света, возможно сопоставление вариантов осветительных установок:

– с разными источниками света и одной и той же арматурой;

– с разной арматурой и одинаковым источником света;

– с разными источниками света и разными арматурами.

При сопоставлении образцов оборудования по обобщенному показателю качества можно выбрать наилучшую электроосветительную установку.

Использование при расчете программных роботов на компьютере позволяет легко сопоставлять варианты замены одних устройств другими, т. е. профессионально решать вопросы о замене низкоэффективных образцов осветительного оборудования высокоэффективными, что поможет добиться максимальной экономии электрической энергии.

Power Automate Desktop позволяет в короткие сроки создавать программные роботы различной степени сложности.

Интуитивно понятный интерфейс делают его хорошим выбором как для профессиональных, так и для начинающих пользователей.

Кроме того, в отличие от других платформ, предоставляющих инструменты для создания программных роботов, Power Automate Desktop является бесплатным программным средством.

Изложенный способ может быть использован не только для выбора осветительных устройств, но и для любого другого оборудования.

Список литературы

1. Кириленко А. И. Нормирование освещения и энергоэффективность // Энергия и менеджмент. 2001. № 3. С. 23−25.

2. Битно Л. Г., Битно Ю. Л. Экологические светильники, или «ЭПРА» в Беларуси // Энергоэффективность. 2001. № 7. С. 24–31.

3. Дробов А. В. Электрическое освещение. Минск: РИПО, 2017. 219 с.

4. Краевская Н. П., Пустовалова Н. Н. Особенности применения метода многокритериального ранжирования при оценке эффективности электрооборудования // Труды БГТУ. Сер. III, Физ.-мат. науки и информатика. 2003. Вып. XI. С. 157–161.

5. Коровкина Н. П., Пустовалова Н. Н. Эффективность замены устаревшего электрооборудования новым, энергосберегающим // Энергоэффективность. 2005. № 7. С. 16–17.

References

1. Kirilenko A.I. Lighting rationing and energy efficiency. *Energiya i menedzhment* [Energy and management], 2001, no. 3, pp. 23–25 (In Russian).

2. Bitno L. G., Bitno Yu. L. Environmental lamps or “EPRA” in Belarus *Energoeffektivnost’* [Energy efficiency], 2001, no. 7, pp. 24−31 (In Russian).

3. Drobov A. V. *Electricheskoye osveshcheniye* [Electric eighting]. Minsk, RIPO Publ., 2017. 219 p. (In Russian).

4. Kraevskaya N. P., Pustovalova N. N. Features of the use of the multi-criteria ranking method in assessing the effectiveness of electrical equipment. *Trudy BGTU* [Proceedings of BSTU], series III, Physics and Mathematics. Informatics, 2003, issue XI, pp. 157–161 (In Russian).

5. Korovkina N. P., Pustovalova N. N. Efficiency of replacing outdated electrical equipment with energy-saving. *Energoeffektivnost’* [Energy efficiency], 2005, no. 7, pp. 16−17 (In Russian).

Информация об авторах

Пустовалова Наталья Николаевна – кандидат технических наук, доцент, доцент кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: pnn1900@yandex.by.

Коровкина Наталья Павловна − кандидат педагогических наук, доцент, доцент кафедры автоматизации производственных процессов и электротехники. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: Knp193902@yandex.by.

Information about the authors

Pustovalova Natalya Nikolaevna – PhD (Engineering), Associate Professor, Assistant Professor, the Department of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: pnn1900@yandex.by

Korovkina Natalia Pavlovna – PhD (Pedagogical), Associate Professor, Assistant Professor of the Department of Automation of Production Processes and Electrical Engineering. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: Knp193902@yandex.by

Поступила после доработки 07.09.2022

ОБРАБОТКА И ПЕРЕДАЧА ИНФОРМАЦИИ
PROCESSING AND TRANSMISSION OF INFORMATION

УДК [004.056 + 003.26](075.8)

О. А. Нистюк, П. П. Урбанович
Белорусский государственный технологический университет

МЕТОД И МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ МОДИФИКАЦИИ КОНТУРА СИМВОЛОВ ТЕКСТА-КОНТЕЙНЕРА

Текстовая стеганография является одним из направлений исследований и разработок, которая позволяет достаточно эффективно решать проблему тайной передачи или хранения информации. В статье описывается стеганографический метод, основанный на использовании параметров текста, в котором в качестве контейнера применяется документ формата .doc или .docx. Новизна рассматриваемого метода заключается в размещении тайного сообщения на основе модификации такого параметра символов текста, как контур. Излагаются особенности использования стеганографического метода в электронных изданиях с целью защиты документов-контейнеров от несанкционированного копирования или распространения. Представлено разработанное программное средство, демонстрирующее работу стеганографического метода: описан пользовательский интерфейс приложения, технология разработки, а также основные структурные элементы его архитектуры.

Ключевые слова: стеганография, документ, .docx, метод, сокрытие.

Для цитирования: Нистюк О. А., Урбанович П. П. Метод и математическая модель стеганографического преобразования информации на основе модификации контура символов текста-контейнера // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2022. № 2 (260). С. 92–98.

O. A. Nistyuk, P. P. Urbanovich
Belarusian State Technological University

METHOD AND MATHEMATICAL MODEL OF STEGANOGRAPHIC INFORMATION CONVERSION BASED ON MODIFICATION OF CONTOUR OF TEXT-CONTAINER SYMBOLS

Text steganography is one of the areas of research and development, which allows to solve the problem of secret transmission or storage of information quite effectively. The article describes a steganographic method based on the use of text parameters, in which a .doc or .docx document is used as a container. The novelty of the considered method lies in the placement of a secret message based on the modification of such a parameter of text characters as a contour. The features of the use of the steganographic method in electronic publications are outlined in order to protect container documents from unauthorized copying or distribution. The developed software tool demonstrating the operation of the steganographic method is presented: the user interface of the application, the development technology, as well as the main structural elements of its architecture are described.

Key words: steganography, document, .docx, method, hiding.

For citation: Nistyuk O. A., Urbanovich P. P. Method and mathematical model of steganographic information conversion based on modification of contour of text-container symbols. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*, 2022, no. 2 (260), pp. 92–98 (In Russian).

Введение. Значительная часть информации, относящейся к различным сторонам деятельности предприятий или организаций, а также частных лиц, сейчас хранится или передается в электронном виде. В связи с этим проблема надежной ее защиты от несанкционированного копирования, модификации или использования является чрезвычайно актуальной. Существуют различные

методы и средства для реализации такой защиты. Текстовая стеганография является одним из направлений исследований и разработок, которая позволяет достаточно эффективно решать указанную проблему.

Основы методов размещения тайной информации в текстовых документах-контейнерах были описаны в работах, датируемых концом прошлого века. В это время появились статьи Дж. Брассила (J. Brassil), Н. Максемчука (N. Maxemchuk) и др. (см., например, [1]). Элементами текстовых документов-контейнеров, модификация которых позволяла размещать (осаждать) тайную информацию, были расстояния между строками, между словами в строке, невидимые символы окончания строки и др. Позднее к числу таких модифицируемых элементов добавились цветовые и пространственно-геометрические параметры (апрош и кернинг) используемых символов текста [2–5], а также иные параметры текстов и составляющих их элементов [6–7]. При более детальном анализе системных свойств и параметров текстовых документов [8] выявилось, в частности, еще одно направление для стеганографического приложения, заключающееся в возможности размещения тайной информации путем модификации свойств такого параметра, как контур символов.

Рассмотрение и анализ сущности метода и особенностей алгоритма его реализации в виде конечного программного продукта составляют предмет настоящей статьи.

Основная часть. Среди множества известных на данный момент методов защиты текстовой информации ни один не дает гарантии полного сокрытия сообщения в носителе. Процесс размещения тайного сообщения (или цифрового водяного знака) подразумевает изменение некоторых параметров контейнера.

Компьютерная графика добавила символам текста еще одну существенную характеристику – контур, который также может быть использован для размещения тайной информации в текст по аналогии с известными методами графической стеганографии [1–6].

При рассмотрении метода будем использовать общую терминологию [9]. Документ, который мы хотим защитить, называется контейнером или файлом-контейнером, *C*. Текст, с помощью которого осуществляется такая защита путем его размещения в контейнере или же который размещается для передачи, – стегосообщение, *M*. Контейнер с размещенным сообщением – стегоконтейнер, *S*.

На рис. 1 приведено диалоговое окно текстового процессора MSWord, в котором отображены параметры контура. Численные значения этих параметров (справа) приводят к наименее заметным для человеческого глаза изменениям. Это установлено нами на основе множественных экспериментов и тестов.

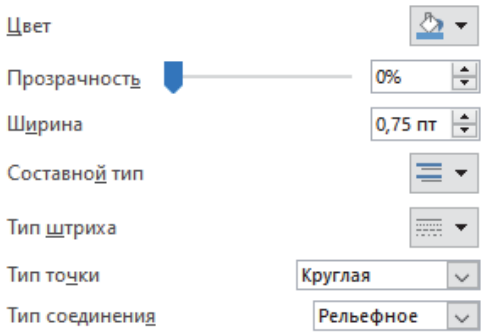

Рис. 1. Параметры контура символа

Подробнее охарактеризуем каждый параметр контура.

1. *Цвет*. Данный параметр варьируется по цветовому кругу. В предлагаемом методе предполагается, что значение этой характеристики должно соответствовать цвету (коду на основе модели RGB) символов основного текста (контейнера).

2. *Прозрачность*. Параметр характеризует уровень прозрачности контура текста. Значения данного параметра находится в диапазоне от 0 до 100%. На визуальном уровне 95% прозрачность контура заметна человеческому глазу в виде неровностей контура при масштабируемости до 500%. Однако значение 96% и более является оптимальным в использовании.

3. *Ширина* контура показывает значение толщины линии вне буквы в пунктах (пт). Параметр не имеет отрицательной величины, а также не имеет максимального значения. Значение данной характеристики необходимо устанавливать в диапазоне от 0,05 пт и меньше, так как при большей величине данного параметра визуально заметны изменения в очертании символа, что было выявлено при опросе студентов.

4. *Составной тип*. Данный параметр отвечает за то, каким образом будет выглядеть линия. Может принимать следующие значения: простая, двойная, толстая-тонкая, тонкая-толстая, тройная. Для метода целесообразно выбирать тип «непрерывная» (простая), так как в других случаях могут быть заметны пустоты на очертаниях контура.

5. *Тип штриха*. Параметр отвечает за то, каким образом будет строиться линия, из каких частей она будет состоять. Возможны следующие типы: сплошная линия, круглые точки, квадратные точки, штрих, штрих-пунктир, длинный штрих, длинный штрих-пунктир, длинный штрих-двойной пунктир.

Параметр зависит от шрифта основного текста. Если шрифт без засечек, необходимо использовать либо сплошную линию, либо круглые точки. Однако при использовании шрифта с засечками

лучше использовать квадратные точки, чтобы убрать лишнюю плавность на изгибах символа.

6. *Тип завершения*. Каждая линия состоит из множества точек. Данный параметр отвечает за форму точки на конце кривой. Доступны для выбора следующие значения: прямоугольное, плоское, скругленное. Данный параметр работает аналогично предыдущему. Он также зависит от шрифта текста.

7. *Тип соединения*. Параметр отвечает за то, каким образом будут соединяться точки между собой. Значения: скошенное, скругленное, фацетное. Тип соединения точек зависит от всех вышеперечисленных параметров, то есть от типа линии, типа завершения, толщины.

Необходимо выставить определенные (из числа перечисленных) параметры символа так, чтобы это было визуально незаметно. Таким образом можно скрыть необходимую информацию в документе-контейнере.

На рис. 2 приведен пример модификации параметров контура для различных символов алфавита. Даже при большом увеличении визуально незаметны какие-либо изменения в символах текста, хотя к некоторым символам добавлен контур.

Рис. 2. Пример использования контура

Предлагаемая модель стеганографического преобразования строится на основе следующих обозначений и положений.

Пусть M – это конечное множество сообщений, которые могут быть тайно размещены в контейнере: $M = \{M_1, M_2, ..., M_s\}$; каждое из таких сообщений может быть представлено в бинарной форме: $M_i \to M_i^2 = \{m_{i1}, m_{i2}, ..., m_{in}\}$, где $m_{\_\_}$ – символ битовой последовательности, а $i = \overline{1,s}$; C – это конечное множество используемых контейнеров: $C = \{C_1, C_2, ..., C_p\}$; контейнер C_j можно представить как совокупность отдельных символов текста $C_j = \{c_{j1}, c_{j2}, ..., c_{jd}\}$, здесь $j = \overline{1,p}$, при этом должно выполняться условие $d \ge \frac{n}{x} + 1$, где $x = \{2, 4, 8\}$; x соответствует количеству битов сообщения M_i^2 на символ контейнера C_j.

Сообщение M_i^2 представляется как конкатенация из q двоичных блоков: $M_i^2 = \{b_{i1}, b_{i2}, \ldots, b_{iq}\}$, где $b_{\_\_}$ – двоичный блок, а $q = \frac{n}{x}$ – блок $b_{ik} = \{m_{ie} \mid m_{ie} \in M_i^2,\ x(k-1)+1 \le e \le kx, k = \overline{1,q}\}$.

Каждый блок делится на две равные части длины $\frac{x}{2}$ битов: $b_{ik} = (b_{ik}^l, b_{ik}^r)$, где индексы l и r обозначают левую и правую половины блока соответственно.

Определено вспомогательное множество $B = \{!, ", \#, \$, \%, \&, ', (,), *, +, «,», -, ., /, :, ;, <, =, >, ?, @, [,], ^, _, `, {, |, }, ~, –, \\s, \}$. В него включены символы, которые не могут быть дополнены контуром.

В предлагаемом методе используются такие характеристики контура символа: прозрачность (этот параметр обозначим символом t) и толщина (этот параметр обозначим символом w).

Пусть C_j контейнер, в который внедряется сообщение, а c_{jg} – g-й символ этого контейнера. Тогда после осаждения информации с использованием предложенного метода c_{jg} примет вид c_{jg}^{tw}.

$$c_{jg}^{tw} = \begin{cases} c_{jg},\ c_{jg} \in B, \\ c_{jg}^{f(b_{ik}^l) f(b_{ik}^r)},\ c_{jg} \notin B, \end{cases} \qquad (1)$$

$$f : A \to H,$$

где A – множество значений $b_{ik}^l,\ b_{ik}^r$ и $H = \{h \mid 1 \le h \le 2^{x/2}\}$; H – множество состояний параметров контура символов.

В обозначении вида c_{jg}^{tw} индексы t и w – состояния прозрачности и толщины контура соответственно, где соотношение между состояниями и конкретными значениями устанавливаются следующими функциями:

$$f' : H \to T; \qquad (2)$$

$$f'(t) = t'_{\min} + \frac{t'_{\max} - t'_{\min}}{2^{x/2} - 1} \cdot (t-1), \qquad (3)$$

здесь $t'_{\min}$ – минимальное значение прозрачности контура $t'_{\min} = 96\%$; $t'_{\max}$ – максимальное значение прозрачности контура, $t'_{\max} = 100\%$.

При этом точность вычислений прозрачности принимается на уровне трех знаков после запятой.

$$g' : H \to W; \qquad (4)$$

$$g'(w) = w'_{\min} + \frac{w'_{\max} - w'_{\min}}{2^{x/2} - 1} \cdot (w-1), \qquad (5)$$

здесь $w'_{\min}$ – минимальное значение толщины контура, $w'_{\min} = 0{,}05$ пт; $w'_{\max}$ – максимальное значение толщины контура, $w'_{\max} = 0{,}10$ пт.

При этом точность вычислений толщины принимается на уровне двух знаков после запятой.

В результате внедрения сообщения M_i в документ-контейнер C_j состояние последнего можно записать в форме

$$C_j = \{c_{j1}^{tw}, c_{j2}^{tw}, ..., c_{jg}^{tw}\}.$$

Для более высокой стегостойкости системы информация размещается не в последовательно идущие символы контейнера, а по принципу псевдослучайности. Длина используемого диапазона контейнера для внедрения вычисляется по следующей формуле:

$$r = \left[\frac{\left| C_j^{'} \right|}{(n / x)} \right]; \quad (6)$$

$$C_j^{'} = \{c_{jg} \mid c_{jg} \in C_i,\ c_{jg} \notin B\}; \quad (7)$$

$$F : \mathrm{X} \to Z, \mathrm{X} = \{\chi \mid 1 \le \chi \le r\}, \quad (8)$$

где $C_j^{'}$ – подмножество символов контейнера, за исключением символов, входящих в множество B; X – множество всех возможных значений случайной величины; r – длина подпоследовательности символов контейнера, в случайный элемент которой будет осаждено x битов информации.

Рассмотрим алгоритмические особенности реализации предлагаемого метода, в котором осаждение информации производится путем изменения параметров контура символов в соответствии с определенными правилами размещения информации в контейнере.

Предположим, необходимо скрыть информацию M_i в файле-контейнере C_j, который имеет размер d (d – количество символов в тексте).

Сообщение M_i преобразуется в двоичный вид M_i^2. Вычисляется также параметр n – количество символов сообщения M_i^2. Например, C = «Helloworld». Здесь d = 10. Пусть M = «M». Тогда M_i^2 = 11001100, т. е. n = 8.

При конвертации текстовой информации в битовую последовательность используются коды из таблицы Win-1251. В данном методе важна кодировка, поскольку при переводе символов, используемых в стегосообщении, в бинарный вид нужно, чтобы длина битовой последовательности любого символа была одинаковой.

Необходимо, чтобы выполнялось условие

$$d \ge \frac{n}{x} + 1, \quad (9)$$

где d – количество символов файла-контейнера; n – количество символов битовой последовательности тайного сообщения; x – количество битов на символ носителя.

В соответствии с (9) выполняется проверка того, достаточен ли объем контейнера C для внедрения M. В правой части неравенства производится расчет минимально необходимого количества символов для данного сообщения M. Дополнительный символ необходим для обозначения флага конца внедряемого сообщения.

Для внедрения M в файл-контейнер с расширением .docx нужно выполнить нижеуказанную последовательность операций.

1. Создать тайное сообщение M формата .docx, .doc, .txt либо .pdf (назовем его *Test*1).

2. Преобразовать текст из документа *Test1* в бинарную форму. Полученную последовательность назовем M_i^2.

3. Вычислить n полученного бинарного сообщения M_i^2.

4. Создать контейнер формата .docx (*Test*2). Размещенный внутри документа текст назовем C.

5. Посчитать d в контейнере C, не учитывая знаки препинания, так как при применении контура к знакам препинания визуально заметна деформация символов.

6. Выбрать число x = {2, 4, 8}, представляющее количество битов бинарного сообщения на символ контейнера.

7. Если справедливо условие (8), то выполнить процесс внедрения сообщения M_i^2 в контейнер согласно пунктам (8–11).

8. Извлечь x битов сообщения M_i^2. Сдвиг битовой последовательности произвести на x позиции вправо для того, чтобы алгоритм прошел по всем значениям бинарного представления сообщения.

9. Первые $\frac{x}{2}$ извлеченных битов «отвечают» за значение прозрачности контура, а оставшиеся – за толщину контура символа.

10. На основе значений битов применить к символу параметр контура с определёнными характеристиками. Значения характеристик контура при конкретных значениях битов определяются в соответствии с математической моделью.

11. Если битовая последовательность закончилась, то процесс сокрытия считать завершенным. Иначе, возвращаемся к п. 8.

Для извлечения сообщения M необходимо соблюдать следующую последовательность действий.

1. Получить контейнер *Test*2 с внедренной информацией.

2. Перейти к символу C_j, где C_j – j-й символ текста носителя. Начальное значение j = 1.

3. Извлечь информацию о контуре символа C_j.

4. Если у символа обнаружен контур, то перейти к п. 5, иначе – к п. 6

5. В соответствии с математической моделью, приведенной выше, извлечь биты информации.

6. Записать в общую бинарную последовательность извлеченные биты со сдвигом влево. Значение сдвига n вычисляется по формуле (10):

$$n = 2 \cdot (j - 1). \quad (10)$$

7. Для перехода к следующему символу увеличить значение i на 1.

8. Если выполняется неравенство (11), то перейти к п. 2. Иначе, перейти к пункту 9.

$$j < d. \quad (11)$$

9. Перевести извлеченную бинарную последовательность в символьное представление.

Далее необходимо оценить, как влияет процесс внедрения сообщения в контейнер на объем файла. Алгоритм реализации метода характеризуется линейной сложностью $O(n)$.

При исследовании влияния сообщения на объем контейнера необходимо учитывать следующие характеристики:

1) объем внедряемого сообщения;

2) объем документа-контейнера;

3) количество информации в документе, которая не подлежит осаждению;

4) количество битов сообщения, переведенного в двоичный вид, на символ контейнера.

Сравним объем контейнеров C и C', где C – контейнер без внедренной информации; C' – носитель информации. Рис. 3 дает определенное представление об изменении анализируемого параметра.

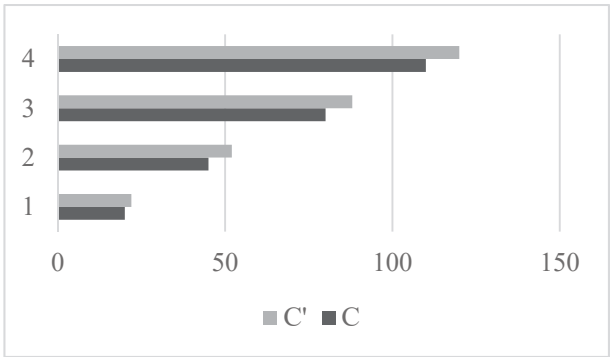

Рис. 3. Влияние модификации контура на размер файла-контейнера

Создано приложение, которое реализует предложенный метод. Программная платформа – язык программирования C#10 (платформа .NET6) с использованием фреймворка Windows Presentation Foundation (WPF). Для работы с word-файлами использовалась библиотека Open XML 2.16, для работы с pdf-файлами – iText 7.

В приложении реализованы следующие функции.

1. *Внедрение информации*. При осаждении информации необходимо выбрать файл либо ввести сообщение, затем выбрать файл-контейнер, нажав на кнопку «Открыть документ-контейнер». Далее необходимо выбрать, какое количество бит сообщения будет осаждаться в один символ файла-контейнера. Проверить, соответствует ли размер сообщения размерам контейнера в соответствии с методом по нажатию на кнопку «Проверить условие» (рис. 4). Для осаждения информации нажимаем на кнопку «Внедрить сообщение». Если слово «Статус» имеет зеленый цвет, то осаждение информации в носитель произошло успешно, если красный – процесс завершен с ошибкой.

2. Извлечение информации. При извлечении сообщения из файла необходимо выбрать носитель, количество битов на символ сообщения и нажать на кнопку «Извлечь сообщение». В окне вывода появится тайное сообщение (рис. 5). Также можно сохранить извлеченное сообщение в файл.

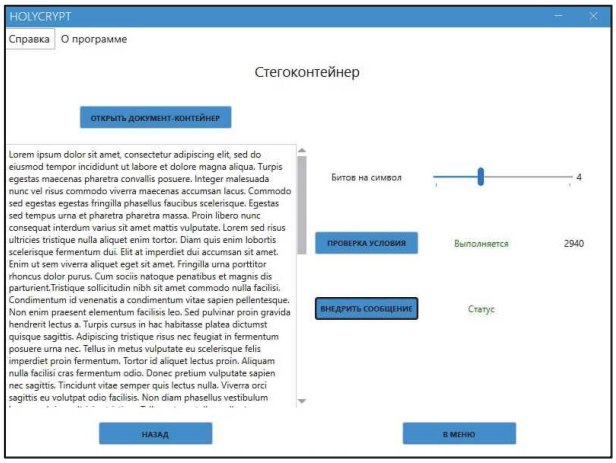

Рис. 4. Вид окна приложения при внедрении сообщения

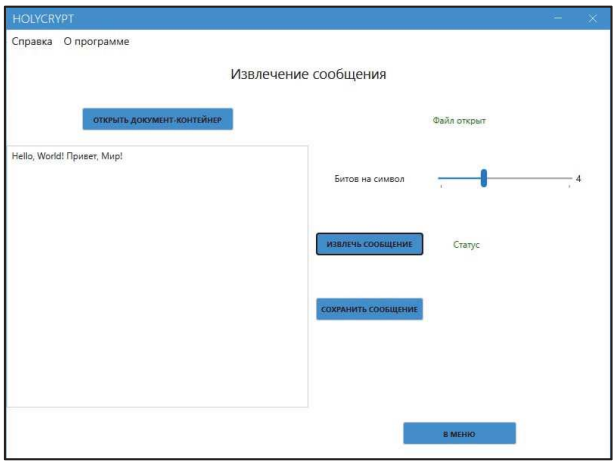

Рис. 5. Вид окна приложения при извлечении сообщения

Сравнительная характеристика методов

Метод	Соотношение «сигнал – шум»	Устойчивость	Скрытость	Качество сокрытия
Метод изменения регистров символа	10	5	5	0
Метод добавления хвостовых пробелов	0	5	0	5
Знаки одинакового начертания	5	5	0	0
Метод изменения контура символа	5	3	8	9

Заключение. Предложенный и проанализированный стеганографический метод передачи информации в тексте-контейнере основан на изменении контура символов контейнера. В результате анализа различных модификаций характеристик параметра символа получен алгоритм, исследованы наиболее уязвимые характеристики параметра текста.

Для сравнения с известными стеганографическими методами (например, метод изменения регистров символа, метод добавления хвостовых пробелов, знаки одинакового начертания) можно использовать следующие характеристики: качество сокрытия (нельзя выразить численно, так что лучший способ измерить эту характеристику – представить нескольким наблюдателям контейнеры до и после внедрения), скрытость (атакующая сторона может определить наличие сообщения в контейнере путем подсчета определенных статистических свойств файла и сравнения полученных результатов со значениями, которые ожидаются от таких типов файла), устойчивость (мера способности алгоритма сохранять сообщение даже после того, как контейнер подвергался неким изменениям), соотношение «сигнал – шум» (эта величина является мерой качества).

Таким образом, была составлена таблица, в которой даны оценки каждой характеристики метода (0 – худшее ожидание, 10 – лучшее значение характеристики). В таблице представлены сравнительные характеристики трех вышеперечисленных методов и предложенного метода с использованием контура символа (4).

В результате исследования проведен анализ предложенного метода по вышеперечисленным характеристикам.

Список литературы

1. Electronic Marking and Identification Techniques to Discourage Document Copying / J. Brassil [et al.] // IEEE Journal on Sel. Areas in Commun., 13. 1995, No. 8, P. 1495–1504.

2. Шутько Н. П. Алгоритмы реализации методов текстовой стеганографии на основе модификации пространственно-геометрических и цветовых параметров текста // Труды БГТУ. 2016. № 6 (188): Физ.-мат. науки и информатика. С. 160–165.

3. Shutko N. The use of aprosh and kerning in text steganography // PrzeglądElektrotechniczny. 2016. No. 10. P. 222–225.

4. Shutko N., Urbanovich P., Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh // PrzeglądElektrotechniczny. 2018. R. 94, NR 6. P. 82–85.

5. Сущеня А. А., Блинова Е. А., Урбанович П. П. Модификация стеганографического метода изменения междустрочного расстояния электронного документа // Технические средства защиты информации: тез. докл. XVI Белорусско-российской науч.-техн. конф., Минск, 5 июня 2018 г. Минск, 2018. С. 90.

6. Agarwal M. Text steganographic approaches: a comparison // International Journal of Network Security & Its Applications (IJNSA). 2013. Vol. 5, No. 1. P. 91–103.

7. Сущеня А. А., Урбанович П. П. Применение форматов электронных книг при передаче конфиденциальной информации методами компьютерной стеганографии // Информационные технологии: материалы 83-й науч.-техн. конф. профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4–15 февраля 2019 г. Минск, 2019. С. 39–40.

8. Урбанович, П. П., Юрашевич Д. Э. Использование системных свойств и параметров текстовых файлов в стеганографических приложениях // Теоретическая и прикладная криптография: материалы междунар. науч. конф., Минск, 20–21 октября 2020 г. Минск, 2020. С. 68–73.

9. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. Минск: БГТУ, 2016. 220 с.

References

1. Brassil J., Low S., Maxemchuk N. F., O'Gorman L. Electronic Marking and Identification Techniques to Discourage Document Copying. *IEEE Journal on Sel. Areas in Commun*., 13, 1995, no. 8, pp. 1495–1504.

2. Shutko N. P. Algorithms for the implementation of text steganography methods based on the modification of spatial-geometric and color parameters of the text. Trudy BGTU [Proceedings of BSTU]. 2016, no. 6 (188): Physics and Mathematics. Informatics. pp. 160–165 (In Russian).

3. Shutko N. The use of aprosh and kerning in text steganography. *PrzeglądElektrotechniczny*. 2016. no. 10, pp. 222–225.

4. Shutko N., Urbanovich P., Zukowski P. A method of syntactic text steganography based on modification of the document-container aprosh. *PrzeglądElektrotechniczny*. 2018. R. 94, NR 6, pp. 82–85.

5. Sushchenya A. A., Blinova E. A., Urbanovich P. P. Modification of the steganographic method of changing the line spacing of an electronic document. Tekhnicheskie sredstva zashchity informacii: tezisy dokladov XVI Belorussko-rossijskoj nauchno-tekhnicheskoj konferencii [Technical means of information protection: abstracts of reports of the XVI Belarusian-Russian scientific-technical conference]. Minsk, BGUIR, 2018, p. 90 (In Russian).

6. Agarwal M. Text steganographic approaches: a comparison. *International Journal of Network Security & Its Applications* (*IJNSA*), 2013, Vol. 5, no. 1, pp. 91–103.

7. Sushchenya A. A., Urbanovich P. P. The use of electronic book formats in the transmission of confidential information using computer steganography methods. Informacionnye tekhnologii: materialy 83-j nauchno-tekhnicheskoj konferencii professorsko-prepodavatel'skogo sostava, nauchnyh sotrudnikov i aspirantov (s mezhdunarodnym uchastiem) [Information technologies: materials of the 83rd scientific and technical conference of professors teaching staff, researchers and graduate students (with international participation)]. Minsk, BSTU, 2019. pp. 39–40. (In Russian).

8. Urbanovich P. P., Yurashevich D. E. Using system properties and parameters of text files in steganographic applications. Teoreticheskaya i prikladnaya kriptografiya: materialy mezhdunarodnoj nauchnoj konferencii [Theoretical and applied cryptography: materials of the international scientific conference]. Minsk, 2020, pp. 68–73. (In Russian).

9. Urbanovich P. P. *Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii: ucheb.-metod. posobiye* [Protection of information by cryptography, steganography and obfuscation methods: textbook. allowance]. Minsk: BGTU, 2016. 220 p. (In Russian).

Информация об авторах

Нистюк Ольга Александровна – магистрант кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: nistyuk@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

Nistyuk Olga Alexandrovna – Master's degree student, the Department of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: nistyuk@belstu.by

Urbanovich Pavel Pavlovich – DSc (Engineering), Professor, Professor of 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 после доработки 07.09.2022