Original article
DOI: 10.14529/ctcr230302

APPLICATION OF CUTTER–JORDAN–BOSSEN METHOD FOR DATA HIDING IN THE IMAGE SPATIAL AREA

***I.E. Zhigalov**, ikgij@vlsu.ru, https://orcid.org/0000-0003-2664-4405*
***M.I. Ozerova**, ozerovam@rambler.ru, https://orcid.org/0000-0001-7658-010X*
***A.V. Evstigneev**, Grandvil1999@mail.ru*
Vladimir State University named after Alexander and Nicolay Stoletovs,
Vladimir, Russia

Abstract. The article deals with the main methods of digital steganography and presents a classification scheme. Special attention is paid to Cutter–Jordan–Bossen method for hiding data in the spatial area of the image. **Aim.** The study of digital shorthand methods, as well as the assessment of their applicability for hiding information in images. The main task is to analyze the Cutter–Jordan–Bossen method for hiding data in the spatial area of the image and evaluate its effectiveness under various conditions. **Materials and methods.** In this work, various methods of digital shorthand were used, including the Cutter–Jordan–Bossen method. Images of various types and quality, as well as various embedding parameters were used for testing. **Results.** As a result of the study, it was revealed that the Cutter–Jordan–Bossen method is effective for hiding information in the spatial area of the image. The dependence of the data extraction quality on the embedding parameters was tested, which showed that the optimal parameters depend on the type of image and its quality. The resistance of the information hidden by this method to distortion during compression was also tested. The test results showed that JPEG compression, even at low and high energy values, leads to the destruction of information hidden in the container. It was found that the best results are achieved when using the Cutter–Jordan–Bossen method with optimal embedding parameters, which allows you to save hidden information when compressing an image. **Conclusion.** In conclusion, we can say that the study of digital shorthand methods and their application to conceal information in images is an urgent and important topic. The Cutter–Jordan–Bossen method has shown good results in hiding information in the spatial area of the image, but for each specific case it is necessary to choose the optimal embedding parameters. It was found that JPEG compression can significantly affect the quality of information extraction, so it is necessary to take this factor into account when choosing a method for hiding data in an image. In general, the study of digital shorthand techniques and their application to conceal information in images can be useful for various fields, such as the protection of confidential information and digital watermark.

Keywords: steganography, information hiding, data hiding in the spatial area of the image, digital watermarks, confidentiality of information

For citation: Zhigalov I.E., Ozerova M.I., Evstigneev A.V. Application of Cutter–Jordan–Bossen method for data hiding in the image spatial area. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2023;23(3):16–23. DOI: 10.14529/ctcr230302

Научная статья
УДК 004.932.2:004.932.7
DOI: 10.14529/ctcr230302

ПРИМЕНЕНИЕ МЕТОДА КУТТЕРА – ДЖОРДАНА – БОССЕНА ДЛЯ СОКРЫТИЯ ДАННЫХ В ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ИЗОБРАЖЕНИЯ

***И.Е. Жигалов**, ikgij@vlsu.ru, https://orcid.org/0000-0003-2664-4405*
***М.И. Озерова**, ozerovam@rambler.ru, https://orcid.org/0000-0001-7658-010X*
***А.В. Евстигнеев**, Grandvil1999@mail.ru*
Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия

Аннотация. В статье рассмотрены основные методы цифровой стенографии и представлена схема классификации. Особое внимание уделено методу Куттера – Джордана – Боссена для сокрытия данных в пространственной области изображения. **Цель исследования:** изучение методов цифровой стенографии, а также оценка их применимости для сокрытия информации в изображениях. Основной задачей является анализ метода Куттера – Джордана – Боссена для сокрытия данных в пространственной области изображения и оценка его эффективности при различных условиях. **Материал и методы.** В данной работе были использованы различные методы цифровой стенографии, включая метод Куттера – Джордана – Боссена. Для тестирования были использованы изображения различного типа и качества, а также различные параметры встраивания. **Результаты.** В результате исследования было выявлено, что метод Куттера – Джордана – Боссена является эффективным для сокрытия информации в пространственной области изображения. Было проведено тестирование зависимости качества извлечения данных от параметров встраивания, которое показало, что оптимальные параметры зависят от типа изображения и его качества. Также была проверена стойкость информации, скрытой с помощью данного метода, к искажениям при сжатии. Результаты тестирования показали, что сжатие JPEG даже при низком уровне и высоком значении энергии приводит к уничтожению скрытой в контейнере информации. Было выявлено, что наилучшие результаты достигаются при использовании метода Куттера – Джордана – Боссена с оптимальными параметрами встраивания, что позволяет сохранить скрытую информацию при сжатии изображения. **Заключение.** В заключении можно сказать, что исследование методов цифровой стенографии и их применения для сокрытия информации в изображениях является актуальной и важной темой. Метод Куттера – Джордана – Боссена показал хорошие результаты при сокрытии информации в пространственной области изображения, но для каждого конкретного случая необходимо выбирать оптимальные параметры встраивания. Было выявлено, что сжатие JPEG может значительно повлиять на качество извлечения информации, поэтому необходимо учитывать этот фактор при выборе метода сокрытия данных в изображении. В целом, исследование методов цифровой стенографии и их применения для сокрытия информации в изображениях может быть полезным для различных областей, таких как защита конфиденциальной информации и цифровой водяной знак.

Ключевые слова: стеганография, сокрытие информации, сокрытие данных в пространственной области изображения, цифровые водяные знаки, конфиденциальность информации

Для цитирования: Zhigalov I.E., Ozerova M.I., Evstigneev A.V. Application of Cutter–Jordan–Bossen method for data hiding in the image spatial area // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2023. Т. 23, № 3. С. 16–23. DOI: 10.14529/ctcr230302

Introduction

Digital steganography is a science whose purpose is to conceal the very fact of the content of sensitive information in multimedia objects without attracting the attention of an observer [1].

For the time being, science is widely used by private individuals to transmit classified information through computer networks. There is also another common area – i.e., copy protection (copyright preservation) by embedding a digital watermark. Another area is to check the integrity of the document [2].

Digital steganography methods use the redundancy of a digital container, the choice of which is determined by the conditions of its sufficiency for embedding a hidden message so that the corresponding

changes are invisible neither to a person nor to special hardware and software, therefore images, audio and video are used as digital containers (Fig. 1).

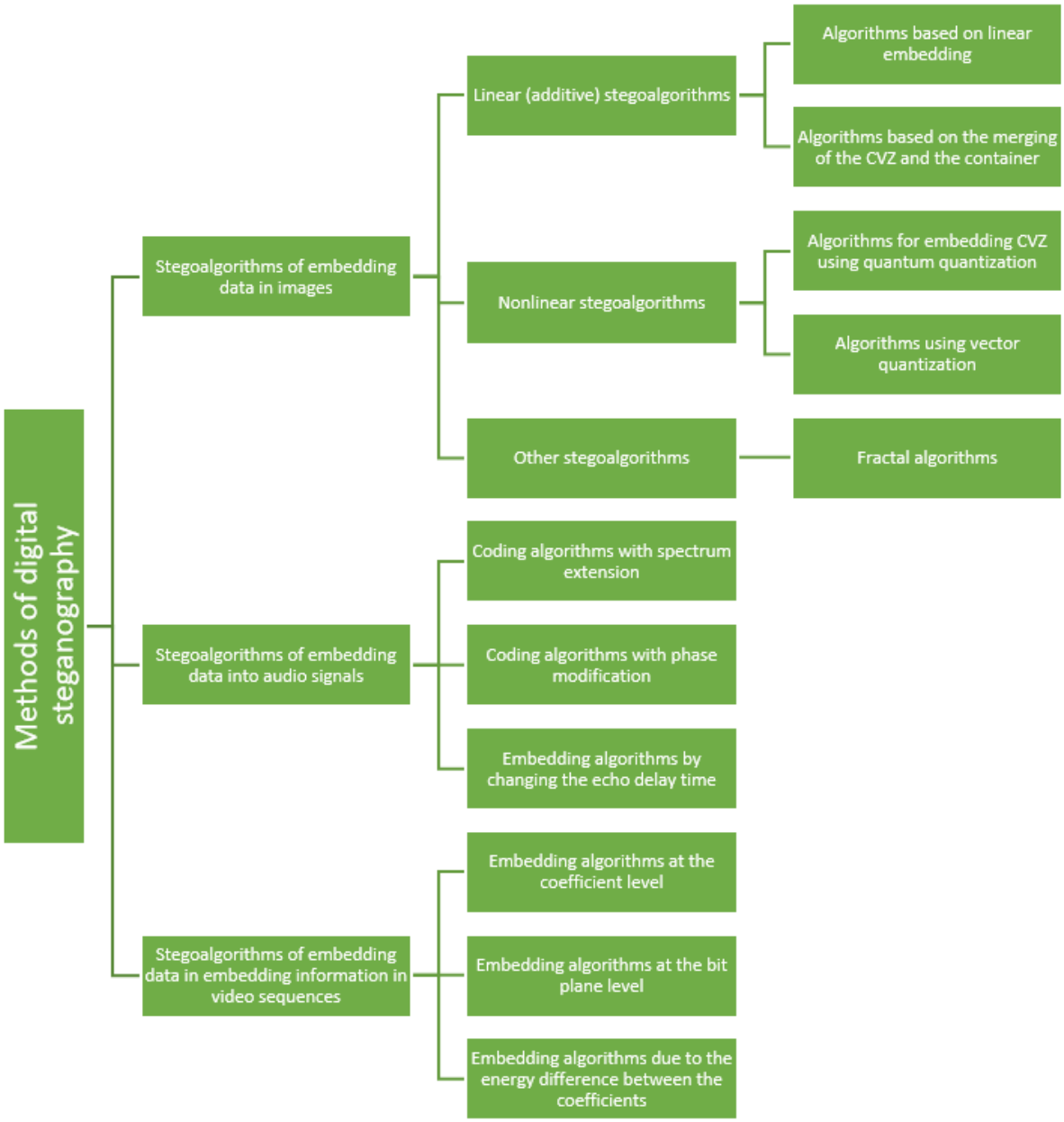

Fig. 1. Classification of digital steganography methods

According to the method of embedding information in the image, stegoalgorithms can be divided into linear (additive), nonlinear and others. In additive algorithms for the introduction of digital watermarks (DW), there assumed linear embedding of data, and their subsequent extraction in the decoder involves the use of correlation methods. In this case, the DW is either folded with the selected image, or "fused" into it. In nonlinear stegoalgorithms, scalar or vector quantization methods are used, when embedding information.

Hiding data in the spatial domain is embedding data into the original image using a computationally simple algorithm: the method of least significant bit (LSB); the method of block hiding; the method of replacing the palette; Cutter–Jordan–Bossen method. Hiding data in the frequency domain is the use of the same transformation as in compression: the method of replacing the values of the DCT coefficients (which is basic in JPEG); the method of hiding the values of the coefficients of Wavelet transform; using the features of file formats – hiding information in metadata and reserved file fields [3].

1. Kutter–Jordan–Bossen method

Kutter–Jordan–Bossen method, or the "cross method" is based on the property of the human visual system, for the eye to be least sensitive to the blue color.

The algorithm for embedding a message into an image: for embedding, you will need a container $C = \{R, G, B\}$ including information about the brightness of the red, green and blue colors of each pixel, m_i – i-th bit of the embedded message [4]. RC5 can be used as the secret key k, which sets a pseudo-random sequence for determining the coordinates of the pixel which is the object of embedding one bit of the message [5].

Among the stegoalgorithms, that cannot be directly attributed to linear or nonlinear algorithms using the ideas of fractal image encoding are now actively developing.

The implementation information will be a 1-bit message in a 1-pixel container [6]. When embedding, the brightness of the red and green colors remain unchanged, and the brightness of the blue changes according to the formula:

$$B'_{x,y} = \begin{cases} B_{x,y} + \upsilon \cdot L_{x,y}, & \text{when } m_i = 0; \\ B_{x,y} - \upsilon \cdot L_{x,y}, & \text{when } m_i = 1, \end{cases} \quad (1)$$

where $B_{x,y}$ is the brightness of the blue color in pixels with coordinates (x, y); v is a constant that determines the energy of the embedded bit, the larger it is, the better the resistance to interference, but the higher the visibility ($0 < v \le 1$); $L_{x,y}$ is the pixel brightness, determined by the formula:

$$L_{x,y} = 0.299 \cdot R_{x,y} + 0.587 \cdot G_{x,y} + 0.114 \cdot B_{x,y}. \quad (2)$$

Besides, to reduce errors during extraction, you can repeat the embedding of a bit of information t times, which will enable to reduce energy (v) of the embedded bit. The optimal value can be considered $v \approx 0.15$ and $t < 20$ [4].

In order to perform the extraction, the recipient will have to predict the blue brightness value of the modified pixel based on the neighboring ones. The "cross" algorithm (pixels located in the same row and in the same column) is 7 by 7 in size [7].

To predict the value, you will need: a secret key k, the number of repetitions t, the dimension of the "cross" δ – the number of pixels on all sides from the center ($\delta = 3$ with sizes 7 by 7, Fig. 2) [8].

The prediction of the initial brightness of the modified pixel is made according to the formula:

$$\hat{B}_{x,y} = \frac{\sum_{i=-\sigma}^{\sigma} B_{x+i,y} + \sum_{i=-\sigma}^{\sigma} B_{x,y+i} - 2 \cdot B_{x,y}}{4 \cdot \sigma}. \quad (3)$$

Next, to determine the bit of the embedded message, the difference between the current and predicted values of the brightness of the blue color of the pixel is calculated, the resulting differences are averaged [9]:

$$\overline{\delta} = \frac{\sum_{i=1}^{\tau} \left(B_{x,yi} - \hat{B}_{x,yi} \right)}{\tau}. \quad (4)$$

And if $\delta > 0$, then the embedded message bit $m_i = 1$, if $\delta \le 0$, then $m_i = 0$.

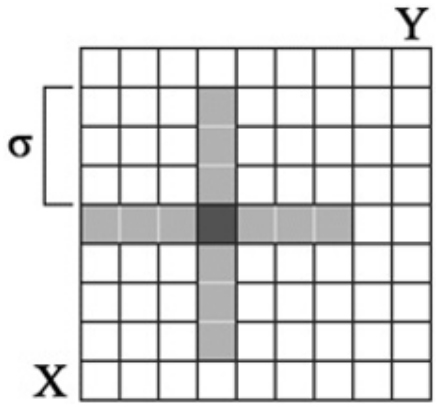

Fig. 2. Example of the evaluating "cross"

2. Testing

Embedding will occur in the image (Fig. 3a) having the size of 385×512 pixels and a bmp extension, message "Vladimir State University" with parameters: key $k = 375$, the number of rounds of calculation $r = 8$ (used for the RC5 cipher), the number of repetitions $r = 10$, energy $v = 0.2$; Fig. 3b being obtained as a result.

If you do not look closely at the image, then the modified pixels do not visually stand out, but with a detailed examination in the sky area at a special angle, you can notice the modified pixels. But if you look into the area of trees and grass, it will be quite difficult (almost impossible) to notice the modified pixels. I.e., we can conclude that the visual component of the stegosystem strongly depends on the origi-

nal container. When extracting with the same embedding parameters and $\delta = 3$, we get the original message "Vladimir State University".

a) **b)**

Fig. 3. Container: empty and filled

Let us conduct several tests of the dependence of the number of characters in the message on the percentage of correct extraction (Fig. 4).

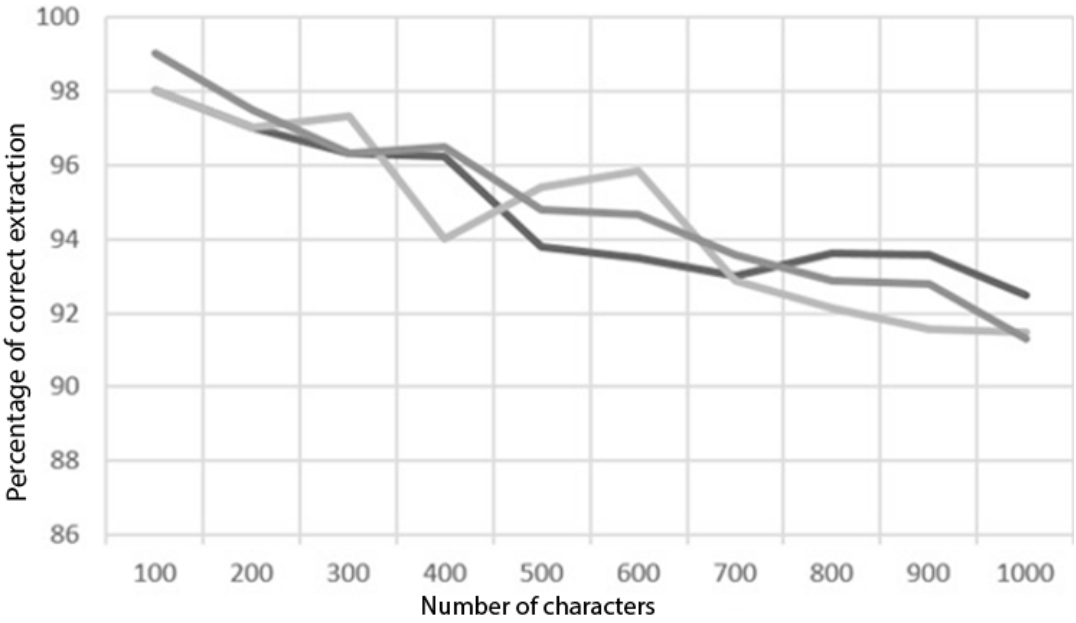

Fig. 4. Graph of the dependence of the number of characters on the percentage of correctness of the message extraction

We can make a positive conclusion that even with 1000 characters, the correctness of extracting a message from the image with a rather small resolution is above 90%. But it is obvious that a high number of characters degrades both the image quality and the extraction, since this will take up more space.

We will also conduct several tests when compressing a filled image into JPEG with the same parameters, and with the embedding energy equal to 0.9 (Fig. 5). Quality level 0 corresponds to maximum compression, and quality level 100 corresponds to minimum compression.

Embedded messages:

1 – @Ram:='{01^2-S#}!_S'

2 – QwErTy IoXaSdVgHjKlZx VbNqWxAh

3 – Lorem ipsum dolor sit amet, consectetuer

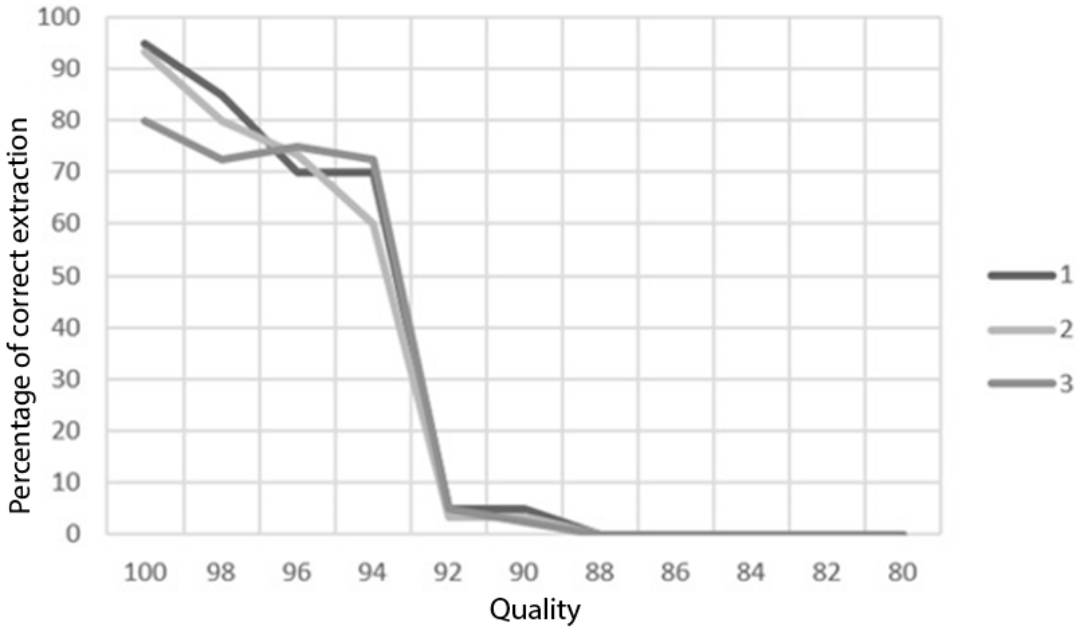

Fig. 5. Graph of the dependence of the quality level on the percentage of correctness of the message extraction

Thus, it can be concluded that JPEG compression, even at a low level and a high energy value, leads to the destruction of information hidden in the container, which is caused by the type of concealment method [10].

We will also conduct a test (Fig. 6) of the dependence of the embedding energy on the extraction quality with minimal compression of the filled image in JPEG with the same embedding parameters of the same three messages.

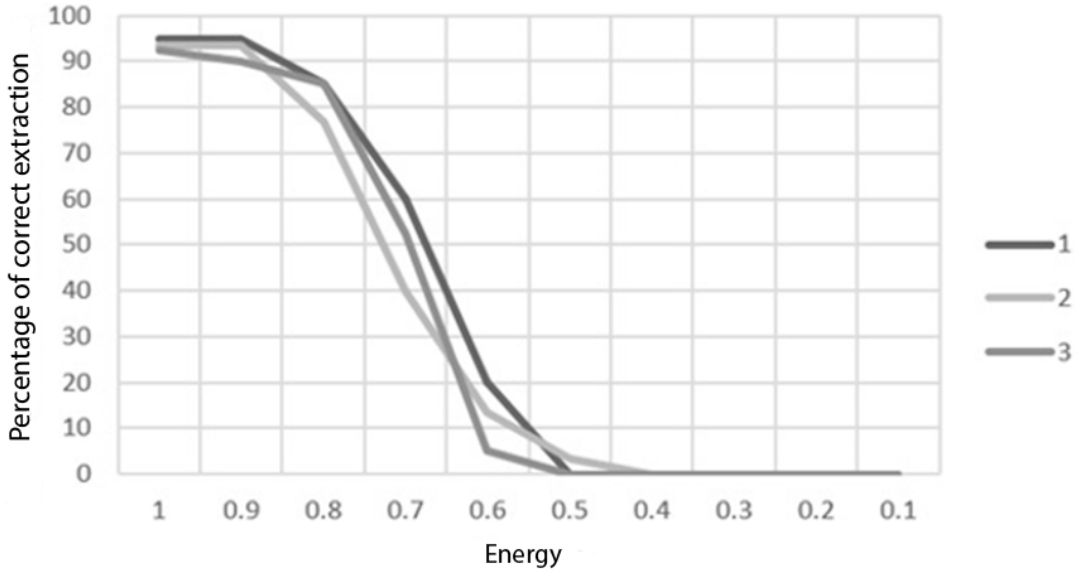

Fig. 6. Graph of energy dependence on the percentage of correctness of message extraction

Thus, this leads to the conclusion, that the optimal value of the embedding energy when compressed into JPEG lies in the range from 1 to 0.8. But such energy values will visually stand out and attract the attention of the attacker. So it is better to avoid compressing a container holding hidden information.

Conclusion

Today, due to the development of information technologies, the demand for personal information protection is growing. Digital steganography offers many new methods for this [11–13]. Digital ste-

ganography complements cryptography [14]. Their mutual integration will help to develop newer and more effective methods of ensuring security. It is also a promising and developing area of information protection, which still has problems with resistance to distortion (compression), as well as with the search for the optimal ratio of secrecy and the volume of secret data [15].

The authors express their gratitude to Associate Professor of the Department of "Foreign Languages of Professional Communication" Tatyana Ivanovna Koikova for her help and assistance in translating the article into English.

References

1. Chvarkova I.L., Tikhonenko S.G., Sadov V.S. *Povyshenie propusknoy sposobnosti i stoykosti steganograficheskikh sistem* [Increasing the throughput and durability of steganographic systems]. LAP LAMBERT Academic Publishing; 2013. 136 p. (In Russ.)

2. Ryabko B.Ya., Fionov A.N. *Osnovy sovremennoy kriptografii i steganografii* [Fundamentals of modern cryptography and steganography]. 2nd ed. Moscow: Goryachaya liniya – Telekom; 2013. 232 p. (In Russ.)

3. Korzhik V.I., Nebaeva K.A., Gerling E.Yu. *Tsifrovaya steganografiya* [Digital steganography]. Moscow: KnoRus; 2016. 225 p. (In Russ.)

4. Agranovskiy A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A. *Steganografiya, tsifrovye vodyanye znaki i stegoanaliz: monogr.* [Steganography, digital watermarks and steganalysis: monograph]. Moscow: Vuzovskaya kniga; 2009. 220 p. (In Russ.)

5. Zavadskaya T.V., Krakhmal M.V. The study of steganography methods during embedding hidden information in the frequency region of an image // Informatics and Cybernetics. 2020;1(19):18–26. (In Russ.)

6. Konakhovich G.F., Puzyrenko A.Yu. *Komp'yuternaya steganografiya. Teoriya i praktika* [Computer steganography. Theory and practice]. Kyiv: MK-Press; 2006. 288 p. (In Russ.)

7. Gubenko N.Ye., Sipakov D.S. Analysis of the features of digital steganography to protect information transmitted via open channels. Informatics and Cybernetics. 2015;2:28–38. (In Russ.)

8. Nazarova V.I. Stegosystem of the digital watermarks. *Information security of the regions*. 2010; 2(7):111–114. (In Russ.)

9. Zashcholkin K.V., Ivaschenko A.I., Ivanova E.N. Improvement of the Kutter–Jordan–Bossen method of information hiding. In: *MNPK "Modern information and electronic technologies"*. Odessa; 2013. P. 214–216. (In Russ.)

10. Bykov S.F. [JPEG compression algorithm from the position of computer steganography]. *Information Protection. Confidant*. 2000;3:26–31. (In Russ.)

11. Gribunin V.G., Okov I.N., Turintsev I.V. *Tsifrovaya steganografiya* [Digital steganography]. Moscow: SOLON-Press; 2009. 265 p. (In Russ.)

12. Cox I.J., Miller M.L., Bloom J.A., Fridrich J., Kalker T. Digital watermarking and steganography. San Francisco: Morgan Kaufmann Publishing; 2008. 624 p.

13. Dryuchenko M.A., Sirota A.A. Image stegoanalysis using deep neural networks and heteroassociative integral transformations. *Applied discrete mathematics*. 2022;55:35–58. (In Russ.) DOI: 10.17223/20710410/55/3

14. Vasina T.S. Review of modern steganography algorithms. *Science and education*. 2012;04:1–8. (In Russ.)

15. Okatov A.V. *Metody tsifrovoy steganografii* [Methods of digital steganography]. St. Petersburg: SUAI; 2016. 64 p. (In Russ.)

Список литературы

1. Чваркова И.Л., Тихоненко С.Г., Садов В.С. Повышение пропускной способности и стойкости стеганографических систем. LAP LAMBERT Academic Publishing, 2013. 136 с.

2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. 2-е изд. М.: Горячая линия – Телеком, 2013. 232 с.

3. Коржик В.И., Небаева К.А., Герлинг Е.Ю. Цифровая стеганография. М.: КноРус, 2016. 225 с.

4. Стеганография, цифровые водяные знаки и стегоанализ: моногр. / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. М.: Вузовская книга, 2009. 220 с.

5. Завадская Т.В., Крахмаль М.В. Исследование методов стеганографии при встраивании скрытой информации в частотную область изображения // Информатика и кибернетика. 2020. № 1 (19). С. 18–26.

6. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. 288 с.

7. Губенко Н.Е., Сипаков Д.С. Анализ особенностей методов цифровой стеганографии для защиты информации, передаваемой по открытым каналам // Информатика и кибернетика. 2015. № 2. С. 28–38.

8. Назарова В.И. Стегосистемы цифровых водяных знаков // Информационная безопасность регионов. 2010. № 2 (7). С. 111–114.

9. Защелкин К.В., Иващенко А.И., Иванова Е.Н. Усовершенствование метода скрытия данных Куттера – Джордана – Боссена // МНПК «Современные информационные и электронные технологии». Одесса, 2013. С. 214–216.

10. Быков С.Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии // Защита информации. Конфидент. 2000. № 3. С. 26–31.

11. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-Пресс, 2009. 265 с.

12. Digital watermarking and steganography / I.J. Cox, M.L. Miller, J.A. Bloom et al. San Francisco: Morgan Kaufmann Publishing, 2008. 624 p.

13. Дрюченко М.А., Сирота А.А. Стегоанализ цифровых изображений с использованием глубоких нейронных сетей и гетероассоциативных интегральных преобразований // Прикладная дискретная математика. 2022. № 55. С. 35–58. DOI: 10.17223/20710410/55/3

14. Васина Т.С. Обзор современных алгоритмов стеганографии // Наука и образование. 2012. № 04. С. 1–8.

15. Окатов А.В. Методы цифровой стеганографии. СПб.: ГУАП, 2016. 64 с.

Information about the authors

Ilya E. Zhigalov, Dr. Sci. (Eng.), Prof., Head of the Department of Information Systems and Software Engineering, Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia; ikgij@vlsu.ru.

Marina I. Ozerova, Cand. Sci. (Eng.), Ass. Prof. of the Department of Information Systems and Software Engineering, Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia; ozerovam@rambler.ru.

Andrey V. Evstigneev, master's degree student of the Department of Information Systems and Software Engineering, Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia; Grandvil1999@mail.ru.

Информация об авторах

Жигалов Илья Евгеньевич, д-р техн. наук, проф., заведующий кафедрой информационных систем и программной инженерии, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия; ikgij@vlsu.ru.

Озерова Марина Игоревна, канд. техн. наук, доц. кафедры информационных систем и программной инженерии, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия; ozerovam@rambler.ru.

Евстигнеев Андрей Васильевич, магистрант кафедры информационных систем и программной инженерии, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия; Grandvil1999@mail.ru.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

The article was submitted 18.03.2023
Статья поступила в редакцию 18.03.2023