Paul II Lublin Catholic University

USAGE OF STATISTICAL CHARACTERISTICS OF TEXT DOCUMENTS HALFTONE SCREENING IN STEGANOGRAPHIC APPLICATIONS

Digital content can be created or transformed using vector or raster graphics. Rasterization of the text fragments of the a birth content leads to the blurring of the contours of the letters and the transition of color into a gradient. This feature of the vector-raster transformation can specified a way to solve applied problems based on steganographic methods, creating secret channels for storing or transmitting data. To increase the throughput and steganographic stability of such channels, it is advisable to introduce elements of the deposited message into the symbols of the container document, relying on certain spatial and geometric parameters and properties of these symbols. The article presents the results of the analysis and classification of the letters of the Russian alphabet according to several statistical features. In accordance with this, all letters are conditionally divided into three groups. The results of the analysis of pixel distributions for displaying letters when converting content according to the PDF – PNG scheme can be used to develop steganographic methods by creating secret channels for storing (digital watermark) or transmitting

information. The choice of appropriate symbols belonging to different groups for the placement of secret information not only increases the bandwidth of the channel and reduces the effectiveness of visual or other attacks on the steganocontainer, but also will simplify the algorithms for the introduction (extraction) of secret information.

Keywords: steganography, halftone screening, text, font, statistical parameters.

For citation: Saveleva M. G., Urbanovich P. P. Usage of statistical characteristics of text documents halftone screening in steganographic applications. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*, 2023, no. 2 (272), pp. 89–96. DOI: 10.52065/2520-6141-2023-272-2-13 (In Russian).

Введение. Защита цифрового контента направлена на обеспечение безопасности и неприкосновенности цифровых материалов для нелегитимного использования. Цифровой контент может быть скопирован и распространен в Интернете или на других носителях без разрешения владельца авторских прав, что может привести к ущербу для его создателя или правообладателя [1].

Для решения указанных проблем могут быть использованы стеганографические методы и средства. Скрытие информации, т. е. цифровых водяных знаков (ЦВЗ), внутри охраняемых от несанкционированного распространения документов-контейнеров или использование последних для тайной передачи данных реализуется фактически путем создания тайных информационных каналов [2–6].

Компании, например, могут использовать стеганографию для скрытия уникальных идентификаторов внутри своих конфиденциальных документов. Эти идентификаторы могут быть применены для отслеживания, кто имеет доступ к документам, и пресечения незаконного распространения.

Существуют другие (кроме ЦВЗ) методы защиты цифрового контента [2, 7–11]. В любом случае, защита рассматриваемого информационного ресурса является важной задачей, которая помогает защитить интересы правообладателей и обеспечивает безопасность цифровых материалов.

Стеганографические преобразования контейнеров-изображений часто базируются на основе цветовой модели RGB (Red-Green-Blue). Это техника скрытой передачи информации, которая встраивается в изображение с использованием изменения в параметрах цветовых каналов RGB [5, 6, 10, 12]. В модели RGB пиксель, формирующий изображение, имеет три значения: красный (R), зеленый (G) и синий (B). Каждое из этих значений может быть представлено в виде числа от 0 до 255, что позволяет отобразить цвет пикселя в виде трехбайтовой последовательности.

Исследования в области цветовой теории играют важную роль в создании методов стеганографии для защиты электронного контента от несанкционированного использования или модификации, например для защиты авторских прав при конвертации контента в другой формат. Оптимизация выбора букв или группы букв для размещения тайной информации внутри изображения является ключевым фактором для повышения пропускной способности тайного канала и снижения эффективности визуальных или других атак на защищаемый контент. Важно учитывать, что каждая буква имеет свойства, влияющие на визуальное восприятие текста внутри изображения либо отдельного текстового документа, а также на «способность» букв маскировать тайную информацию.

Далее проанализируем выявленные нами важные особенности, которые целесообразно учитывать при разработке и реализации методов стеганографии на основе векторной и растровой графики.

Основная часть. Электронные текстовые документы, такие, например, как файлы MS Word PDF, являются основным средствами обмена информацией внутри Интернета. Однако при передаче в этих документах могут появиться случайные или преднамеренно созданные третьими лицами изменения. Существует множество инструментов и техник, позволяющих вносить такие изменения.

Каждый из документов может быть представлен в виде графического изображения, которое может быть как растровым, так и векторным. Это значит, что мы можем рассматривать любой текстовый документ как изображение, которое состоит из пикселей или геометрических фигур, определяющих его внешний вид и форму.

Конвертация растровой графики в векторную – это процесс преобразования изображения, состоящего из пикселей (растровое изображение), в изображение, состоящее из геометрических форм (векторное изображение).

При изменении или преобразовании текстовых документов-контейнеров [5, 6, 11, 12] одной из проблем может быть потеря качества текста, когда он становится растровым изображением. Процесс растрирования векторного изображения происходит путем разбиения его на множество маленьких ячеек, нанесения на них растровой сетки и закрашивания каждой ячейки, в зависимости от наличия в ней точек из исходной фигуры серым цветом с уровнем от 0 до 255. Ячейки, содержащие меньше точек, получают более светлый оттенок серого цвета, а ячейки с большим

количеством точек – более темный оттенок, что создает полутоновое изображение [13, 14].

Для повышения пропускной способности стеганоканала, т. е. для размещения в контейнере информации большего объема в расчете на единицу объема контейнера, следует определить и учитывать преобладающие оттенки в элементах переходных оттенков растрированных символов. Для выявления закономерностей при анализе преобладающих оттенков целесообразно классифицировать или разделить все графемы на группы. Это, по нашему мнению, упростит алгоритмы осаждения (извлечения) тайной информации.

В источнике [15] 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 (здесь и ниже даются заглавные начертания знаков) – «г», «н», «п», «т», «ц», «ш», «щ»;

– буквы второй группы, состоящие только из вертикальных, горизонтальных и наклонных линий – «ж», «и», «к», «м», «х»;

– буквы третьей группы, в которых прямые штрихи соединяются с округлыми, – «б», «в», «д», «й», «л», «р», «у», «ф», «ч», «ъ», «ы», «ь», «ю», «я», «а», «е», «ё», «э»;

– буквы четвертой группы (круглые буквы) – «з», «о», «с».

Для обработки графем в электронном виде и внедрения сообщения данное разбиение не является удачным, так как при растрировании буквы с наклонными линиями, округлыми и (или) круглыми элементами не будет отличаться друг от друга за счет того, что квадратными пикселями невозможно создать округлые, круглые и наклонные штрихи правильного вида. Поэтому для разбиения на группы, исходя из особенностей отображения букв при растрировании, был проведен анализ преобладающих переходных оттенков для каждой буквы русского алфавита.

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 12–20 пт – для основного текста; 8–14 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 растрировании 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 [16].

Для анализа отображения символов (количества оттенков) 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 табл. 1, 2.

Таблица 1

Количество оттенков для отображения графемы гарнитурой Times New Roman

Графема	Times New Roman								
	8pt	9pt	10pt	11pt	12pt	14pt	16pt	18pt	20pt
а	15	15	17	15	15	15	15	18	15
б	15	15	15	15	15	15	15	15	15
в	15	15	15	14	14	14	15	15	15
г	11	13	14	12	14	13	15	15	15
д	15	15	15	15	15	15	15	15	15
е	15	15	15	15	15	15	15	15	15
ё	15	15	15	15	15	15	15	15	15
ж	15	15	15	15	15	15	15	15	15
з	15	14	14	14	14	15	18	15	15
и	13	15	15	15	15	14	15	15	15
й	15	15	15	15	15	15	15	15	15
к	14	15	15	17	14	17	15	15	15
л	11	14	14	15	15	15	16	16	15
м	15	15	15	15	14	15	15	15	15
н	11	14	13	11	13	12	15	15	15

Окончание табл. 1

Графема	Times New Roman								
	8pt	9pt	10pt	11pt	12pt	14pt	16pt	18pt	20pt
о	15	15	15	15	15	15	15	15	15
п	13	13	11	10	10	10	12	15	13
р	14	15	14	15	14	15	15	15	15
с	15	15	15	15	15	15	15	15	15
т	13	10	15	15	13	15	14	15	15
у	15	15	15	15	15	15	15	15	15
ф	15	15	15	15	15	15	15	15	15
х	15	15	15	15	14	15	15	15	14
ц	12	15	13	14	15	14	14	15	14
ч	13	14	13	15	15	15	15	15	15
ш	12	15	15	15	15	15	15	15	15
щ	12	15	15	15	15	15	15	15	15
ъ	15	13	15	15	14	15	15	15	15
ы	15	15	15	14	15	15	15	15	15
ь	13	14	13	13	14	14	15	15	15
э	14	14	15	15	15	15	15	15	15
ю	15	15	15	15	17	15	15	15	15
я	15	15	15	15	15	15	15	15	14

Таблица 2

Количество оттенков для отображения графемы гарнитурой Arial

Графема	Arial								
	8pt	9pt	10pt	11pt	12pt	14pt	16pt	18pt	20pt
а	14	15	15	15	15	15	15	15	15
б	15	15	15	15	15	15	15	15	15
в	13	14	14	15	15	15	15	15	15
г	4	3	4	4	3	3	3	3	3
д	10	13	15	15	15	15	15	15	15
е	14	15	15	15	15	15	15	15	15
ё	15	15	15	14	15	15	15	15	15
ж	15	15	15	15	15	14	15	15	15
з	15	14	15	15	15	15	15	15	15
и	8	13	15	13	15	15	15	15	15
й	15	15	14	14	15	15	15	15	15
к	14	14	14	15	15	15	15	15	15
л	9	9	9	10	10	11	14	12	13
м	15	15	15	15	15	15	15	14	15
н	5	3	4	5	4	2	3	5	4
о	15	15	15	15	15	15	15	15	15
п	4	5	4	3	3	3	5	4	2
р	15	15	15	15	15	15	15	15	15
с	14	15	15	15	15	15	15	15	15
т	5	5	4	5	4	4	5	5	4
у	15	15	15	15	15	15	15	15	15
ф	14	15	15	15	15	15	15	15	15
х	15	15	15	14	15	15	15	15	15
ц	7	6	6	6	6	5	4	4	6
ч	12	13	13	13	14	14	14	14	15
ш	5	5	6	7	5	5	5	5	6
щ	6	6	6	8	5	6	5	5	6
ъ	12	11	12	14	14	14	15	15	15
ы	12	12	12	13	13	14	14	15	14
ь	11	10	13	13	15	14	14	14	15
э	15	15	15	15	15	15	15	15	15
ю	13	15	15	15	15	15	15	15	15
я	13	15	15	15	15	15	15	15	15

Дальнейшие рассуждения будем строить на основе использования основных числовых характеристик распределения дискретной случайной величины [17]. В нашем случае дискретная случайная величина (ДСВ) ξ соответствует определенной букве алфавита и задана рядом распределения, соответствующим строке табл. 1 или 2. В общем случае ξ принимает значения $x_1, x_2, \ldots, x_n$ с вероятностями $p_1, p_2, \ldots, p_n$. Здесь x_i – числовое значение оттенков, необходимое для отображения выбранной буквы при различном кегле, $x_i \in [1, 254]$ (белый цвет – цвет фона – не используется для отображения символа, но хотя бы 1 оттенок должен использоваться для отображения), p_i – вероятность того, что для определенной буквы при использовании различных кеглей $\xi = x_i$, $i \in [1, n]$, n – количество уникальных значений оттенков для отображения буквы различного кегля. В общем случае размер кегля в MS Word может принимать значения от 1 до 1638 с шагом 0,5. Основное практическое применение находят размеры от 8 до 20 пт, как и указано в табл. 1 и 2 (верхняя строка). Тогда, выражение

$$M\xi = \sum_{i=1}^{n} x_i p_i \qquad (1)$$

позволит определить центр анализируемых распределений ДСВ. Полученное таким образом среднее значение ДСВ ξ является математическим ожиданием.

Дисперсию ДСВ ξ ($D\xi$) вычислим стандартным образом:

$$D\xi = M(\xi - M\xi)^2. \qquad (2)$$

Полученные результаты представлены на рис. 1 и рис. 2.

Для разделения букв алфавита на группы в соответствии с целью нашего анализа выделим минимальное значение $D\xi$, отличное от 0: $D\xi_{min} = 0{,}094$. Это значение соответствует ситуации, когда один из кеглей графемы имеет количество оттенков x_n, меньшее на единицу от количества оттенков в остальных кеглях (в основном за счет небольшого размера). Выделим также $D\xi = 1$. Это значение соответствует ситуациям, при которых одно значение x_i существенно отличается от $M\xi$, или существенная часть x_i отличается от $M\xi$ на одно-два значения.

На основе полученных данных выделим группы графем по следующему принципу (см. рис. 2):

– первая группа, состоящая из букв, у которых значения дисперсии каждой гарнитуры меньше $D\xi_{min}$ («б», «е», «ё», «ж», «о», «с», «у», «ф»);

– вторая группа – значения дисперсии каждой гарнитуры меньше 1 («в», «й», «м», «р», «х», «ц», «ч», «ш», «щ», «э», «ю», «я»);

– третья группа – значения дисперсии хотя бы одной гарнитуры больше 1 («а», «г», «д», «и», «к», «л», «н», «п», «т», «ъ», «ы», «ь»).

Фактически разбиение на группы произошло в зависимости от сложности отображения буквы при растрировании.

Буквы первой группы наиболее предсказуемы. Они имеют более сложное написание по сравнению с остальными (верхние выносные элементы, нижние выносные элементы, акценты, хвосты, капли, наплывы, овалы и т. д., различные комбинации этих элементов). Из-за сложной структуры при различном кегле начертания букв сжимаются только по вертикали, по горизонтали размер изменяется незначительно. За счет этого графемы имеют немалое количество переходных оттенков.

Буквы второй группы имеют более простую структуру. В каждой появляются горизонтальные или вертикальные штрихи в комбинации с более сложными элементами. Эти графемы более подвержены сжатию, из-за чего количество оттенков при малых размерах кегля уменьшается, т. е. они становятся менее предсказуемыми.

Буквы третьей категории имеют самую простую структуру (большое количество горизонтальных или вертикальных штрихов). Сравнивая количество оттенков при большом и малом кеглях, можно заметить уменьшение количества оттенков в малом размере до 60% по отношению к большему.

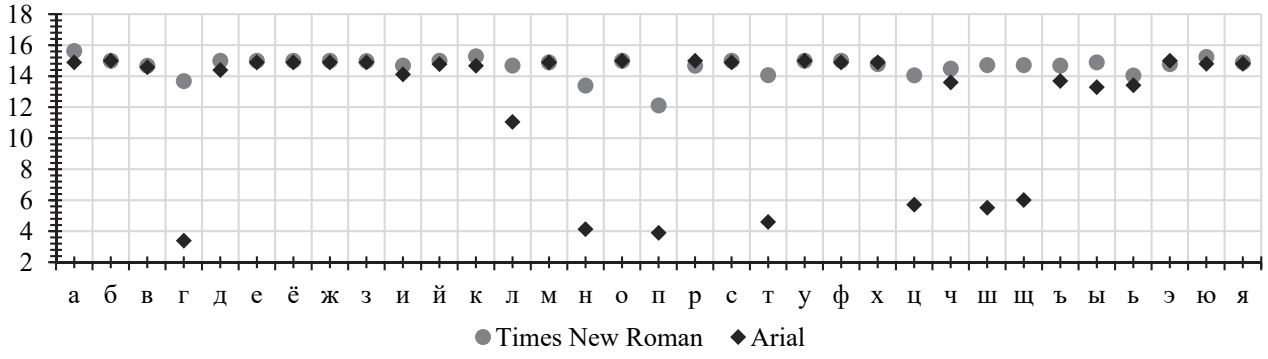

Рис. 1. Математическое ожидание значений оттенков при растрировании символов текста

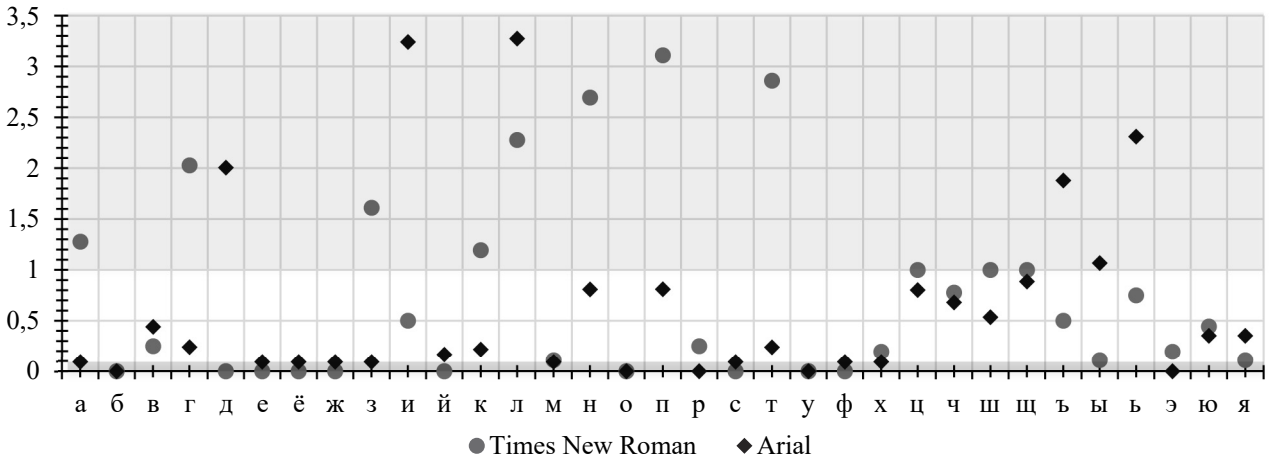

Рис. 2. Дисперсия значений оттенков при растрировании символов текста

Самым простым и удобным способом сокрытия элементов тайного сообщения в графеме будет внедрение в графемы первой группы. При осаждении в символы второй группы нужно выполнить предварительный анализ, учитывая размер кегля, конкретный документ-контейнер, количество требуемых оттенков пикселей. При сокрытии в символах третьей группы нужно анализировать конкретный документ-контейнер, учитывая не только размер кегля, но и гарнитуру, что требует больше ресурсов времени и объема оперативной памяти компьютера.

Заключение. В статье проведен анализ дискретных распределений букв русского алфавита по размеру используемого кегля и вероятностям появления определенного числа оттенков, образующихся при растрировании текстового документа (используемого в качестве стеганоконтейнера, *S*). Этот анализ основан на вычислении и использовании основных статистических параметров, что позволило разделить все буквы на три группы. А это, в свою очередь, делает алгоритм внедрения тайной информации в *S* более гибким (позволяет находить лучшие решения по быстродействию и пропускной способности) и устойчивым к случайным или преднамеренным преобразованиям *S*. При обработке графем в электронном виде предложенное разбиение на группы предполагает внедрение сообщения в наиболее сложные по строению буквы. При внедрении в остальные группы следует анализировать *S* на наличие достаточного количества оттенков для размещения информации.

Кроме того, анализ распределений пикселей при конвертации контента из PDF в PNG может быть использован для защиты авторского права путем скрытого хранения цифровых водяных знаков. Чтобы это сделать, нужно выбирать символы из разных групп, что повысит пропускную способность канала и уменьшит возможность обнаружения стеганоконтейнера визуальными или другими способами, а также упростит алгоритмы встраивания (извлечения) скрытой информации.

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., Романенко Д. М. Компьютерные сети и сетевые технологии. Минск: БГТУ, 2022. 608 с.

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. Micunocic 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. Шутько Н. П. Защита и передача текстовой информации на основе изменения кернинга // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2017. № 2 (200). С. 92–95.

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. Guo, L., Meng, X. Digital Content Provision and Optimal Copyright Protection // Management Science. 2015. Vol. 61 (5). P. 1183–1196. DOI: https://doi.org/10.1287/mnsc.2014.1972.

9. Bouchoux D. E. Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets. CengageLearning, 2017. 576 с.

10. Блинова Е. А. Стеганографический метод на основе изменения междустрочного расстояния неотображаемых символов строк электронного текстового документа // 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 // PrzeglądElektrotechniczny. 2018. Vol. 6. P. 82–85. DOI: 10.15199/48.2018.06.15.

12. 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.

13. 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.

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

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

16. 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/10.52065/2520-6729-2022-255-1-18.

17. Ковалев Е. А., Медведев Г. А. Теория вероятностей и математическая статистика для экономистов: учебник и практикум для прикладного бакалавриата. М.: Юрайт, 2016. 284 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., Romanenko D. M. *Komp'yuternyye seti i setevyye tekhnologii* [Computer networks and network technologies]. Minsk, BSTU Publ., 2022. 608 p. (In Russian).

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

4. Micunocic 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. Shutko N. P. Protection and transmission of textual information based on change. *Trudy BGTU* [Proceedings of BSTU], issue 3, Physics and Mathematics. Informatics, 2017, no. 2, pp. 92–95 (In Russian).

6. Shutko N. P. Copyright protection for electronic text documents using steganography methods. *Trudy BGTU* [Proceedings of BSTU], 2013, no. 6: 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 in-dustry, logistics and social sphere (ITI – 2019): abstracts X International scientific and technical conference]. Minsk, 2019, pp. 22–25 (In Russian).

8. Guo, L., Meng, X. Digital Content Provision and Optimal Copyright Protection. *Management Science*, 2015, vol. 61 (5), pp. 1183–1196. DOI: https://doi.org/10.1287/mnsc.2014.1972.

9. Bouchoux D. E. Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets. Cengage Learning, 2017. 576 p.

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: 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. *PrzeglądElektrotechniczny*, 2018, vol. 6, pp. 82–85. DOI: 10.15199/48.2018.06.15.

12. 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).

13. 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.

14. Ageyev V. N., Solomykov V. S. Modeling the process of rasterization of vector fonts in low-resolution output devices. *Izvestiya TulGU. Tekhnicheskiye nauki* [News of TulGU. Technical science], 2013, no. 3, pp. 9–16 (In Russian).

15. Toots Willu. *Sovremennyy shrift* [Modern typeface]. Moscow, Kniga Publ., 1966. 272 p. (In Russian).

16. 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 (In Russian). DOI: https://doi.org/10.52065/2520-6729-2022-255-1-18.

17. Kovalev E. A., Medvedev G. A. *Teoriya veroyatnostey i matematicheskaya statistika dlya ekonomistov: uchebnik i praktikum dlya prikladnogo bakalavriata* [Probability theory and mathematical statistics for economists: textbook and workshop for applied baccalaureate]. Moscow, Yurayt Publ., 2016. 284 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, pavel.urbanovich@kul.pl

Information about the authors

Saveleva Margarita Gennadievna – 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, pavel.urbanovich@kul.pl

Поступила 05.05.2023