INFORMATION SECURITY

DOI 10.20535/2411-1031.2020.8.2.222589
UDC 681.322:621.391

STEPAN BILAN,
VIACHESLAV RIABTSEV,
ANDRIY DANILTSO

VOLUME INCREASING OF SECRET MESSAGE IN A FIXED GRAPHICAL STEGO CONTAINER BASED ON INTELLIGENT IMAGE ANALYSIS

The paper considers methods of edge pixel selection based on Roberts, Previtt, and Sobel operators, as well as technologies of cellular automata to increase the volume of the implemented secret message. Based on the methods used, templates with selected pixels were formed, into the codes of which secret message bits were embedded. The templates were formed using threshold additional processing, which allowed to select the optimal threshold for the selection of the corresponding pixels of the image of the container. Thresholds ranging from 100 to 300 were selected for the Roberts operator, and thresholds ranging from 1,000,000 to 15,000,000 were selected for the Previtt and Sobel operator. To select pixels based on cell technology, four cell neighborhood shapes were used for binary and color imaging. Experimental studies were performed for all methods of pixel selection, which made it possible to determine the optimal numerical threshold, as well as the number of lower bits of each selected pixel to implement the bits of the secret message. It has been experimentally established that for all methods, except for the two lower bits of the code of each pixel, the bits of the secret message are also embedded in the four lower bits of each byte of code of the selected pixel, which significantly increases the volume of the embedded message. When using two lower bits of all pixels and four lower bits of selected pixels for many templates, no change in the visual images of the containers was observed. Using the fifth lower bit in each byte of the selected pixel code to enter the secret bit results in significant distortion of the visual picture. The experiments were performed for different brightness thresholds during binarization. In total, six additional secret bits were added to the code of each selected pixel. For the efficiency of the experiments, bit sequences containing only one zero, one unit, and randomly generated bit sequences were introduced into the containers.

Keywords: steganography, container, image, edge detection, cellular automata, secret message.

Problem statement. The modern growth of information technology has provoked a great need for methods and means of protecting information. The last few decades have been characterized by the widespread adoption of digital technologies, which are accompanied by methods of information protection and resistance to unauthorized interference. Each time, the methods of hacking security systems are improved, which leads to the need to create new methods and means of protection. Among the existing methods of protecting information, cryptography and steganography are highlighted [1] - [6]. These methods are used when transmitting messages on digital transmission channels. Recently, steganographic information security methods are becoming more and more popular. The essence of steganographic information protection methods is to hide secret information in other information. Both information is presented in electronic form. The most often secret information is text, and as portable information can be used: text, image, sound, etc. Information in which classified information is embedded is presented in a file of the appropriate format. Such files are called containers.

The containers can be of different sizes. Also, containers can be chosen arbitrarily, or they can be fixed. If the container is chosen arbitrarily, then the enemy may suspect that it contains secret information. To distract the enemy's suspicion, it is better to use a container of a fixed volume and

known to everyone. As a rule, a container known to the enemy reduces the suspicion. However, the known container has a fixed volume and structure, which limits the volume of the embedded secret message.

This work solves the problem of increasing the volume of a secret message being embedded into a container of a fixed length, represented in a graphic format based on intelligent image analysis. Images are used as containers. Research is being carried out aimed at finding the pixels of the container image, the distortion of the color and brightness characteristics of which does not lead to distortion of the general visual characteristics. To solve this problem, methods of edge detection in the image are used based on the Roberts, Prewitt, and Sobel operators, as well as cellular automata (CA) technologies.

Analysis of recent researches and publications. Methods of steganographic information protection are described in various information sources [1] - [6]. They use containers of various formats. Steganographic information protection methods are constantly being improved. At the same time, they are aimed at solving the main task, which is to increase the volume of embedded information without significant changes in the container, perceived by the human sense organs.

For containers represented by graphic formats, the main characteristics are: visual picture and the amount of information is embedded. These parameters are mutually influencing. Therefore, the methods are developed taking into account the reduction of this effect. The most famous steganographic method is the LSB method [2] - [7]. It implements the embedding of the secret message bits in the least significant bits of the codes of each pixel of the image. At the same time, there are no significant visual changes. The number of embedded secret bits is determined by the number of image pixels. To increase the volume of an embedded message in a container of a fixed length, methods of searching for pixels in the image are used, changing the brightness characteristics of which does not lead to a change in the visual characteristics of the image [5], [8] - [10]. In this direction, in these works, studies were carried out that determine the maximum number of embedded pixels. In this case, various technologies are used, which are based on technologies for analyzing neighboring pixels by each pixel. In [8], a method of embedding the bits of a secret message into pixels, which are allocated using the Roberts operator [11]. However, the method can lead to distortions of the visual picture, since the Roberts operator assumes the selection of two adjacent pixels. Also, the Roberts operator uses a 2×2 pattern, which, although it produces thin edges, produces fewer pixels than the 3×3 operators do. Another approach is to embed pixels in the original image, which are perceived as image noise. [9], [10]. Research based on these methods allowed to determine the optimal percentage of noise pixels. However, little research has been done towards finding the locations of noise pixels.

In this work, research is carried out in the direction of finding methods for separating pixels in the container image to increase the number of embedded bits of a secret message.

The purpose of the article is an increase in the volume of a secret message being embedded into a container of a fixed size, represented by a graphical file.

The main material research. The first frequently used operator for extracting edge pixels in an image is the Roberts operator [11]. The Roberts operator is implemented based on the following formula

$$Q = \sqrt{Q_1^2 + Q_2^2} = \sqrt{\left(\sqrt{y_{ij}} - \sqrt{y_{i+1,\,j+1}}\right)^2 + \left(\sqrt{y_{i+1,\,j}} - \sqrt{y_{i,\,j+1}}\right)^2}, \quad (1)$$

where y_{ij} – pixel code with coordinates i and j.

Convolution of images with two arrays of coefficients is used.

$$\begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & +1 \\ -1 & 0 \end{bmatrix}.$$

In [8], the Roberts operator is used only for images presented in grayscale and, based on the selected pixels, a standard is formed, which indicates the pixels for embedding the bits of a secret message. Thereafter, an experimentally determined threshold value is set. The higher the threshold

value, the fewer pixels are selected. It should be borne in mind that many visual characteristics are distorted during the threshold conversion of a color image to gray. In this work, the Roberts operator is applied directly to color images.

Also, the work uses the Prewitt operator, which is used to detect edges in the image [12], [13]. To implement the Prewitt operator, the following formula is used.

$$M = \sqrt{\left(M_x(x,y)\right)^2 + \left(M_y(x,y)\right)^2} \tag{2}$$

The components of this formula are calculated using 3×3 templates, in which the coefficients are different from others

$$\begin{bmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 1 & 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{bmatrix}$$

Another operator that uses the 3×3 matrix pattern is the Sobel operator [12], which is implemented by the following coefficients

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

The practical application of such operators in Fig. 1 is shown.

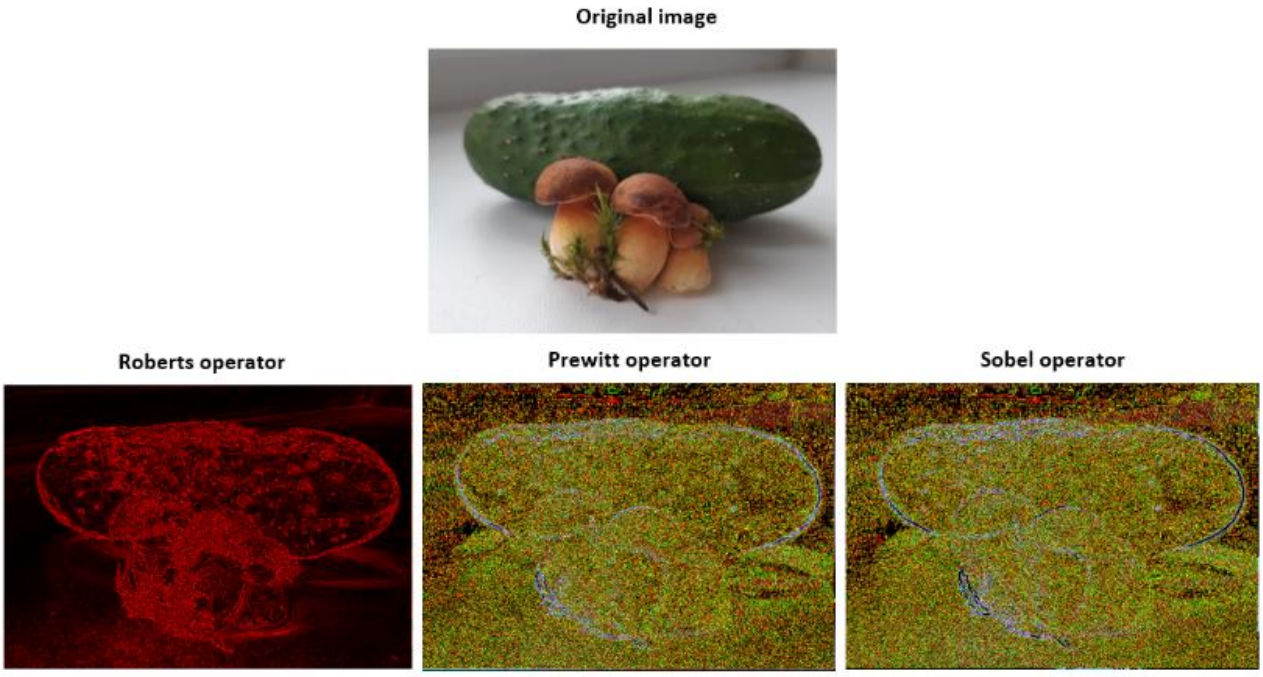

Figure 1 – Application of the Roberts, Prewitt, and Sobel operators

The figure shows that using a 3×3 template increases the number of selected pixels in the image. However, a sufficiently large number of pixels are increased, which leads to significant visual distortions when introducing secret bits. Therefore, the number of bits is reduced by using the selected threshold according to the formula.

$$M_{x,y}(t+1) = \begin{cases} M_{x,y}(t), \textit{ if } M_{x,y}(t) > \mathrm{R}, \\ 0, \textit{ in other case}, \end{cases} \tag{3}$$

where R – selected threshold.

Numeric arrays were formed as shown in the works [8] - [10]. For the Roberts operator, the thresholds were chosen in the range from 100 to 300, and for the Prewitt and Sobel operator, the thresholds were chosen in the range from 1,000,000 to 15,000,000. Images obtained after thresholding for all three operators in Fig. 2 are shown.

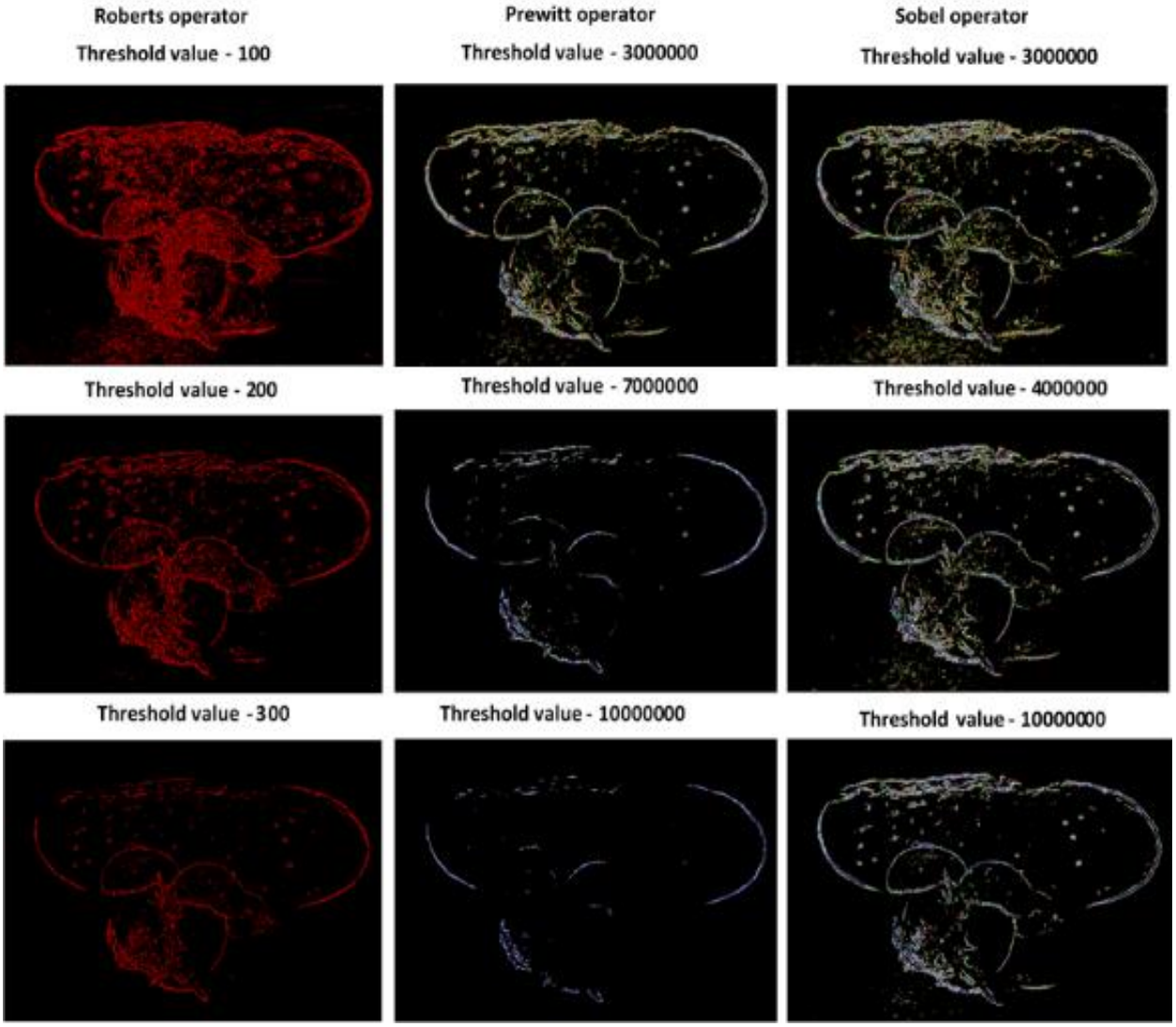

Figure 2 – Images after applying the Roberts, Prewitt, and Sobel operators and after thresholding

The resulting images (see Fig. 2) are used as templates for embedding secret bits into the codes of the corresponding pixels of the original image. To embed the bits of a secret message into the allocated bits, various algorithms for enumerating them are used, and a different number of least significant bits is selected depending on the threshold value. Cellular automata are also used to select image pixels whose code change does not significantly change the visual picture of the image [15]. Extraction of edges in binary and color images is described in the paper [16]. Various neighborhood structures are used, both popular (von Neumann and Moore neighborhoods) and little-studied. The structures of such neighborhoods in Fig. 3 are shown.

The results of using such neighborhoods to select edge pixels on Fig. 4 are shown. Many different binarization thresholds were used, and only one in Fig. 4 is presented. The results of using only one threshold for the binarization of all neighborhoods are presented. Figure 4 shows that for different shapes of the neighborhoods, different contour shapes are distinguished and a different number of selected pixels is formed. This approach requires preliminary binarization of the color image. For this, various numerical thresholds are used.

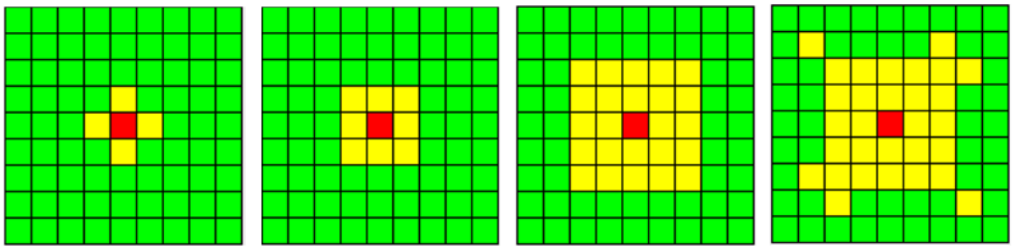

Figure 3 – Neighborhood structures used in the experiment

Also in [16], the selection of edge pixels for color and gray images is described. Pixels are selected according to the following formula.

$$G(t+1)=\begin{cases} G(t), \ if \ \dfrac{\sum_{i=1}^{k} I_i(t)}{k} < G(t) > B(t), \\ 0, \ in \ other \ case, \end{cases} \quad (4)$$

where $G(t)$ – pixel intensity value at time t (before thresholding);

$B(t)$ – the value of the background intensity at time t;

$I_i(t)$ – the intensity value of the i th cell belonging to the neighborhood of the cell $G(t)$;

k – the number of cells that make up the neighborhood for a cell $G(t)$.

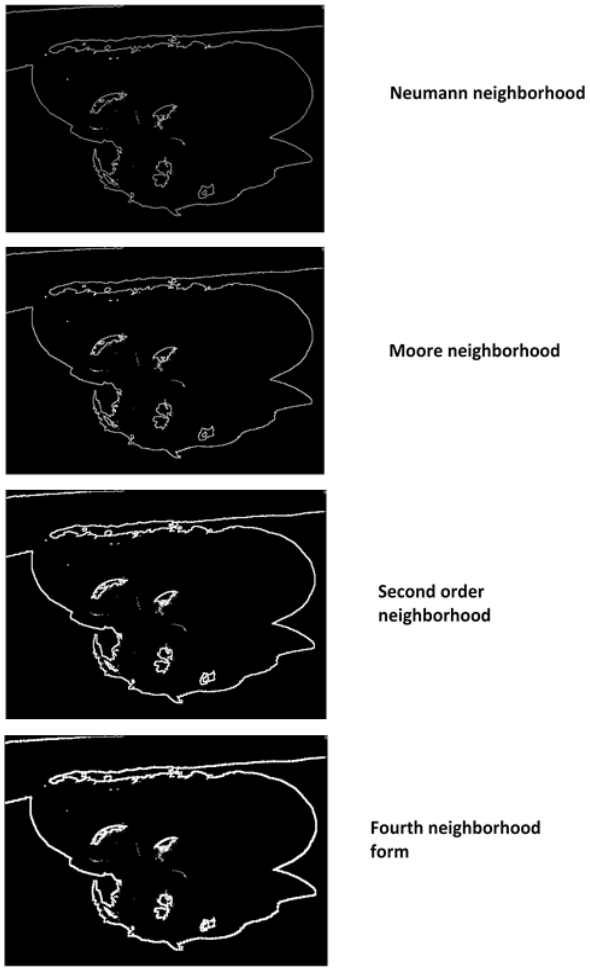

Figure 4 – The results of extracting edge pixels after using the spacecraft with the neighborhoods shown in Fig. 3

We also used a formula that takes into account the average of the entire image

$$G(t+1)=\begin{cases} G(t), \ if \ \dfrac{\sum_{i=1}^{D} I_i(t)}{k} < G(t), \\ 0, \ in \ other \ case, \end{cases} \quad (5)$$

where D – the number of all pixels in the image.

The images of selected pixels for luminance thresholds corresponding to 30%, 50%, and 100% on Fig. 5 are shown.

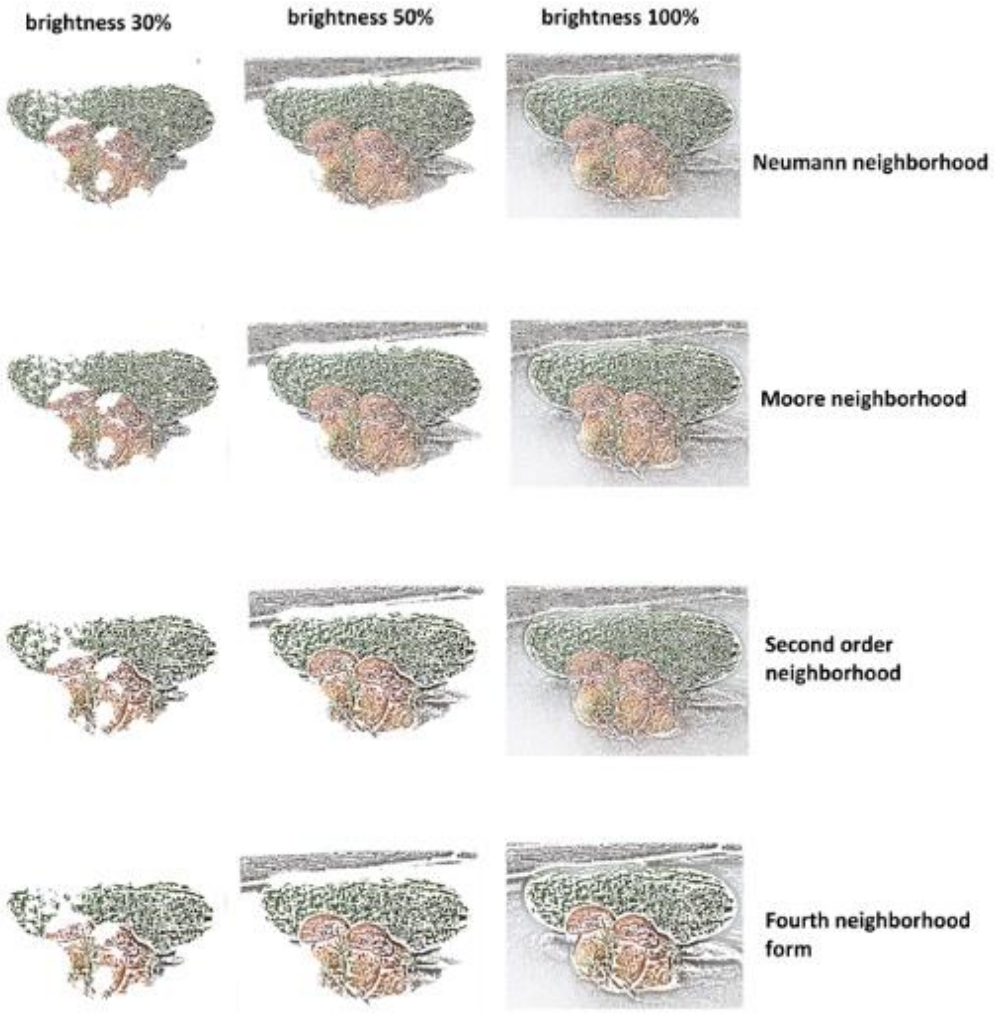

Figure 5 – Edge detection results of the described method and for brightness thresholds of 30%, 50%, and 100%

However, this method produces a fairly large number of pixels, which can lead to significant visual distortion. Therefore, to reduce the number of selected pixels, thresholding is used, as described earlier. For this, pixel codes are studied for different brightness thresholds. Fig. 6 shows the results of applying thresholding for the images obtained in Fig. 5. To experiment, we used image templates with selected pixels obtained by using all the previously considered operators and CA technologies. Image templates with selected pixels were generated for different numerical thresholds and different shapes of the neighborhoods. Secret messages were generated, presented in the form of bit sequences, and containing all zeros, all ones, and bit sequences generated randomly. These bit sequences were presented in the form of a text document, which, using a special program, in the selected bits of the container were embedded.

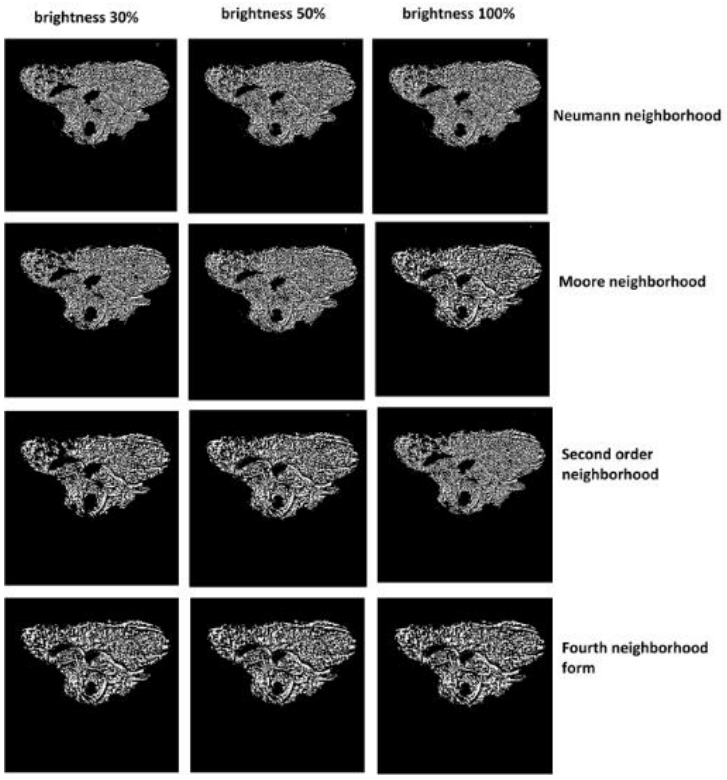

Figure 6 – The results of applying thresholding for the images obtained in Fig. 5

The program injected the bits of the secret message by bit layers into the selected bits of the pixel code. First, the number of low-order bits of codes of all pixels of the container image was determined, the change of which did not distort the visual picture. Each pixel code was represented in binary and decimal code. The binary code consists of 24 bits (3 bytes). The least significant byte encodes the red color and its shades, the middle byte encodes the green color and its shades, and the high byte encodes the blue color and its shades. An example of a code image with embedded two zeros and ones on Fig. 7 is shown.

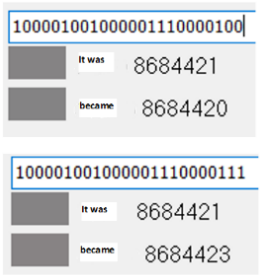

Figure 7 – Example of codes with embedded bits (00, 11) in the least significant bits

The visual picture shows that there are no significant visual differences. The images participating in the experiment have a dimension of 500 × 349. 349000 bits of a secret message are preliminarily embedded in such an image using this technique. Studies have shown that images of container with embedded bits in the least significant two bits of each pixel in the original image do not distort the visual picture. After introducing the secret bits into the two least significant bits of the codes of all pixels, the generated templates were selected for different thresholds. Templates are images of selected pixels on a black background. Background pixels are zero-coded and selected pixels are coded greater than 0.

With the help of the program, the secret bits were embedded in the third and fourth least significant bits of each byte of the codes of the selected pixels. When using the two least significant

bits of all pixels and the four least significant bits of the selected pixels, for many templates, no change in the visual picture of containers was observed. Thus, six additional secret bits were introduced into the code of each selected pixel. For almost all edge pixel extraction technologies used, the use of the fifth least significant bit for introducing the secret bit leads to significant distortions of the visual picture.

Images of containers with embedded secret bits in the four least significant bits of each byte of the codes of the allocated pixels on Fig. 8 are shown, and images of containers with real distortions on Fig. 9 are shown. Figure 8 shows that almost all the considered methods of extracting edge pixels make it possible to embed secret bits in the four least significant bits of each byte of the code of the selected pixels. This significantly increases the volume of the embedded secret message.

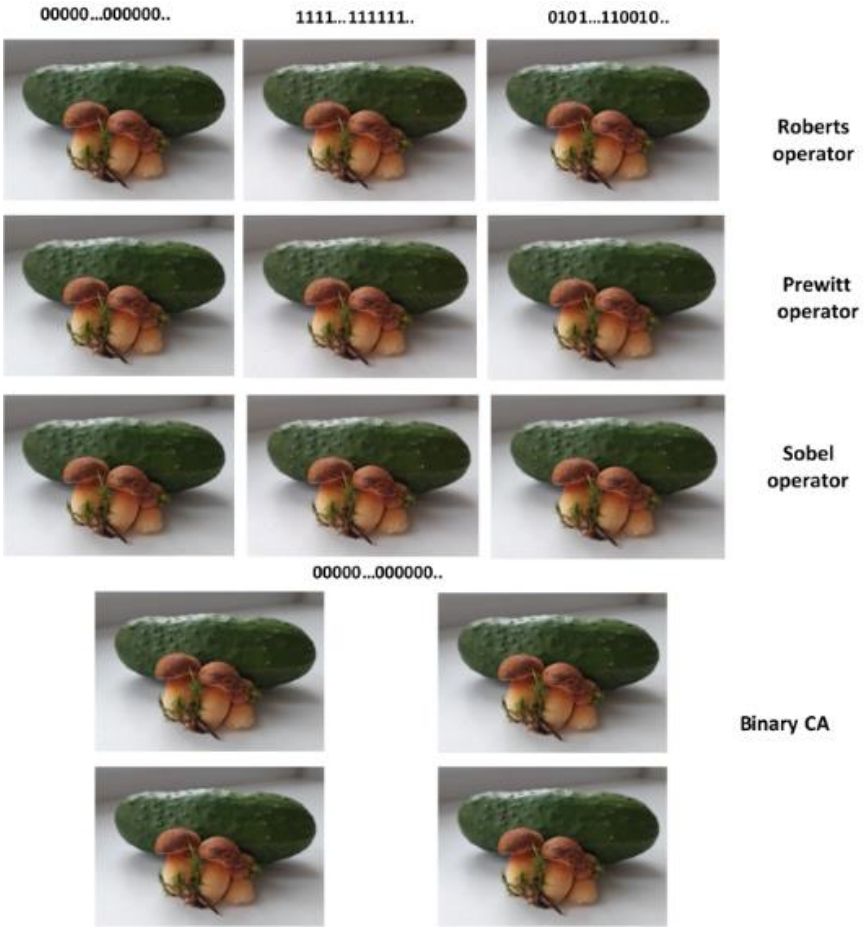

Figure 8 – Examples of images of containers with embedded secret bits in the four least significant bits of each byte of codes of allocated pixels

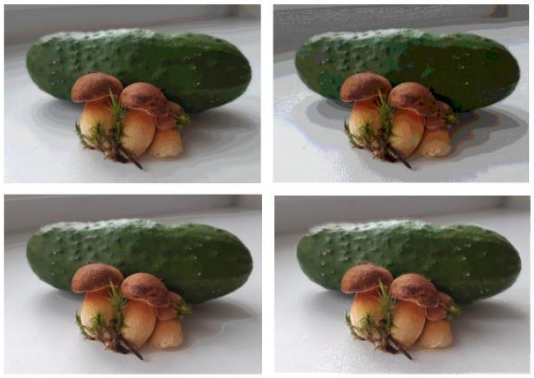

Figure 9 – Examples of images of containers with visual distortion

Conclusions. The paper analyzes the existing methods for selecting the edge pixels of an image to find pixels of container images, changing the properties of which (changing the code) does not lead to distortions of the visual picture of the image. It was found that the use of the Roberts, Prewitt and Sobel operators, as well as cellular automata technologies, made it possible to select pixels in the image of containers that do not change the visual picture when the four least significant bits of each byte of the code of the selected pixels are changed. For each used pixel extraction method, the optimal numerical threshold was experimentally established. Analysis of these methods for extracting edge pixels made it possible to target researchers to further search for new approaches to determining pixels that have little effect on the overall visual picture of the container image.

Further research. The authors investigated several methods for extracting edge pixels. We plan in the future to focus research on the selection of other pixels in the image, as well as to search for pixels with such properties, into which it is possible to embed message fragments of certain properties.

REFERENCE

[1] H. Sajedi, *Recent Advances in Steganography*. London: November 07, 2012, doi: 10.5772/2501.

[2] G. Kipper. *Investigator's Guide to Steganography*. Boca Raton: Auerbach Publications, 2003.

[3] E. Cole. *Hiding in Plain Sight: Steganography and the Art of Covert Communication*. Hoboken: Wiley, 2003.

[4] A. Yahya, *Steganography Techniques for Digital Images*. Cham: Springer, 2019, doi: 10.1007/978-3-319-78597-4.

[5] M. Bilan, and A. Bilan, "Research of Methods of Steganographic Protection of Audio Information Based on Video Containers". *Handbook of Research on Intelligent Data Processing and Information Security Systems. Edited by Bilan, S. M., & Al-Zoubi, S. I.* Hershey: IGI Global, pp. 79-94, 2019.

[6] M. Saracevic, A. Selimi, and S. Pepić, "Implementation of Encryption and Data Hiding in E-Health Application" *Handbook of Research on Intelligent Data Processing and Information Security Systems.* Edited by Bilan, S. M., & Al-Zoubi, S. I. Hershey: IGI Global, pp. 25-42, 2019.

[7] G. Blokdyk, *Steganography*. 5STARCooks, 2019.

[8] N. Albdour, and N. Zanoon, "A Steganographic Method Based on Roberts Operator", *Jordan Journal of Electrical Engineering*, vol. 6, iss. 3, pp. 265-273, 2020.

[9] N. Albdour, "Selection image points method for steganography protection of information", *WSEAS Transactions on Signal Processing*, vol. 14, pp. 151-159, 2018.

[10] S. Bilan, and O. Kolochun, "Method of steganographic concealing information based on modified containers", *Collection of scientific work of the State economic and technological university of transport*, vol. 25, pp. 107-113, 2014.

[11] L. Roberts, "Machine Perception of Three-Dimensional Solids", *Optical and ElectroOptical Information Processing*. Cambridge: MIT Press, pp. 159-197, 1965.

[12] J. M. S. Prewitt, "Object Enhancement and Extraction", *Picture processing and Psychopictorics*. Academic Press, 1970.

[13] J. M. S. Prewitt, and M. L. Mendelsohn, "The Analysis of Cell Images", *Ann. N.Y. Acad. Sci.*, vol. 128, pp. 1035-1053, 1966, doi: 10.1111/j.1749-6632.1965.tb11715.x.

[14] I. E. Sobel, Camera Models and Machine Perception, PhD Thesis, Stanford Univ, 1970.

[15] S. Bilan, *Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities*. Hershey: IGI Global, 2017.

[16] S. Bilan. "Models and hardware implementation of methods of Pre-processing Images based on the Cellular Automata", *Advances in Image and Video Processing*, vol. 2, iss. 5, pp. 76-90, 2014, doi: 10.14738/aivp.25.561.

The article was received 03.09.2020.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] H. Sajedi, *Recent Advances in Steganography*. London: November 07, 2012, doi: 10.5772/2501.

[2] G. Kipper. *Investigator's Guide to Steganography*. Boca Raton: Auerbach Publications, 2003.

[3] E. Cole. *Hiding in Plain Sight: Steganography and the Art of Covert Communication*. Hoboken: Wiley, 2003.

[4] A. Yahya, *Steganography Techniques for Digital Images*. Cham: Springer, 2019, doi: 10.1007/978-3-319-78597-4.

[5] M. Bilan, and A. Bilan, "Research of Methods of Steganographic Protection of Audio Information Based on Video Containers". *Handbook of Research on Intelligent Data Processing and Information Security Systems. Edited by Bilan, S. M., & Al-Zoubi, S. I.* Hershey: IGI Global, pp. 79-94, 2019.

[6] M. Saracevic, A. Selimi, and S. Pepić, "Implementation of Encryption and Data Hiding in E-Health Application" *Handbook of Research on Intelligent Data Processing and Information Security Systems.* Edited by Bilan, S. M., & Al-Zoubi, S. I. Hershey: IGI Global, pp. 25-42, 2019.

[7] G. Blokdyk, *Steganography*. 5STARCooks, 2019.

[8] N. Albdour, and N. Zanoon, "A Steganographic Method Based on Roberts Operator", *Jordan Journal of Electrical Engineering*, vol. 6, iss. 3, pp. 265-273, 2020.

[9] N. Albdour, "Selection image points method for steganography protection of information", *WSEAS Transactions on Signal Processing*, vol. 14, pp. 151-159, 2018.

[10] S. Bilan, and O. Kolochun, "Method of steganographic concealing information based on modified containers", *Collection of scientific work of the State economic and technological university of transport*, vol. 25, pp. 107-113, 2014.

[11] L. Roberts, "Machine Perception of Three-Dimensional Solids", *Optical and ElectroOptical Information Processing*. Cambridge: MIT Press, pp. 159-197, 1965.

[12] J. M. S. Prewitt, "Object Enhancement and Extraction", *Picture processing and Psychopictorics*. Academic Press, 1970.

[13] J. M. S. Prewitt, and M. L. Mendelsohn, "The Analysis of Cell Images", *Ann. N.Y. Acad. Sci.*, vol. 128, pp. 1035-1053, 1966, doi: 10.1111/j.1749-6632.1965.tb11715.x.

[14] I. E. Sobel, Camera Models and Machine Perception, PhD Thesis, Stanford Univ, 1970.

[15] S. Bilan, *Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities*. Hershey: IGI Global, 2017.

[16] S. Bilan. "Models and hardware implementation of methods of Pre-processing Images based on the Cellular Automata", *Advances in Image and Video Processing*, vol. 2, iss. 5, pp. 76-90, 2014, doi: 10.14738/aivp.25.561.

СТЕПАН БІЛАН,
ВЯЧЕСЛАВ РЯБЦЕВ,
АНДРІЙ ДАНИЛЬЦО

ПІДВИЩЕННЯ ОБСЯГУ ПРИХОВАНИХ ПОВІДОМЛЕНЬ У ФІКСОВАНОМУ ГРАФІЧНОМУ СТЕГОКОНТЕЙНЕРІ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ЗОБРАЖЕНЬ

Розглянуто методи виділення крайових пікселів на основі операторів Робертса, Превітта і Собеля, а також технологій клітинних автоматів для збільшення обсягу впроваджуваного прихованого повідомлення. На основі використовуваних методів формувалися шаблони з виділеними пікселями, в коди яких впроваджувалися приховані біти повідомлень. Шаблони формувалися з використанням порогової додаткової обробки, що дозволило обрати

оптимальний поріг для виділення відповідних пікселів зображення контейнеру. Для оператора Робертса вибиралися пороги в межах від 100 до 300, а для операторів Превітта та Собеля – від 1000000 до 15000000. Для виділення пікселів на основі клітинних технологій використовувалося чотири форми околиці клітин за аналогією з бінарними та кольоровими зображеннями. Проведено експериментальні дослідження для всіх методів виділення пікселів, які дали можливість визначити оптимальний числовий поріг, а також кількість молодших біт кожного виділеного пікселя для впровадження в них бітів прихованого повідомлення. Експериментально встановлено, що для всіх методів, окрім двох молодших біт коду кожного пікселя, біти прихованого повідомлення впроваджуються також у чотири молодших біти кожного байту коду виділеного пікселю, що значно збільшує обсяг впроваджуваного повідомлення у контейнер фіксованого розміру. При використанні двох молодших розрядів усіх пікселів та чотирьох молодших бітів виділених пікселів для багатьох шаблонів, зміни візуальних зображень контейнерів не спостерігалося. Використання п'ятого молодшого біта у кожному байті коду виділеного пікселя для введення прихованого біта приводить до значущих спотворень візуальної картини. Експерименти проводилися для різних порогів яскравості при бінарізації. У цілому у код кожного виділеного пікселю додатково впроваджувалось шість прихованих біт. Для ефективності експериментів у контейнерах використовувалися бітові послідовності, які містили тільки одні нулі, одні одиниці та бітові послідовності, що сформовані випадково.

Ключові слова: стеганографія, контейнер, зображення, виявлення країв, клітинний автомат, приховане повідомлення.

Bilan Stepan, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

ORCID: 0000-0002-2978-5556.

E-mail: bstepan@ukr.net.

Riabtsev Viacheslav, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

ORCID: 0000-0001-8331-0132.

E-mail: viacheslav.riabtsev@gmail.com.

Daniltso Andriy, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

ORCID: 0000-0003-3783-8838.

E-mail: zzzavanturist98@gmail.com.

Білан Степан Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

Рябцев Вячеслав Віталійович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

Данильцо Андрій Сергійович, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.