Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

DOI: 10.37943/AITU.2020.15.23.009
UDC: 621.397

O. Kan
PhD, Associate Professor, Department of Information Technology and Security
saspet@mail.ru, orcid.org/0000-0002-0661-5968
Karaganda State Technical University, Kazakhstan

E. Murykh
Senior Lecturer, Department of Information Technology and Security
murykh@mail.ru, orcid.org/0000-0002-9347-2036
Karaganda State Technical University, Kazakhstan

CONFIDENTIAL INFORMATION SECRET METHOD

Abstract: The article deals with the issues of hiding text information in a graphic file. Most often, one or two least significant bits of the image pixels are modified. To do this, each byte of the secret message is divided into 8 or 4 parts. The use of the least significant bits of the graphic file for transmitting a secret message significantly limits the size of the original message, in addition, it allows steganographic analysis programs to detect and decrypt the transmitted data. A formula for hiding textual information in image pixels is proposed. The algorithm for hiding information is that the bytes of the secret message are mixed with the bytes of pixels of the key image using a secret formula. The result is new bytes of image pixels. A steganography scheme has been developed for embedding secret text in random image pixels. Random bytes are pre-embedded in each pixel row of the original image. As a result of the operations, a key image is obtained. Text codes are embedded in random pixel bytes of a given RGB channel. To generate a secret message, the characters of the table of ASCII codes are used. The detection and decryption program compares the pixels of the received image with the pixels of the key image in the specified RGB channel and extracts the codes of the encrypted text. The use of abstract images as a key image significantly increases the reliability of the protection of confidential information, since in such images there is a random change in pixel values. Demonstration programs for encryption and decryption in the Python 3.5.2 programming language have been developed. A graphic file is used as the decryption key. The developed steganography scheme allows not only transmitting sensitive information, but also adding digital fingerprints or hidden tags to the image.

Keywords: steganography, information hiding, image key, image pixels, embedding formula.

DOI: 10.37943/AITU.2020.15.23.009

Кан О.А.
к.т.н., доцент кафедры информационных технологий и безопасности
saspet@mail.ru, orcid.org/0000-0002-0661-5968
Карагандинский государственный технический университет, Казахстан

Мурых Е.Л.
старший преподаватель кафедры информационных технологий и безопасности
murykh@mail.ru, orcid.org/0000-0002-9347-2036
Карагандинский государственный технический университет, Казахстан

МЕТОД СОКРЫТИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Аннотация: Рассмотрены вопросы сокрытия текстовой информации в графическом файле. Наиболее часто модифицируют один или два младших бита пикселов изображения. Для этого каждый байт секретного сообщения разбиваются на 8 или 4 части. Использование младших битов графического файла для передачи секретного сообщения значительно ограничивает размеры исходного сообщения, кроме того, позволяет программам стеганографического анализа обнаруживать и дешифровать передаваемые данные. Предложена формула и разработан алгоритм встраивания секретного текста в случайные пиксели изображения. Алгоритм сокрытия информации заключается в том, что байты секретного сообщения смешиваются с байтами пикселей изображения-ключа по секретной формуле. В результате получаются новые байты пикселей изображения. В каждую строку пикселей исходного изображения предварительно встраиваются случайные байты. В результате проведенных операций получается изображение-ключ. Коды текста встраиваются в случайные байты пикселей заданного канал RGB. Для формирования секретного сообщения использованы символы таблицы ASCII кодов. Программа обнаружения и дешифрования сравнивает пиксели принятого изображения с пикселами изображения-ключа в заданном канале RGB и выделяет коды зашифрованного текста. Применение абстрактных картинок в качестве изображения-ключа значительно повышает надежность защиты конфиденциальной информации, так как в таких картинках присутствует случайное изменение значений пикселей. Разработаны программы шифрования и дешифрования на языке программирования Python 3.5.2. В качестве ключа для дешифрования используется графический файл. Разработанная схема стеганографии позволяет не только передавать секретную информацию, но и добавлять к изображению цифровые отпечатки или скрытые метки.

Ключевые слова: стеганография, сокрытие информации, изображение-ключ, пиксели изображения, формула встраивания.

Введение

В последние годы развитие информационных технологий предъявляет повышенные требования к решению вопросов информационной безопасности. В этой связи возникает задача поиска и разработки новых методов защиты информации. Современные компьютерные технологии и прогресс в области компьютерных сетей обеспечивает возможность разработки и реализации новых методов, предназначенных для обеспечения компьютерной информационной безопасности. В последние годы получило развитие новое направление в области защиты информации – компьютерная стеганография.

Методы компьютерной стеганографии могут быть классифицированы по целям использования, по виду выбранного контейнера для встраивания, по структуре контейнера. По виду контейнера методы стеганографии классифицируют на методы, подвергающие моди-

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

фикации, данные и программы, текст, графические изображения, аудио и видео [1,2]. Методы компьютерной стеганографии основаны на избыточности передаваемой информации в файлах видео, аудио и изображений. В графических файлах изменение или искажение отдельных пикселей не сказывается на их качестве, но позволяет скрытно передавать конфиденциальную информацию.

Анализ последних исследований и публикаций

Среди методов сокрытия информации в графических изображениях широко применятся метод скрытия информации LSB, в котором младшие биты в байтах изображения, отвечающих за кодирование цвета, заменяются на биты секретного сообщения [2,3]. Наиболее часто модифицируют один или два младших бита пикселов изображения. Для этого каждый байт секретного сообщения разбиваются на 8 или 4 части. Затем полученные части заменяют младшие биты байтов изображения. При изменении младших бит в каждом байте изображение практически не искажается, так как данные изменения не существенны. В результате получим возможность скрытно передать сообщение размером в 1/8 размера файла-контейнера при использовании одного младшего бита в каждом байте изображения, или размером в 1/4 размера файла-контейнера при использовании двух младших бит в байтах изображения [4]. Недостатком метода LSB является простота обнаружения скрытой информации существующими методами дешифрования.

Другим популярным методом стеганографии является использование особенностей форматов данных, использующих сжатие с потерей данных. Этот метод (в отличие от LSB-метода) более стоек к преобразованиям и обнаружению, так как имеется возможность в широком диапазоне варьировать качество сжатого изображения, что делает практически невозможным обнаружение встроенной информации [4-6]. В качестве данных может использоваться любая информация: текст, звуковое сообщение, изображение и т. п.

Классификация известных методов стеганографии, являющихся основой для разработки новых алгоритмов, представлена в [1]. Развитие методов встраивания данных как в пространственной, так и в частотной области шло, как правило, по пути усложнения алгоритмов встраивания и поиска функций для выбора бит, подлежащих замене, максимально похожим на случайную величину [7,8].

Широко используются методы стеганографии для добавления к изображению stegomarks. Это незаметные без специальной обработки биты, идентичные для всех файлов одного человека. Например, такие метки записываются в цифровые фотографии для того, чтобы можно было доказать их авторство [9-10].

В работе [4] предлагается модификация метода встраивания секретной информации для метода графической стеганографии LSB. Суть модификации заключается в следующем. Секретный текст в соответствии с кодировкой ASCII преобразуется в соответствующие числовые коды. Например, исходный текст ABBA заменяется числовым кодом 65 66 66 65. Для встраивания четырех чисел в рассматриваемом случае потребуется четыре пикселя изображения. В данном методе используется замена значений трех составляющих цвета каждого пикселя (red, green, blue) не в двоичном, как в классическом LSB методе, а в десятичном виде. Замене подлежат наименее значимые (младшие) цифры значений соответствующего цветового канала. Так как числа двухзначные, то используются две составляющие цвета red и blue. При использовании символов кириллицы (ASCII коды >127), потребуется задействовать и зеленую составляющую пикселя.

Анализ современных методов стеганографии показал, что они лишь частично удовлетворяют требованиям, предъявляемых к системам скрытой передачи данных. Использование младших битов графического файла для передачи секретного сообщения значительно ограничивает размеры исходного сообщения, кроме того, позволяет программам стега-

DOI: 10.37943/AITU.2020.15.23.009

нографического анализа обнаруживать и дешифровать передаваемые данные. Именно поэтому задача создания стойкого алгоритма и разработка на его основе программного продукта для скрытия достаточно большого объема данных методами цифровой стеганографии является весьма актуальной.

Алгоритм сокрытия информации

В статье предлагается алгоритм стеганографии, в которой полностью используются все биты байтов графического файла, а в качестве секретного ключа используется изображение-ключ. С целью повышения безопасности, в каждую строку пикселей исходного изображения предварительно встраиваются случайные байты. В результате проведенных операций получается изображение-ключ. Встраивание секретной информации производится в случайные байты каналов RGB графического файла (изображения-ключа). Следует отметить, что для изображения-ключа выбирается графический файл с большим количеством часто меняющихся цветов.

Алгоритм сокрытия информации заключается в том, что байты секретного сообщения смешиваются с байтами пикселей изображения-ключа по секретной формуле. В результате получаются новые байты пикселей изображения. Полученный графический файл-контейнер с встроенным сообщением передается получателю по каналу передачи, например, через интернет. Программа обнаружения и дешифрования сравнивает пиксели принятого изображения с пикселами изображения-ключа в заданном канале RGB и выделяет коды зашифрованного текста. Затем с помощью алгоритма дешифрования получают исходное сообщение. Изображение-ключ и программа для дешифрования передаются получателю заранее любым защищенным способом, исключающим перехват другими лицами. Периодически можно менять изображение-ключ с целью повышения безопасности.

В программе используется для встраивания секретной информации канал RED графического файла. После окончания работы цикла встраивания байтов секретной информации, изображение сохраняется в файле p2.png (изображение-контейнер). В качестве исходного изображения используется файл p1.png (изображение-ключ). После запуска программы открывается диалоговое окно для ввода секретного сообщения. На рисунке 1 показано диалоговое окно для ввода секретного текста.

Рис. 1. Диалоговое окно для ввода секретной информации

На рисунке 2 показана блок-схема алгоритма встраивания байтов секретного сообщения в файл изображения-ключа. Алгоритм стеганографии реализован на языке Python 3.5.2. Для формирования секретного сообщения использованы символы таблицы ASCII-кодов.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

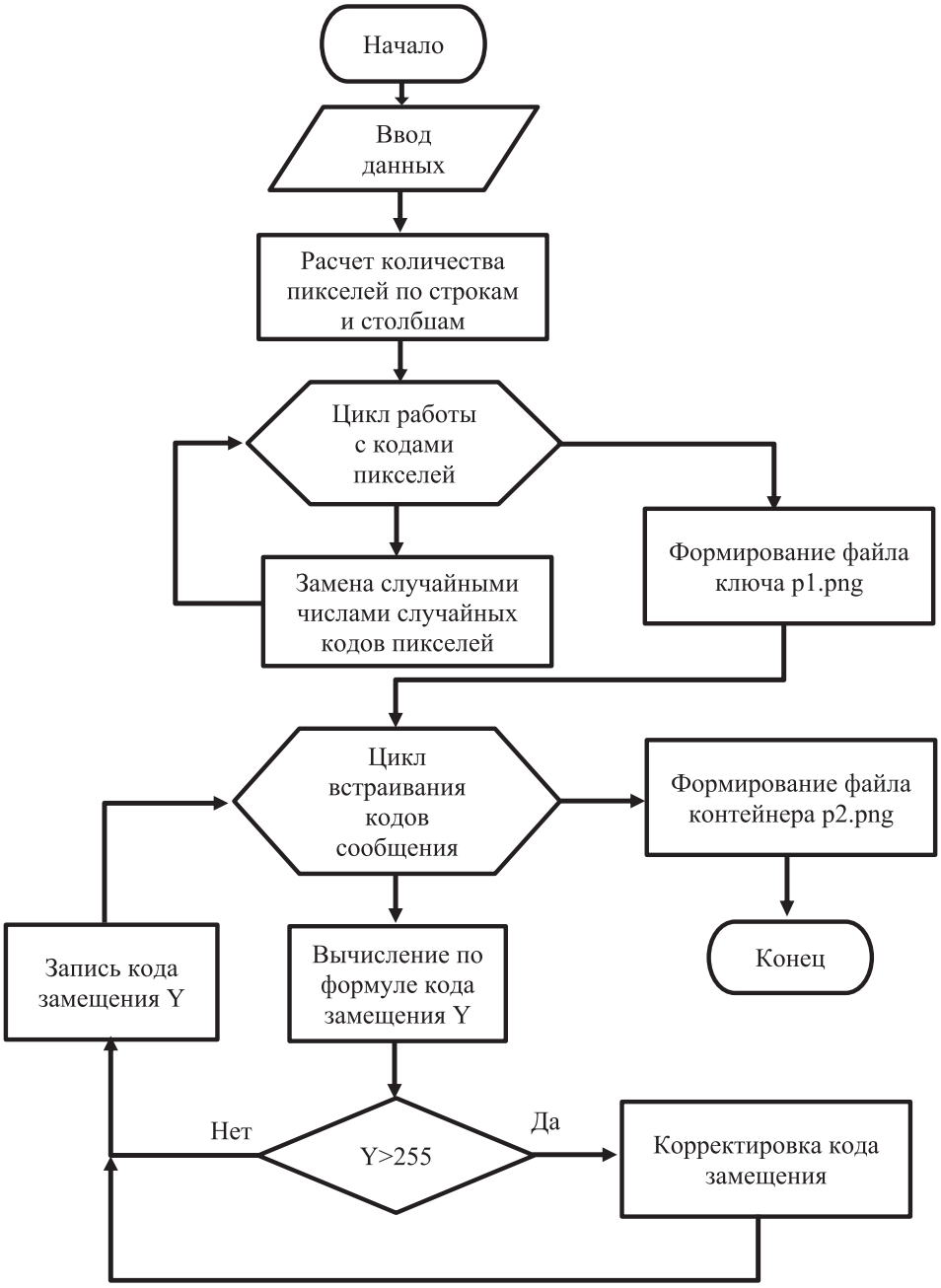

Рис. 2. Блок-схема алгоритма встраивания секретного сообщения в файл изображения

Для встраивания больших объемов данных можно использовать все каналы RGB изображения-ключа. В демонстрационной программе используется для встраивания секретной информации канал RED графического файла. После окончания работы цикла встраивания байтов секретной информации, изображение сохраняется в файле p2.png (изображение -контейнер). В качестве исходного изображения используется файл p1.png (изображения -ключа).

Полученный файл-контейнер p2.png с встроенной секретной информацией передается получателю по открытому каналу. Получатель с помощью программы дешифрования и изображения-ключа p1.png извлекает секретный текст сообщения. Для этого программа дешифрования сравнивает пикселы двух изображений и выделяет байты секретного сообщения. На рисунке 3 показана блок-схема алгоритма дешифрования встроенного секретного сообщения.

DOI: 10.37943/AITU.2020.15.23.009

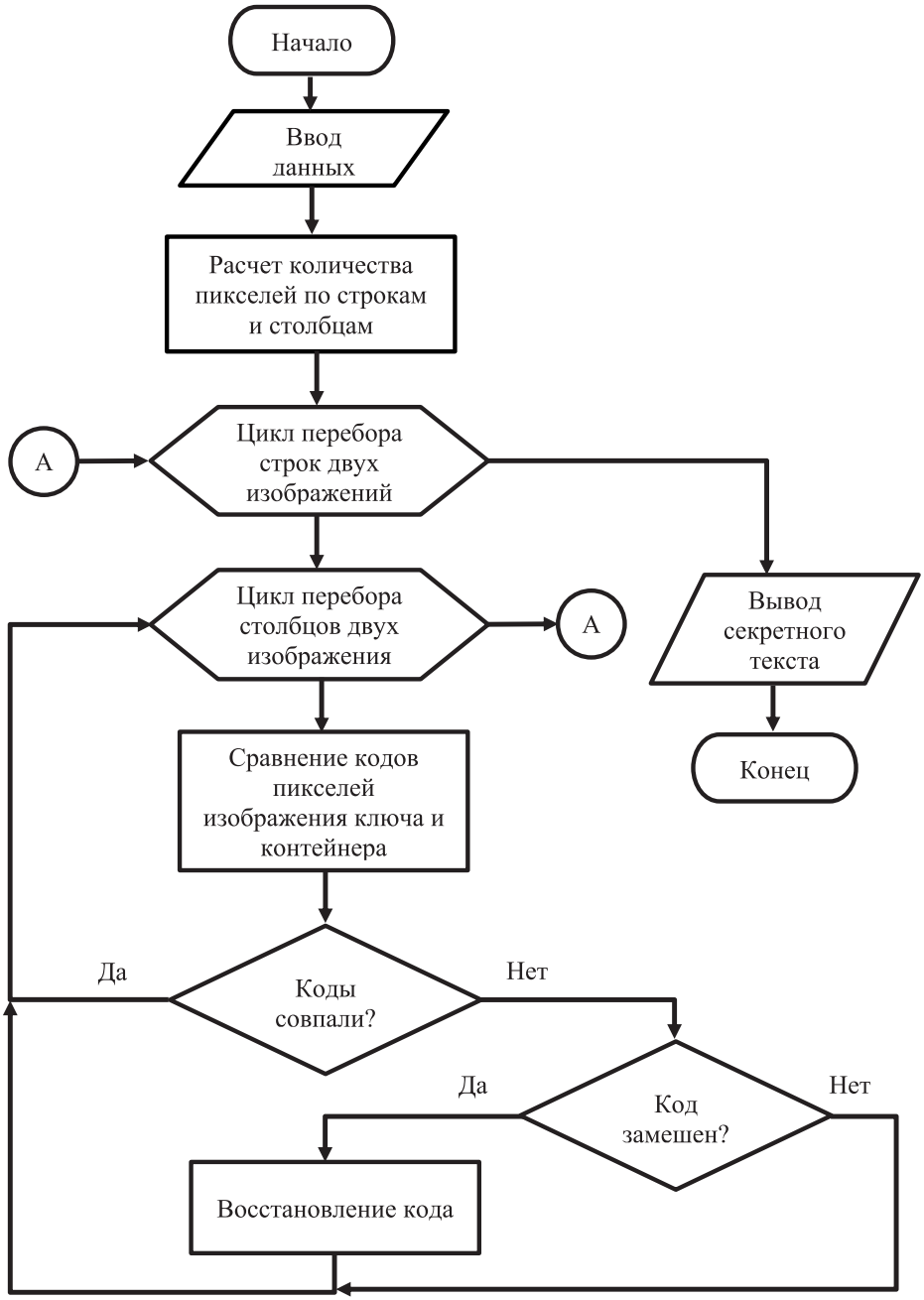

Рис. 3. Блок-схема алгоритма расшифровки секретного сообщения

В программе дешифрования производится сравнение байтов канала RED принятого графического файла с байтами изображения-ключа. В результате сравнения получаются байты сообщения, которые выдаются на экран. После запуска программы дешифрования появится диалоговое окно с переданным сообщением (рис. 4).

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

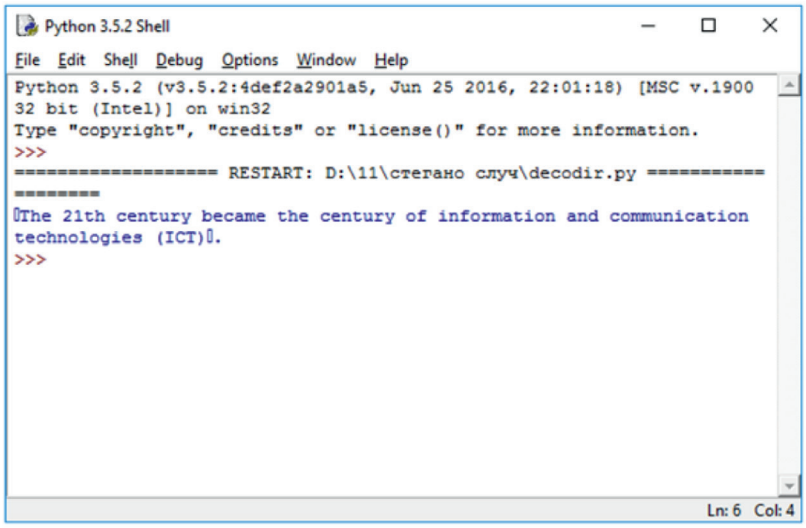

Рис. 4. Диалоговое окно с переданным сообщением

Пример изображения-ключа показан на рис. 5. Применение абстрактных картинок в качестве изображения-ключа значительно повышает надежность защиты конфиденциальной информации, так как в таких картинках присутствует случайное изменение значений пикселей. Кроме того, в каждую строку пикселей исходного изображения предварительно встраиваются случайные байты. В результате проведенных операций получается изображение-ключ, в котором присутствуют случайные байты. Это значительно затрудняет работу программы криптоанализа.

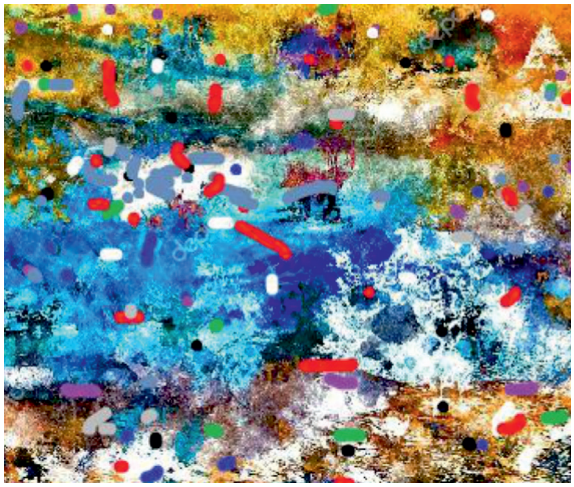

Рис. 5. Изображение-ключ

Выводы

Таким образом, с помощью предложенной схемы стеганографии и алгоритма встраивания байтов секретного сообщения в графический файл, значительно повышается объем встраиваемых данных за счет замены случайных байтов графического файла. Встраивание случайных байт в изображение-ключ позволяет значительно повысить защиту от обнаружения скрытой информации. Достоинством данной схемы стеганографии заключается в том, что для дешифрования используется изображение-ключ, в который предварительно встраиваются случайные байты. Кроме того, все биты пикселей изображения-контейнера используются для отображения оттенков цвета.

Также можно отметить, что разработанная схема стеганографии позволяет не только передавать секретную информацию, но и добавлять к изображению цифровые отпечатки или скрытые метки.

DOI: 10.37943/AITU.2020.15.23.009

Литература

1. Абазина Е.С., Ерунов А.А. Цифровая стеганография: состояние и перспективы // Системы управления, связи и безопасности. 2016. №2. С. 182-201. URL: http://sccs.intelgr.com/archive/2016-02/07-Abazina.pdf (дата обращения 26.05.2020).
2. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. – М.: Вузовская книга, 2009. – 220 с.
3. Рябко Б.Я., Фионов А.Н., Шокин Ю.И. Криптография и стеганография в информационных технологиях. – Новосибирск: Наука, 2015. – 239 с.
4. Вахаб А., Романенко Д.М. Методы цифровой стеганографии на основе модификации цветовых параметров изображения // Труды БГТУ, – 2018, серия 3, №1. С. 94-98.
5. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2009. – 265 с.
6. Боброва Е.М., Борисова С.Н. Защита информации с использованием методов стеганографии. Успехи современного естествознания. – 2011. – №7 – С. 80-81.
7. Цветков К.Ю., Федосеев В.Е., Абазина Е.С. Применение двумерных нелинейных сигналов Франка-Уолша, Франка-Крестенсона в методе формирования скрытых каналов с кодовым уплотнением в структуре сжимаемых видеоданных // Наукоемкие технологии в космических исследованиях Земли. – 2013. – №4. С. 32-40.
8. Абазина Е.С., Ерунов А.А. Результаты моделирования метода скрытой передачи информации с кодовым уплотнением в видеоданных // Системы управления, связи и безопасности. – 2015. – №2. С. 1-25. URL: http://journals.intelgr.com/sccs/ archive/ 2015-02/01-Abazina.pdf (дата обращения: 20.03.2016).
9. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: МК-Пресс, 2006. 288 с.
10. K. Priya. Steganography Techniques Used To Hide the Information. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 20, Issue 6, Ver. I (Nov – Dec 2018), PP 16-19, www.iosrjournals.org.

Reference

1. Abazina, E.S., & Erunov, A.A. (2016). Digital steganography: status and prospects. Control, communication and security systems, (2). 182-201. http://sccs.intelgr.com/archive/2016-02/07-Abazina.pdf.
2. Agranovsky, A.V. (2009). Steganography, digital watermarks and steganoanalysis. M.: University book, 220.
3. Ryabko, B.Ya., Fionov A.N., & Shokin Yu.I. (2015) Cryptography and steganography in information technology. Novosibirsk: Nauka, 239.
4. Wahab A., & Romanenko D.M. (2018). Methods of digital steganography based on the modification of color parameters of the image. Transactions of BSTU, (3)1, 94-98.
5. Gribunin V.G., Okov I.N., & Turintsev I.V. (2009). Digital steganography. M.: Solon-Press, 265.
6. Bobrova E.M., & Borisova S.N. (2011). Information security using steganography methods. The successes of modern science, 7, 80-81.
7. Tsvetkov K. Yu., Fedoseev V.E., & Abazina E.S. (2013). Application of two-dimensional nonlinear Frank-Walsh, Frank-Chrestenson signals in the method of forming covert channels with code compression in the structure of compressible video data. High-tech technologies in space exploration of the Earth, 4, 32-40.
8. Abazina E.S., & Erunov A.A. (2015). Simulation results of the method of covert information transmission with code compression in video data. Control, communication and security systems, 2, 1-25. http://journals.intelgr.com/sccs/ archive / 2015-02 / 01-Abazina.pdf (accessed March 20, 2016).
9. Konakhovich G.F., & Puzyrenko A.Yu. (2006) Computer steganography. Theory and practice. M.: MK-Press, 288.
10. K. Priya. (2018). Steganography Techniques Used to Hide the Information. IOSR Journal of Computer Engineering, 20(6), 16-19.