Journal of Theoretical and Applied Information Technology
15th April 2022. Vol.100. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STEGANOGRAPHIC METHOD FOR RESERVING HIDDEN INFORMATION BASED ON EDGE EXTRACTION OPERATORS

AYMAN M MANSOUR*, NASHAT AL BDOUR

Department of Communications, Electronics, and Computer Engineering, College of Engineering, Tafila Technical University, Tafila 66110, Jordan

*Correspondence: mansour@ttu.edu.jo

ABSTRACT

The paper investigates the steganographic method for introducing secret messages into a container represented by the image. The research task is improving of the reliability of message storage in the event of various image distortions after transmission over a communication channel. To solve this problem, a preliminary division of the container image in a form of sectors was used. In the developed method, each sector is embedding the same secret message. The geometric shape of each sector can be different, and it depends on the distribution of the selected pixels into which the message is embedded. Pixel selection is carried out in this paper using edge pixel selection operators in the image, such as: Roberts, Sobel and Prewitt operators. For each container image, there is a different distribution of the extracted pixels and a different number in each sector. Therefore, the size of the secret message is limited to the sector in which the smallest number of extracted pixels is present. The bits of the secret message in each sector are distributed differently since the extracted pixels in each sector differ in their location. In case of destruction of a part of the container image, the secret message is saved in the remaining parts, which include non-destroyed sectors. To embed bits, the shape of the initial container, the geometric shape and location of the sectors, as well as the method for extracting pixels is required to be known. The developed method was tested using different images and the achieved performance was excellent with accuracy 92%.

Keywords: *Steganography, Image, Container, Embedded Message, Edge Pixel Extraction Operator.*

1. INTRODUCTION

Today, methods of steganographic information protection are widely developing and, in terms of their popularity, they reach methods of cryptographic information protection [1-5]. The popularity of steganographic methods is determined by the large number of electronic carriers (containers) of confidential information. Such media include files: images, sound, text document and other media from various software applications. Moreover, all such electronic media can be presented in different formats. Accordingly, different formats require the creation of different methods for steganographic protection of confidential information. The most popular containers are images (files of graphic formats: BMP, JPG, TIF, etc.), into which bits of secret information are embedded.

One of the most used methods of introducing secret bits is the LSB method [3, 6], which is based on replacing the least significant bits of each color byte of the container image. The choice of the byte sequence of the container is set by a special algorithm used by the developer. The same secret information in the same container can be embedded in different ways. However, there is a problem that the transmitted information may be distorted. The container image may be distorted during its transmission via communication channels, during recording on a medium, as well as during its opening by various software applications. Therefore, steganographic methods should be such that hidden information is stored in the container in the event of various container distortions. Various methods are used to solve this problem [7 - 9]. The most used methods are based on the repeated distribution of the same secret information over the entire field of the container. Secret information can be placed in certain sectors at a certain distance. Thus, all secret information can be embedded several times in the bytes of one set of sectors of the container. In addition, secret bits can be distributed into pixels with different colors or into pixels, which are determined by certain mathematical dependencies.

The limitation is the limited amount of classified information, as well as the need to use a container of large capacity. For greater reliability, the volumes of classified information should allow many copies to be created. This approach implements the formation of invisible digital watermarks on the image [10]. In fact, steganographic embedding of secret bits is carried out into selected bytes belonging to certain sectors of the container image. The purpose of this paper is to efficiently allocate secret bits based on a preliminary analysis of the container image.

2. ANALYSIS OF METHODS FOR THE ALLOCATION OF CLASSIFIED INFORMATION IN THE CONTAINER IMAGE

There are many methods for embedding and allocating classified information into a digital image [11]. The most common, but highly vulnerable, is the LSB method [5, 6]. LSB method has poor resistance to attacks. The stability can be increased by the random interval method [12], which allows the random allocation of the bits of the secret message over the container. Placing inline adjacent bits across the entire container field is done at different distances. This results in repeated scans of the container pixels as the secret bits are embedded and read. Rescanning occurs when the coordinate of the next embedded bit is less than the coordinate of the previous one.

The method of block information hiding is also used [13]. The container image is split into non-overlapping free-form blocks. A parity bit is calculated for each block. In each block, one secret bit is hidden. This method reduces the impact of the consequences of embedding secret bits by increasing the block size. Sufficiently resistant to the operations of compression and changing the contrast of the image are the methods PatcWork [14] and PatchTrak [15]. The methods use the analysis of the brightness characteristics of two neighboring pixels, which increases the brightness of one pixel and decreases the brightness of the neighboring pixel. This operation is repeated many times. The sum of the values of all differences and the mathematical expectation of the sum of the differences in an empty container are calculated. If there are embedded bits, then the sum is significantly greater than zero. The described method is unstable to affine transformations of the container.

Embedding of secret bits is also possible based on the frequency representation of the image [16 - 18]. For this, orthogonal transformations of images and redistribution of its energy are used. Secret messages are embedded in the mid-frequency and low-frequency regions. This group of methods includes the Koch and Zhao method [19, 20]. The container image is split into 8x8 pixel blocks. Discrete cosine transform is applied to each block. Each block hides one bit of secret data. Embedding starts after a random selection of a block. This method is highly resistant to compression but degrades the image quality.

Methods based on preliminary analysis of the container image are widely used. Searches for pixels in the image that do not lead to visual distortion is carried out. More secret bits can be embedded in the codes of such pixels [1, 2, 21]. They are based on looking for noise pixels or pixels that represent edges or gradients in brightness. These methods are used in this work.

3. METHODS FOR EXTRACTING LOW-INFORMATIVE PIXELS IN THE CONTAINER IMAGE

The first method used to implement steganographic protection is based on the selection of noise pixels [22], or the so-called isolated cells. These cells are determined by the specified brightness thresholds. The image is being converted to grayscale. For different values of the brightness threshold, a different number of individual pixels was allocated. These are individual white pixels within black-pixel boxes, as well as lone black cells within white-pixel boxes. An example of the selection of such pixels on Figure 1 is shown.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

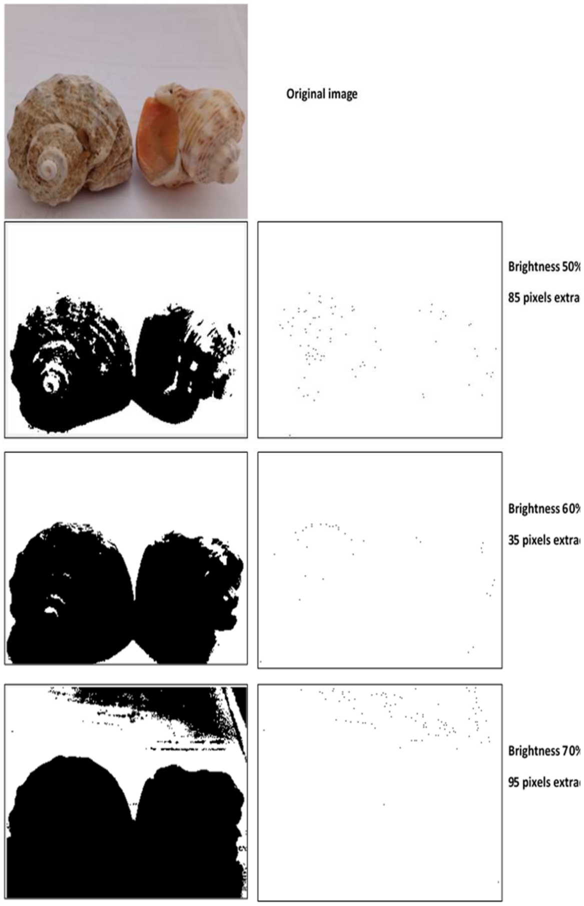


Figure 1: An example of the selection of individual single isolated pixels of the image. Brightness thresholds of 50%, 60% and 70% are used.

Isolation of individual single isolated pixels is carried out using the theory of cellular automata (CA) [23, 24]. In this case, the pixel of the image is considered as a cell. Each cell analyzes the state of the neighborhood cells. The cell is selected, in which all cells of the neighborhood have opposite states. The selection of cells is carried out according to the following logical transition function [25]

$$b_i(t+1) = b_i(t) \wedge \overline{x_1(t)} \wedge \overline{x_2(t)} \wedge \overline{x_3(t)} \wedge \overline{x_4(t)} \vee \overline{b_i(t)} \wedge x_1(t) \wedge x_2(t) \wedge x_3(t) \wedge x_4(t)$$

were $b_i(t)$ - the state of the control cell at time t;

$x_i(t)$ - the state of the neighboring i-th cell at time t.

This function uses four neighboring cells that make up the von Neumann neighborhood. For the Moore neighborhood, eight neighborhood cells are used, located vertically, horizontally and diagonally. The following logical transition function is executed [25]

$$\begin{aligned} b_i(t+1) = b_i(t) &\wedge \overline{x_1(t)} \wedge \overline{x_2(t)} \wedge \overline{x_3(t)} \\ &\wedge \overline{x_4(t)} \wedge \overline{x_5(t)} \wedge \overline{x_6(t)} \\ &\wedge \overline{x_7(t)} \wedge \overline{x_8(t)} \vee \\ \vee \overline{b_i(t)} &\wedge x_1(t) \wedge x_2(t) \wedge x_3(t) \wedge x_4(t) \wedge x_5(t) \\ &\wedge x_6(t) \wedge x_7(t) \wedge x_8(t) \end{aligned}$$

The Moore neighborhood allows for the extraction of completely isolated cells. In this case, the number of isolated cells decreases.In the obtained selected pixels, the bits of the secret message are embedded using the LSB method. An example of introducing secret bits into the two least significant bits of each byte of codes, allocated bits, on Figure 2 is shown.

Figure 2: An example of embedding secret bits into the two least significant bits of the code of the selected pixels for a brightness of 50%

In the example shown, 85 bits are extracted and, accordingly, 510 secret bits are embedded. The message in the form of alternating zeros and ones (010101 ...) is embedded in the least significant bits, and alternating ones and zeros are embedded in the first bits (1010101 ....). Each pixel code consists of three bytes encoding red, blue, and green. As can be seen from Figure 2 and the original image shown in Figure 1, there are no visual differences in the picture.

The second approach, which is used in the work, is based on the use of edge selection operators and, accordingly, the pixels that form these edges [1, 2]. Various operators are used for this. All of them select the edges in different ways and are characterized by a different number of selected pixels. The most frequently used

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

operators are the operators: Roberts [26], Prewitt [27] and Sobel [27]. There are more edge pixel selection operators. However, they were not considered in the work. The paper [2] also considered methods for extracting edge pixels based on the CA. Other papers [28-34] discussed different methods of image steganography. However, they did not show high efficiency when introducing secret bits into the selected pixels.

To select edge pixels, templates of coefficients of various dimensions are used, as well as the necessary formulas. The Roberts operator is implemented based on two patterns of 2x2 coefficients

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

and also formulas

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

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

The Prewitt and Sobel operators are implemented based on two 3 × 3 coefficient patterns

For the Prewitt operator

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

For the Sobel operator

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

The results of using such operators on Figure 3 are shown.

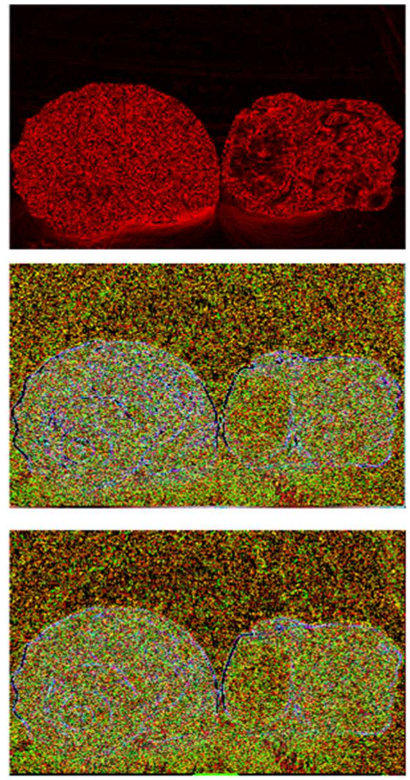


Figure 3: Examples of application of the Roberts, Sobel and Prewitt operators

Figure 3 shows that for complex images there are places of a large local accumulation of selected pixels. There are areas in the image with a dense distribution of the selected pixels, and areas with the same color and brightness characteristics have a low density of the selected pixels. The analysis of the obtained images, after applying the operators for the selection of edge pixels, showed that a uniform distribution over the entire image field is not observed. Using different thresholds after applying edge selection operators also does not give an even distribution of the selected pixels over the entire image area.

4. SECRET MESSAGE ALLOCATION METHOD FOR EMBEDDING IN NON-OVERLAPPING SECTORS

The paper considers a method for the formation of non-intersecting sectors, in each of which one secret message is embedded. The simplest way to form sectors is to split the container image into equal areas. An example of such a separation on Figure 4 is shown.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

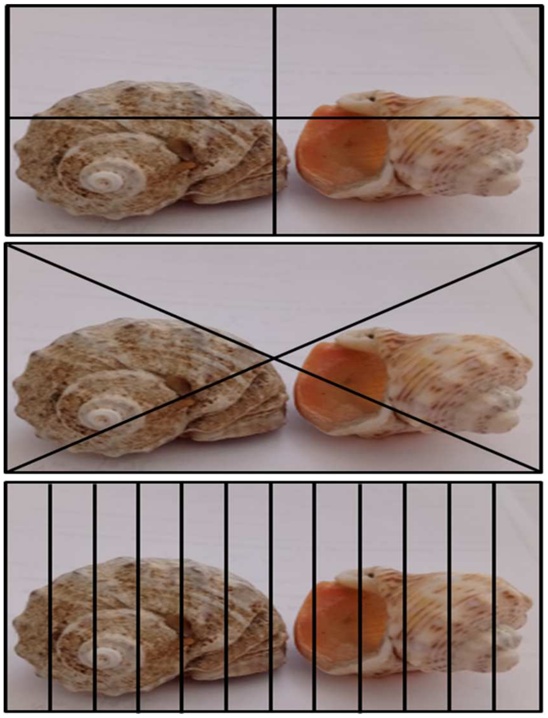


Figure 4: An example of dividing an image with selected pixels into sectors of equal geometric shape (the middle image is divided into sectors with different geometric shapes)

As a result of analyzing the images shown in Figure 4 it becomes obvious that the obtained sectors contain a different number of selected pixels. There are sectors that contain a very small number of selected pixels. The sector that contains the smallest number of pixels limits the size of the embedded secret message. In this situation, for one image of the container, a sector shape can be selected that would make it possible to obtain approximately equal numbers of selected pixels in all formed sectors.

In this case, it is considered that in each sector the selected pixels have an equal location. The embedded of secret bits into the codes of the extracted pixels in each sector are introduced line by line from left to right and from top to bottom. There are several solutions to this problem. The first solution is to select container images that would give the desired distribution of the selected pixels after applying the edge pixel selection operators. In this case, the original image should contain such patterns that the pixels are extracted and distributed over the entire image area (Figure 5).

The disadvantage of this approach is the initial selection of images of a certain structure, which may cause suspicion in the opponent. The second method is based on using images of containers of arbitrary structure. In such images, various options for the location of the selected pixels are possible. Therefore, using one arrangement of sectors in the image is not effective. To determine the shape of the sectors and the structure of dividing the image into sectors, it is necessary to perform a preliminary analysis of the container image. The result of this analysis is the choice of an operator for the selection of edge pixels, the choice of a threshold value for the corresponding operator and the choice of the geometric shape of the sector to cover the container image.

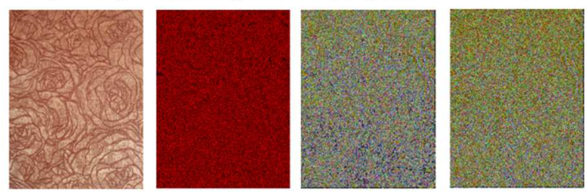


Figure 5: An example of the distribution of selected pixels in an image field with patterns based on the operators of the selection of edge pixels

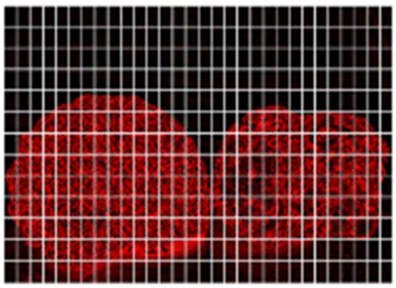
The sector shapes can be different. The number of sectors can also be different. It depends on the size of the secret message that is being embedded in the container. The shapes of the sectors also depend on the location of the selected pixels. If the selected pixels are mainly located in one place, then the geometric shapes of all sectors and their locations should cover partially selected pixels in the container image (Figure 4). Sectors can be in the form of a sector of a circle with a center located in the approximate center of the location of the selected pixels. In this case, the type of template of the geometric pattern of the coating must be known on the receiving side as additional key information. Coating shapes can be different and contain sectors of different sizes and different geometric shapes.

To determine the nature of the location of the selected pixels, you can scan the image template with the selected pixels earlier than the scanning windows are set. The number of selected pixels is calculated and if the number of selected pixels included in the scan field exceeds the specified number of bits of the secret message, then the remaining area of the container image is scanned. An example of dividing an image template into scanning fields in Figure 6 is shown.

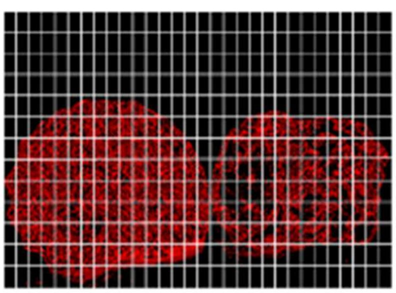
In the example (Figure 6), there are two images of the template with the selected pixels based on the Roberts operator. In the top figure,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the image has not been limited to a threshold value and therefore each scanning field contains enough extracted pixels, which exceeds the specified number of secret bits (the least number of allocated bits is 94, and the maximum is 160). The number of extracted pixels in each sector is shown in the figure as a table of sectors, in which each cell defines a sector of the image. Each sector is 10x16 pixels in size. Pixels with code less than one are set to zero.



102	119	130	131	133	120	131	125	119	131	127	130	121	142	122	123	134	126	132	118	128	122	139	137	118	115	114	142	143	121
117	135	127	130	131	131	127	122	110	119	108	125	113	125	125	127	106	117	137	130	115	121	120	127	127	125	125	122	140	119
140	133	138	138	141	129	126	119	113	143	118	123	118	120	93	106	110	111	106	104	120	130	114	105	94	118	103	121	141	125
106	103	113	130	116	118	119	113	114	132	128	127	129	135	133	128	140	139	136	124	137	144	128	139	131	131	135	123	141	132
120	121	130	140	139	149	157	156	155	156	147	133	134	103	112	128	113	112	108	125	132	134	96	121	97	129	118	118	118	115
133	128	148	159	160	160	160	160	160	160	160	159	159	133	112	113	125	117	147	160	160	159	157	158	160	159	158	156	133	97
124	160	160	160	160	160	160	159	159	160	160	159	159	160	154	124	136	159	159	159	159	160	159	160	159	159	160	160	160	132
143	160	159	160	160	160	160	160	160	160	159	160	160	160	159	145	156	158	154	152	152	160	160	159	158	160	160	160	160	136
158	160	160	160	160	160	159	160	160	160	160	160	160	160	160	157	159	151	156	151	156	159	159	160	160	160	160	160	160	132
152	160	160	159	160	160	159	160	160	160	160	160	160	160	160	160	159	158	160	158	159	158	160	160	159	158	157	159	155	128
155	160	160	160	159	160	157	159	159	160	160	159	160	160	160	159	160	160	158	159	160	159	159	159	160	159	158	159	152	115
158	160	160	159	160	159	160	160	160	160	160	160	160	160	160	160	160	160	160	160	160	160	160	159	156	154	151	154	131	125
152	158	158	160	160	159	160	160	160	160	159	160	159	159	155	139	153	160	159	159	159	160	159	158	152	150	140	143	142	122

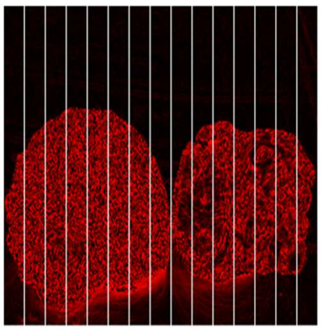


0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	10	49	73	118	108	97	103	85	37	6	0	0	0	0	0	1	23	44	35	1	0	0	0	0	0	0	0
0	4	74	124	116	124	154	135	135	140	132	131	112	61	0	0	0	52	102	130	128	135	120	81	76	75	81	79	23	0
4	155	154	144	144	145	151	145	150	146	148	144	157	95	94	1	42	67	96	80	108	141	92	90	65	92	111	88	126	54
71	131	150	149	135	130	137	118	151	124	141	140	147	145	147	55	101	57	50	49	78	106	101	117	95	80	111	112	109	51
108	154	149	147	148	129	126	137	141	138	147	149	152	142	144	117	103	25	24	27	73	128	137	83	94	106	84	113	107	11
86	157	151	147	120	95	125	126	144	142	149	127	124	145	152	119	105	85	55	85	90	120	105	61	115	70	52	102	93	0
10	108	140	150	126	114	100	115	140	138	154	134	154	129	118	92	26	89	106	102	90	116	136	111	108	52	98	93	53	0
0	15	54	109	133	128	119	151	150	151	157	141	134	124	87	22	3	33	49	67	73	61	42	14	0	0	2	0	0	0
0	3	6	21	47	88	105	85	41	16	7	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

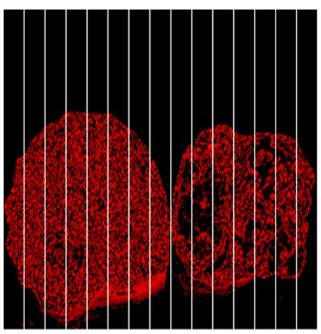
Figure 6: An Example Of Splitting An Image Template With Selected Pixels Into Scanning Fields

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The bottom image is obtained by thresholding the top image (the threshold is 100). The number of selected pixels is less than in the top image. Accordingly, there are sectors that do not contain dedicated pixels. Therefore, the presented template shapes are not suitable for such an image. The following templates are used (Figure 7).



3617	3849	3864	3848	3850	3821	3769	3574	3639	3731	3823	3772	3159	3716	3475



946	1861	2040	2229	2249	2126	1767	1148	786	1044	1476	1291	832	1072	633

Figure 7: An example of dividing an image template with selected pixels into scanning fields separated by vertical borders

Such division is acceptable for both images since each sector of the template contains selected pixels. As you can see, the smallest number of selected pixels (633) contains the last sector for the second template. The first template contains more than 3000 selected pixels in each sector. This template is the most acceptable. As a result, templates with selected pixels are formed, which contain different distributions of the selected pixels (Figure 8).

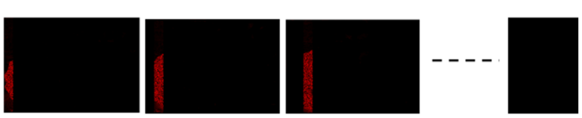


Figure 8: Formed templates for each sector according to Figure 7

With the help of the generated templates, the same secret message is embedded in each sector of the image. In this example, the sectors have the same rectangular shape. As can be seen from the location of the allocated pixels in each sector, the bits of the secret message will be distributed differently in each sector. However, the order of embedding and the order of extracting secret bits in the codes of the extracted pixels is the same. An image of a container into which 15 secret messages are embedded (one secret message is embedded in each selected sector) in Figure 9 is shown. Secret bits are embedded in the least significant three bits of each color byte of the codes of the extracted pixels. This method is acceptable for text secret messages. It is also acceptable for images that can be used as electronic watermarks. However, after implementation, the geometric structure of the embedded images is lost.

The accuracy of the developed method using 400 images were selected randomly were 92%. The test was done through applying a distortion to the images after introducing secret messages into a container. The reliability of message storage in the present of distortions after transmission over a communication channel was enhanced and detected by the receiver.

5. CONCLUSION

The paper considers and investigates a method for introducing classified information into containers, represented by images with multiple duplication over the entire field of the container. For greater reliability and high resistance to destruction, the container image is divided into sectors of various geometric shapes. For efficient storage of classified information, a method of scanning an image template with selected pixels was investigated, which made it possible to analyze the distribution of selected pixels over the entire field of the container image and select the optimal segment shape. The method allows using an image of a container with an arbitrary structure. At the same time, the images of containers should be multi-gradation, and the use of adaptive thresholds made it possible to form templates with the required number and location of the selected pixels. Pixel selection based on edge extraction operators made it possible to use many bits of pixel codes to embed secret bits. The proposed steganographic method does not distort the visual characteristics of the container image. The accuracy of the developed method is 92%.

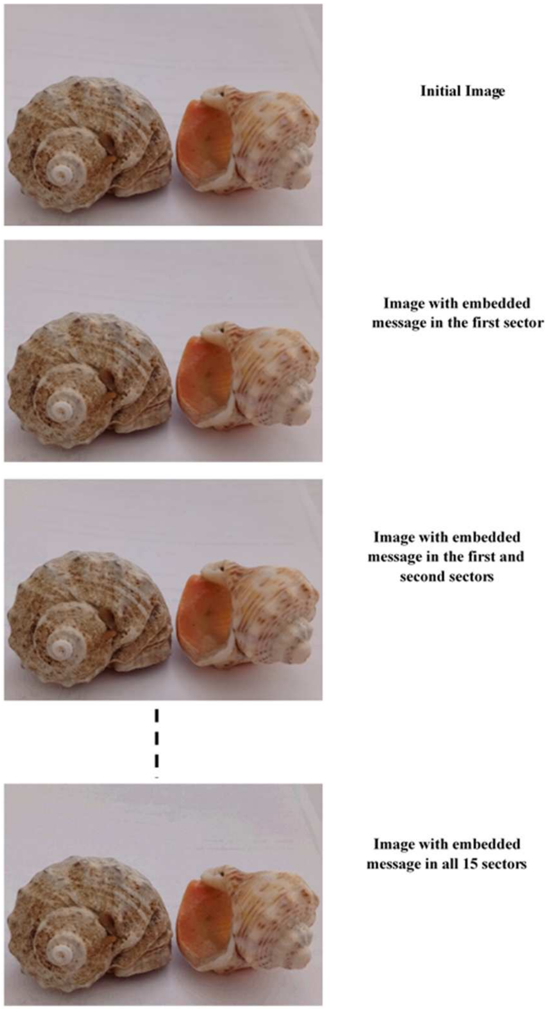


Figure 9: Image of the container, into which 15 secret messages are embedded according to its division into 15 sectors.

REFERENCES:

[1] Nashat Albdour, Nabeel Zanoon. (2020), A Steganographic Method Based on Roberts Operator. Jordan Journal of Electrical Engineering, V. 6, N3: 265-273

[2] Stepan Bilan, Viacheslav Riabtsev, Andriy Daniltso. (2020) Volume increasing of secret message in a fixed graphical stego container based on intelligent image analysis, - Information Technology and Security, Vol. 8, N2, P. 133-143.

[3] Yahya, A., (2019). Steganography Techniques for Digital Images, Springer

[4] Mykola Bilan, Andrii Bilan. (2019). 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, USA: IGI Global: 79 – 94

[5] Blokdyk, G., (2019). Steganography Third Edition, 5STARCooks

[6] Gregory Kipper. Investigator's Guide to Steganography. (2003), Auerbach Publications.

[7] Liu, Y., Wang, J., Fan, J. H. & Gong, L. H. Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences. Multimed. Tools Appl. 75, 4363–4382 (2016).

[8] Wang, X. Y., Zhao, H. Y. & Wang, M. X. A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices. Opt. Laser Technol. 115, 42–57 (2019).

[9] Manish Kumar, Rachid Ait Maalem Lahcen, R. N. Mohapatra, Chandan Alwala, and Surya Vamsi Krishna Kurella. Review of Image Encryption Techniques. - Journal of Computer Engineering.- Volume 22, Issue 1, Ser. I (Jan - Feb 2020), PP 31-37

[10] Lin Keming. Research of Digital Watermark Technology Based on Static Image// International Conference on Computer and Communication Technologies in Agriculture Engineering, 2010. URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5543681

[11] An Existential Review on Text Watermarking Techniques International Journal of Computer Applications (0975 – 8887) Volume 120 – No.1 June 2015, p. 29-32

[12] Moller, S. Computer Based Steganography: How It Works And Why Therefore Any Restriction On Cryptography Are Nonsense, At Best, S. Moller, A. Pfitzmann, I. Stirand , Information Hiding: First International Workshop, Springer as Lecture Notes in Computing Science. , 1996. , Vol.1174. , P.7-21.

[13] Khoroshko, V.O. Fundamentals of Computer Steganography: uch. manual for students and graduate students ,V.O. Good ko, O.D. Azarov, M.E. Rustle. - Vinnytsia: VDTU, 2003

[14] Bender, W. Techniques for Data Hiding, W. Bender, D. Gruhl, N. Morimoto, A. Lu, IBM Systems Journal. – 1996. – Vol. 35. – P. 313-336

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[15] Bender, W. Applications for Data Hiding / W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb, IBM Systems Journal. – 2000. – Vol. 39, No.3&4. – P. 547-568.
[16] https://helpiks.org/6-82906.html
[17] Bhattacharyya D., Kim T. Image Data Hiding Technique Using Discrete Fourier Transformation, Proceedings of the Second International Conference « Ubiquitous Computing and Multimedia Applications» (UCMA 2011). Korea, Daejeon. 2011. P. 315-323.
[18] Chen W-Y. Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation, Applied Mathematics and Computation. 2007. Vol. 185. P. 432-448
[19] Zhao, J. Embedding Robust Labels into Images for Copyright Protection , J. Zhao, E. Koch , Proc. of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies. Munich, Vienna, 1995. P. 242–251.
[20] Zhao, J. Towards Robust and Hidden Image Copyright Labeling, J. Zhao, E. Koch , IEEE Workshop on Nonlinear Signal and Image Processing. Greece, 1995. P. 123–132.
[21] Stepan Bilan, Andrii Demash. High performance encryption tools of visual information based on cellular automata. - Information Technology and Security. - 2016. - Vol. 4, № 1(6). - C. 62-75.
[22] Nashat Albdour. A Novel Methods For Image Steganography By Effective Image Points Selection, - IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE),- Volume 14, Issue 5 Ser. II (Sep. – Oct. 2019), PP 06-11
[23] Stepan Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities.- (2017).- IGI Global, USA.- P. 301
[24] S.M.Bilan, M.M.Bilan, R.L. Motornyuk. New Methods and Paradigms for Modeling Dynamic Processes Based on Cellular Automata. IGI-Global. 2020. — P. 200
[25] N. Albdour, “Selection image points method for steganography protection of information,” WSEAS Transactions on Signal Processing, vol. 14, 2018.
[26] L. Roberts. (1965). Machine Perception of Three-Dimensional Solids, Optical and Electro Optical Information Processing, MIT Press: 159-197.
[27] Prewitt, J.M.S. (1970). "Object Enhancement and Extraction". Picture
[28] X. Duan et al., "High-Capacity Image Steganography Based on Improved FC-DenseNet," in IEEE Access, vol. 8, pp. 170174-170182, 2020.
[29] X. Duan, D. Guo, N. Liu, B. Li, M. Gou and C. Qin, "A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network," in IEEE Access, vol. 8, pp. 25777-25788, 2020.
[30] W. Lu, L. He, Y. Yeung, Y. Xue, H. Liu and B. Feng, "Secure Binary Image Steganography Based on Fused Distortion Measurement," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, no. 6, pp. 1608-1618, June 2019.
[31] W. Lu, Y. Xue, Y. Yeung, H. Liu, J. Huang and Y. -Q. Shi, "Secure Halftone Image Steganography Based on Pixel Density Transition," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1137-1149, 1 May-June 2021.
[32] X. Liao, Y. Yu, B. Li, Z. Li and Z. Qin, "A New Payload Partition Strategy in Color Image Steganography," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 3, pp. 685-696, March 2020.
[33] J. Tao, S. Li, X. Zhang and Z. Wang, "Towards Robust Image Steganography," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, no. 2, pp. 594-600, Feb. 2019.
[34] Q. Liu, T. Qiao, M. Xu and N. Zheng, "Fuzzy Localization of Steganographic Flipped Bits via Modification Map," in IEEE Access, vol. 7, pp. 74157-74167, 2019.