JJEE
Volume 6, Number 3, 2020
Pages 265-273
Jordan Journal of Electrical Engineering
ISSN (Print): 2409-9600, ISSN (Online): 2409-9619

A Steganographic Method Based on Roberts Operator

Nashat Albdour[1*], Nabeel Zanoon[2]

[1] Department of Communications and Computer Engineering, Tafila Technical University, Tafila, Jordan
E-mail: Dr.nashat82@yahoo.com
[2] Department of Applied Science, Al-Balqa' Applied University, Aqaba, Jordan

Received: Mach 22, 2020 *Revised: April 25, 2020* *Accepted: May 8, 2020*

***Abstract*—** This paper proposes a new steganographic method - based on Roberts operator edge detector in digital images - with the aim to increase the size of secret messages that can be embedded and hidden in images. An algorithm is developed to execute the task with two constraints: i) fixed dimensions size of the image and ii) no visual distortion of the resulted image. The proposed methodology embeds data of the built-in secret message into the image's boundary pixels obtained using the Roberts operator. To do this, edge detector threshold selection strategy is proposed to achieve the optimal threshold value by creating a reference images with different numbers of boundary pixels. Finding this optimal threshold value is very important since it decreases the image's visual distortion. The results of the conducted experiments to test the developed algorithm show excellent results in hiding secret messages in the low-order bits of the selected pixel codes of the reference image boundaries.

***Keywords*—** Steganography; Digital image; Roberts operator; Container; Embedded message; Threshold processing.

1. INTRODUCTION

Nowadays, steganographic methods for protecting information are becoming increasingly popular [1-9]. To implement steganographic protection of information in digital data transfer systems, various types of multimedia containers are used such as video files, audio files, digital images and text format files. The main steganography concerns are: i) preservation of the container's structure without significant distortion and ii) implementation of the maximum amount of information. These two concerns are considered as a measure of the steganography method's efficiency and are, popularly, named as perceptual transparency and capacity in digital images [10].

The first concern is achieved by looking for those container objects, whose structures are not affected by the embedding process. For example, using the least significant bit (LSB) method does not change the visual characteristics of the container digital image [2, 8, 11-14].

The second concern of any steganography method is to increase the size of the embedded message into the digital container and; thus, enhancing the capacity. This concern is closely related to the first with respect to its solution. Different steganographic methods and algorithms are proposed in [8, 14-18]. Comparison of different steganographic methods in terms of their capacity can be perfectly achieved only if a container of fixed volume is used.

The most popular and simplest method of embedding a secret message in an image (steganographic container) is the LSB method, which implements the insertion of secret message bits in the lower bits of each pixel code [2-8]. This method is used universally for all types of containers. However, if the adversary knows about the presence of a secret message, he spends all his efforts on calculating the steganographic key. In fact, steganographic protection is reduced to zero, and only determining the steganographic key remains.

* Corresponding author
Article's DOI: 10.5455/jjee.204-1583873433

Currently, many algorithms have been developed for sequentially selecting image pixels and embedding the secret message into these pixels as noise [14, 18]. In this case, the image is generated by the steganographic system and pixels are allocated in it for embedding. Such noise does not cause suspicion of the adversary during observation. At the same time, the image quality is reduced, which may also cause certain questions from the adversary.

If noise is not artificially introduced into the image, the selected pixels can be attributed to noise pixels. To determine the cells assigned and converted to noise, cellular automata are usually used to analyze neighboring cells [19]. The disadvantage of this method is the small number of image cells in which secret bits can be embedded. Also, noise pixels are highlighted by themselves and can attract the attention of an adversary.

Steganographic protection methods, which are based on preliminary analysis of the container image, aim at forming pixel arrays with equal codes [18]. The pixels in the arrays are numbered sequentially and the bits of the secret message are embedded, making changes only to the specified pixels in each code group. These methods have limited capacity because embedding secret message's bits is restricted to the three least significant bits of codes of the selected pixels.

There are methods to increase the volume of embedded messages based on the use of video containers of various formats [8]. These methods are currently being developed and investigated. However, they use containers of large volumes, as well as additional software applications.

In this paper, a steganographic algorithm is introduced for fixed-volume containers which are digital images. This method aims to increase the embedding capacity without decreasing the image quality. It deploys Roberts's operator edge detector to obtain the boundary pixels inside the image to hide the secret message inside them using the LSB technique. The rest of this paper is structured as follows: section 2, introduces the proposed steganographic. Results and discussions are presented in section 3 and section 4 concludes the algorithm and the obtained results.

2. THE DEVELOPED ALGORITHM USING ROBERTS OPERATOR

In modern steganographic systems, digital images are most often used as containers [1-4, 6, 7, 9, 11, 12]. Such containers can be represented by images of various formats like BMP, JPG, TIF, PNG, etc. However, the conversion of one format to another leads to a change in the structure and the volume of the container. The most complete representation of the image is carried out using the BMP format, which is characterized by the use of a large amount of memory. Such images are represented by an array of pixels, each of which is represented by a color and brightness code. An example of an array of image pixel codes is shown in Fig. 1.

Each pixel code represents a decimal number, which is calculated from a 24-bit binary code. Each decimal number consists of 8-bit fields encoding red, green and blue colors.

Since the graphic container has a fixed volume, the embedded secret message has a limited volume. An increase in the volume of the embedded message is made possible by the selection of such pixels of container images. Changing a large number of code bits does not lead to visible visual distortions of the container image because it can be noise pixels.

9618329	8433283	7051373	5341780	4486984	3566653	3303738	2910007	2713142	2647349	238469
9947808	8960654	7447415	5671517	4685391	3961926	3633731	3371073	3503173	3700808	343789
10211493	9421976	8106373	7053685	5738595	4883800	4358226	4227154	4358740	4556376	422792
10474923	10014884	9225111	8370572	7384191	6331760	5411428	4951134	5016927	5149027	534640
10607538	10278573	9949608	9423262	8634002	7449985	7055484	6003310	5476966	5542759	554301
10541744	10607793	10410414	10081448	9686690	8963224	8108173	7121534	6331761	5608295	547670
10410928	10608051	10673844	10673331	10410159	9884072	8963227	8042123	7581571	6660212	541040
10344880	10476466	10608052	10805174	10739124	10213294	9818536	9094555	8567696	7383422	606756
9753770	10279857	10279857	10542516	10739638	10804917	10541745	10080937	9291164	8566671	725029
9293476	9819306	10148271	10476723	10739638	10870967	10936246	10673074	10080937	9290394	810612
8571037	9031074	9622441	9885613	10411700	10674102	10936760	10870710	10541745	9948838	909301
7914905	7914134	8571294	9163687	9623982	10346677	10674615	10739895	10607795	10344109	981699
6996886	6535308	6995088	7718554	8375971	9295788	9886384	10346165	10542774	10607796	102775
6012303	5419396	5419138	6273421	6931094	7916704	8901801	9558447	10083764	10345909	104762
5026949	4631934	4434812	4763007	5486730	6341011	7326109	8376999	9164973	9755570	103461
4304767	4238204	4369276	4238461	4567682	5159048	6012817	6997657	7916961	8902058	975556
3910522	4041081	4369533	4304510	4107645	4633732	5027206	5880974	6997401	8114083	890154
3714171	3844473	3975802	4041081	4238717	4501889	4632962	5224071	6012046	7260058	844202
3386490	3450742	3712630	4106104	4237690	4303740	4172667	4697984	5551495	6602385	778460
2991732	2793326	3055214	3382894	3513967	3776112	4039540	4565114	5090174	6075528	712641
2925169	2135910	2266468	2594149	2987879	3446376	3643241	4103279	4759925	5416314	653351
3055470	2201188	2003038	2264669	2461020	2920032	3181920	3378274	3705698	4625771	541374
3842162	2724964	2395485	2460507	2525274	2853212	3181150	3179866	3310167	3769176	442582
4825976	3708521	3117154	2722396	2787163	3049308	3245404	3309655	2979661	3241292	376609

Fig. 1. An example of a code array of a BMP image snippet (11×24).

Using fixed graphic containers (an image with fixed dimensions) can be a great metric to evaluate the steganographic algorithm in terms of capacity. Increasing capacity means embedding secret messages of maximum volume without visual distortions of the original image. This can be achieved by suggesting a steganographic algorithm that selects more pixels that have less effect on the visual perception and image quality. These pixels would be used to embed the secret message. The selection of appropriate pixels can be done based on a preliminary analysis of the container image as well as a good knowledge of its structure.

The best solution to this problem is to pre-create the container image; and the pixels used are set initially. However, if the container comes from other outside source and cannot be converted to the desired form, then it is necessary to use search methods for the necessary pixels into which the bits of the secret message will be embedded.

This paper develops an algorithm for choosing the image pixels of a fixed container into which bits of a secret message are embedded. Selecting the necessary pixels has been developed and presented in [20]. The Roberts operator is used to select pixels of a multi-gradation image, which form the boundaries between regions with different intensities. There are also many other operators that are used to detect the edges of objects in the image. To implement the Roberts operator, we use the formula:

$$G = \sqrt{G_1^2 + G_2^2} = \sqrt{\left(\sqrt{y_{i,j}} - \sqrt{y_{i+1,j+1}}\right)^2 + \left(\sqrt{y_{i+1,j}} - \sqrt{y_{i,j+1}}\right)^2} \quad (1)$$

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

The following two arrays are used to make it possible to implement this equation

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

These arrays use diagonal pixels. On minor diagonals, the codes are reset to zero, and only the pixel values located on the main diagonals are used. An example of the application of the Roberts operator using Eq. (1) is presented in Fig. 2.

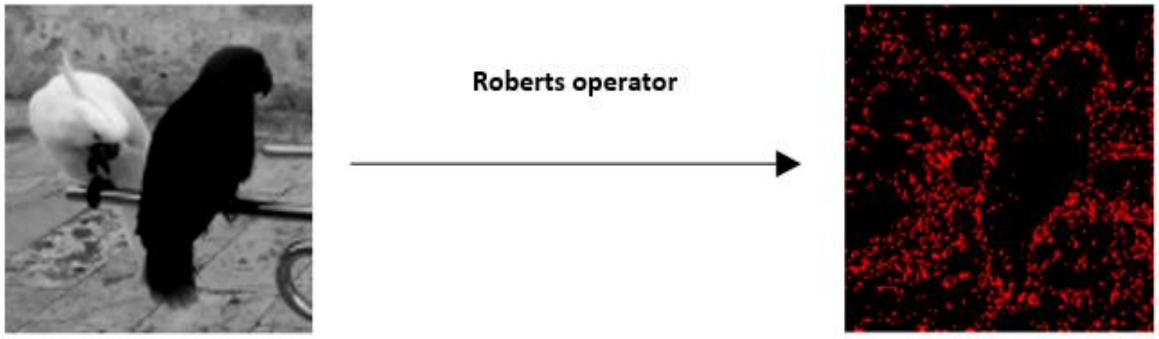

Fig. 2. An example of using the Roberts operator.

The main feature of the Roberts operator is that brightness differences in the image are represented by a sequence of two pixels as shown in Fig. 3. This is due to the arrays used to highlight pixels. It was accepted that such pixels are located on the brightness differences in the image. Pixels forming edges in the image were highlighted using the Roberts operator.

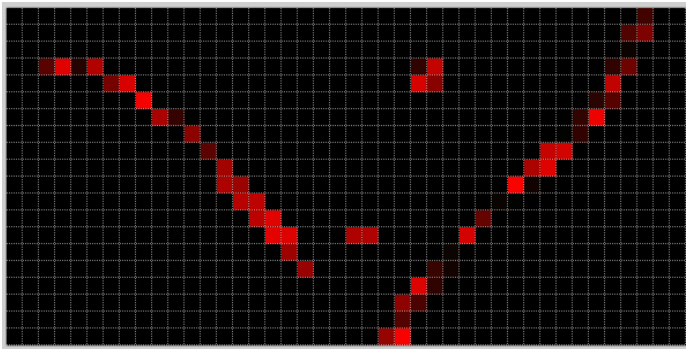

Fig. 3. Fragment of the edge after applying the Roberts operator.

However, the use of the Roberts operator according to Eq. (1) does not solve the problem of images with many brightness drops. Therefore, additional threshold processing is used.

The pixel codes of the converted image were analyzed according to Eq. (1). The code of each pixel was formed using shades of three codes: blue - green - red (BGR). Each color and its shades are represented by an eight-bit code, which was analyzed to perform the threshold processing.

Reference images were generated in which each pixel was encoded according to the formula:

$$G(t+1) = \begin{cases} 0, & if\ G(t) < A \\ G(t) & otherwise \end{cases} \quad (2)$$

where: G (t) – pixel value at time t; A - used threshold value.

3. EXPERIMENTS AND RESULTS

To create reference images, decimal values of the codes of all pixels were considered and the following values of A were used: 100; 200; 300; 400; 500; 600; 700. The obtained reference images are presented in Fig. 4.

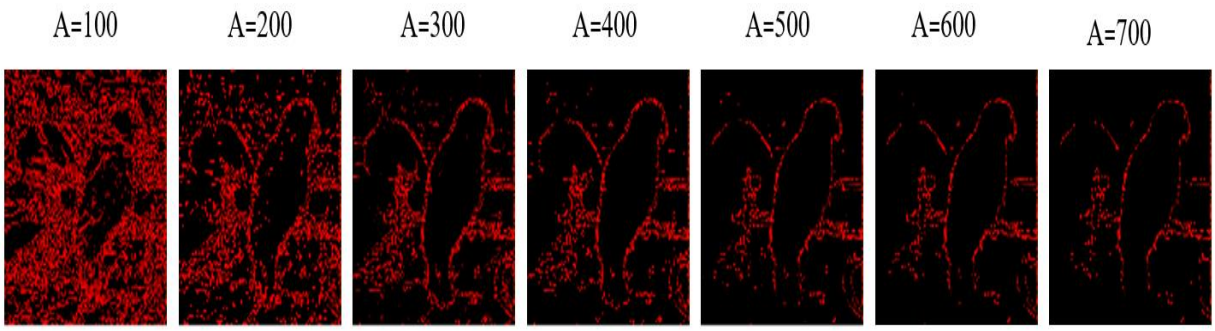

Fig. 4. Reference images obtained by applying threshold processing to different values of A

With increasing A, the number of selected pixels decreases. However, pairing is preserved, as it is inherent in the Roberts operator. Each reference image contains pixels with zero code and pixels that have codes obtained according to Eq. (1).

In accordance with the obtained reference images, the pixels of the original image were determined, which correspond to non-zero pixels in the reference images. Secret message bits were embedded in the codes of the selected pixels of the original image. Secret message bits can be embedded in selected pixels sequentially row-wise and column-wise; or they can be embedded using the selected pseudo-random law [19].

To determine the number of LSB in the codes of the selected pixels, the reference image with the smallest selected threshold was first used (A=100). This image contains the largest number of selected pixels. Therefore, it is believed that a change in color and brightness characteristics will lead to visual distortion. Secret message bits were embedded in the lower bits of the red, green, and blue codes of the separately allocated pixels. Bits were also introduced into the lower bits at the same time of all three colors. The results of embedding the secret message bits in the lower bits of the codes of the allocated pixels (at A = 100) at the lowest threshold are presented in Fig. 5.

Fig. 5 indicates the number of low-order pixels and the color into which the bits and structure of the secret message are embedded. At the top of each group of pixels is the original image of the container, to the right of which the lower bits of the codes of the selected pixels are indicated, into which the bits of the secret message are embedded. To the right of each row of images in the group are the sequences of color codes into which message bits were embedded. For example, if the notation "00 (R_G_B-RGB)" is recorded, this means that the first image in the line represents the original container after the code 00 is inserted into the two least significant bits of the red color code of the selected pixels. The second image is determined by the green color in the code, while the third the image is determined by introducing 00 into the two least significant bits of the blue code. The fourth image shows the result of introducing 00 into the two least significant bits of the red, green, and blue codes at the same time.

To determine the complete picture of distortions, we used messages containing all zeros (00000 ... ..), all ones (11111 ... ..) and the alternation of zeros and ones (101010 ... ..). Moreover, if an alternating sequence of zeros and ones was used, then messages starting from zero (010101 ....) were embedded in even lower order digits (0, 2, 4, ...), and odd digits (1, 3, 5, 7, ...) messages starting with one (10101010 ....) were introduced.

Fig. 5 shows that visible changes in visual characteristics are observed when the bits of a secret message are embedded in the four least significant bits. Moreover, for codes of different colors and for different secret messages, various changes in visual characteristics are observed. It depends on what colors and shades prevail in the initial image of the container.

It is obvious that changing the codes of a large number of pixels in the image of containers leads to a change in its visual characteristics. Therefore, the task is to find the optimal number of pixels of the selected location that does not make visual changes to the initial image of the container.

Fig. 5. Images of containers obtained as a result of embedding bits of a secret message in the lower bits of the codes of the selected pixels at A = 100.

To solve this problem, threshold processing with a large threshold values (A = 200, 300, 400, 500, 600 and 700) was used. The experimental results for such thresholds are shown in Fig. 6. These different thresholds have been tested on images of containers obtained as a result of embedding bits of a secret message in the low-order five bits of codes of the selected pixels.

Analysis of visual characteristics showed that significant changes in visual characteristics of these thresholds were not observed at A = 600 and A = 700. The visual characteristics do not change for any secret messages. Because of this A=600 has been used since A<600 a visual change of original message will be observed.

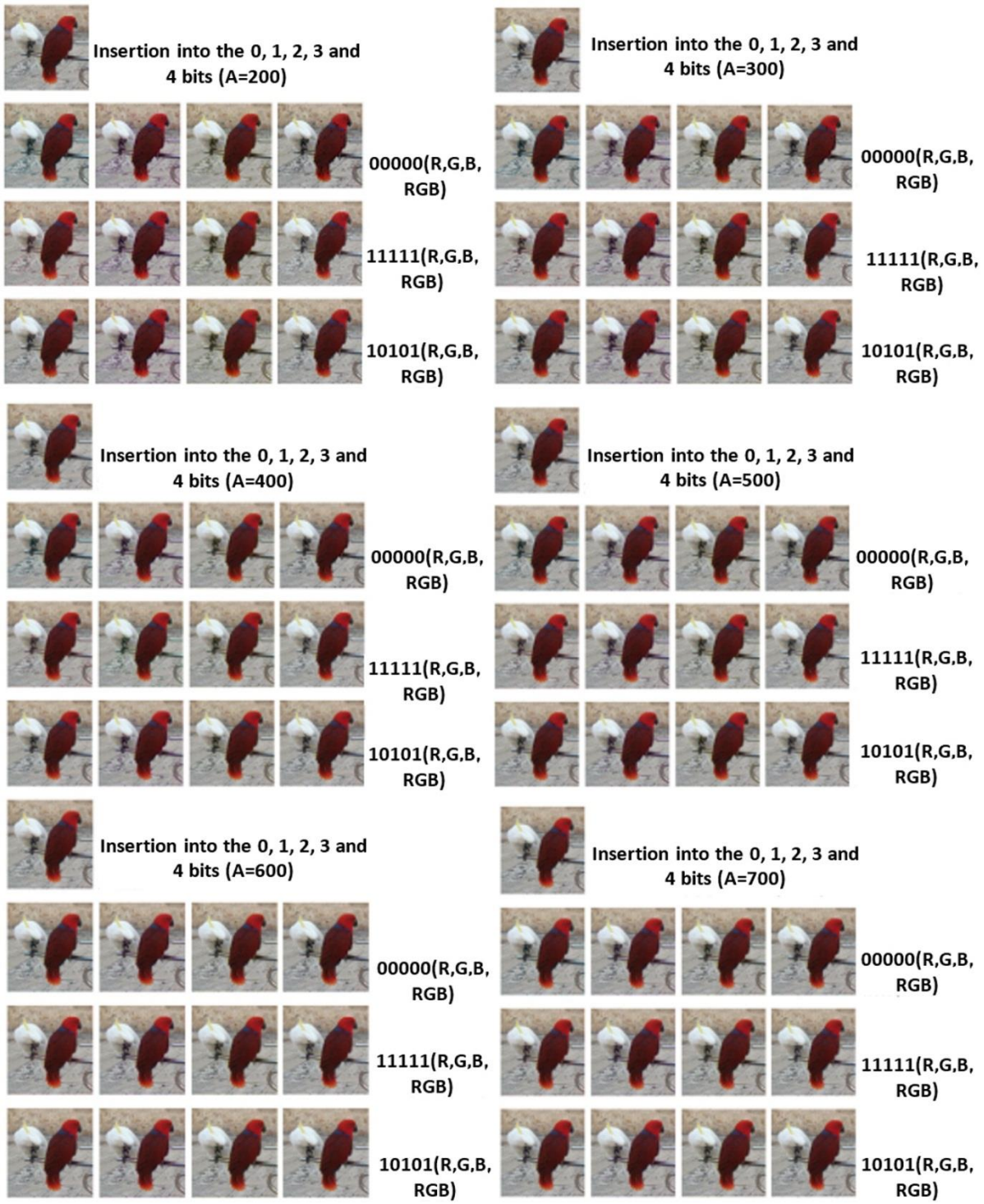

Fig. 6. Images of containers obtained as a result of embedding bits of a secret message in the low-order five bits of codes of the selected pixels with different threshold values.

Fig. 7 shows visible changes in the visual characteristics for another example. The visual characteristics are observed when the bits of a secret message are embedded in the three and five significant bits. We used messages containing all zeros (00000 ... ..), all ones (11111 ... ..) and the alternation of zeros and ones (101010 ... ..). The messages starting from zero (010101 ....) were embedded in even lower order digits (0, 2, 4, ...), and odd digits (1, 3, 5, 7, ...) messages starting with one (10101010 ....) were introduced.

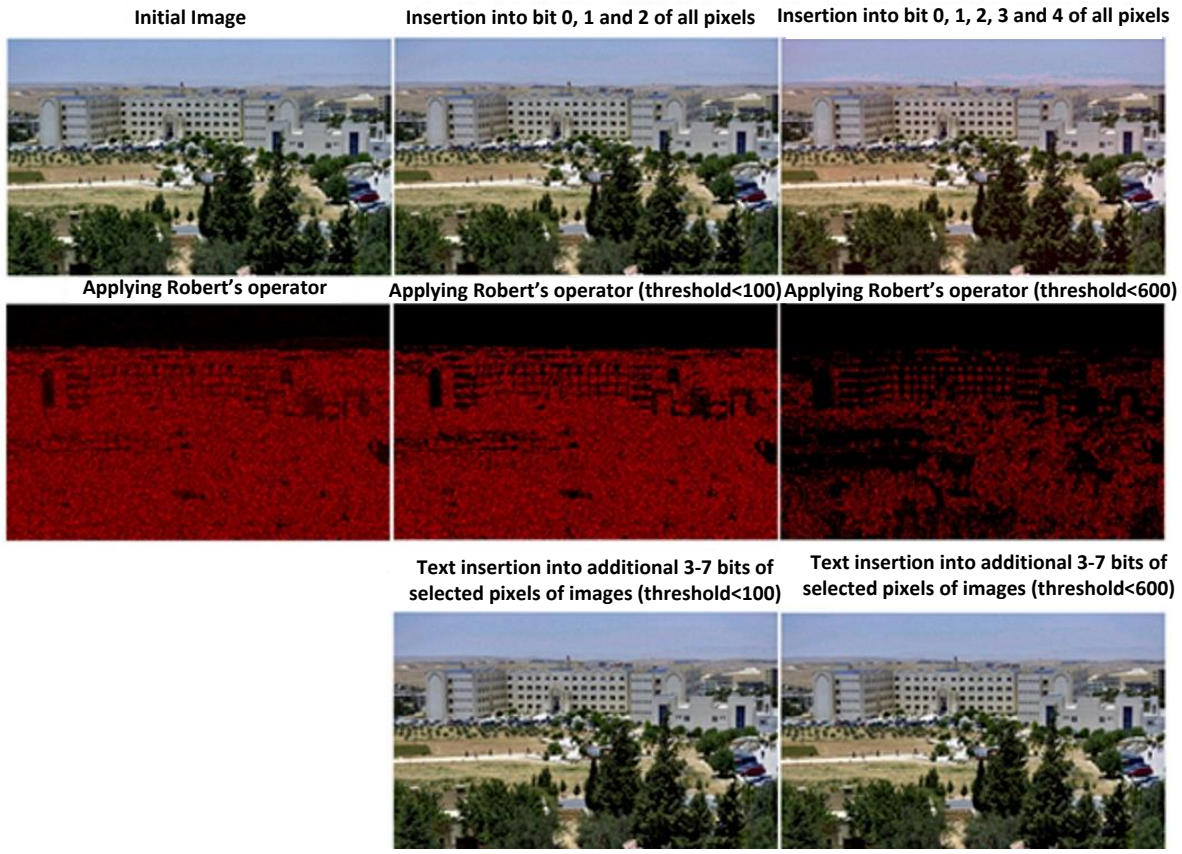

Fig. 7. Images of containers obtained as a result of embedding bits of a secret message in the lower 3 and 5 bits of the codes of the selected pixels at A = 100 and A=600.

In the results obtained earlier, described in [14, 18], it is shown that the secret message bits can be implemented in the three low-order significant bits of all pixels in the container image. Using the selected pixels generated from the Roberts operator, one can embed bits of the secret message in the fourth and fifth least significant bits of the selected pixels with a threshold A = 600. Thus, if the image of the container has a dimension of 100 × 100 pixels, then (30,000 + 2B) pixels can be embedded in it (where B is the number of selected cells, as a result of applying the Roberts operator with a given threshold A).

4. CONCLUSIONS

In this paper, a new method was introduced to detect and determine the cells that can be used to hide a secret message without any visual changes of the original picture. This was done using the Roberts Operator which allowed selecting - in the best way - the pixels that forms the differences in the brightness of the image.

Experiments were done to test the developed method by introducing secret messages in the lower order bits detected by Roberts Operator. The optimal threshold which is used in the experimental part was selected in a way that kept the image without significant visual distortion.

REFERENCES

[1] H. Sajedi, *Recent Advances in Steganography*, InTech, Croatia, *2012*.

[2] G. Kipper, *Investigator's Guide to Steganography*, CRC Press, 2003.

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

[4] A. Yahya, *Steganography Techniques for Digital Images*, Springer, 2019.

[5] M. Hegarty, A. Keane, *Steganography, The World of Secret Communications,* Create Space Independent Publishing Platform, 2018.

[6] P. Kumar, R. Bhagat, S. Suvarna, *Steganography Using Visual Cryptography*, Independently Published, Pratheek, 2017.

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

[8] M. Bilan, 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, USA: IGI Global, 2019.

[9] M. Saracevic, A. Selimi, S. Pepić, *Implementation of Encryption and Data Hiding in E-Health Application*, Handbook of Research on Intelligent Data Processing and Information Security Systems, USA: IGI Global, 2020.

[10] M. Hussain, M. Hussain, "A survey of image steganography techniques," *International Journal of Advanced Science and Technology*, vol. 54, 2013.

[11] V. Reddy, A. Subramanyam, P. Reddy, "Implementation of LSB steganography and its evaluation for various file formats," *International Journal of Advanced Networking and Applications*, vol. 2, no. 5, 2011.

[12] S. Gupta, G. Gujral, N. Aggarwal, "Enhanced least significant bit algorithm for image steganography," *International Journal of Computational Engineering and Management*, vol. 15, no. 4, 2012 .

[13] K. Raja, C. Chowdary, K. Venugopal, L. Patnaik, "A secure image steganography using LSB, DCT and compression techniques on raw images," *3rd International Conference on Intelligent Sensing and Information Processing*, Bangalore, 2005.

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

[15] J. Sprott, *Elegant Fractals: Automated Generation of Computer Art*, World Scientific Publishing Company, 2019.

[16] N. Shehab, *Toward a New Steganographic Algorithm for Information Hiding: With our algorithm, Wendy should not be able to distinguish in any way between cover-image and stego-image*, LAP LAMBERT Academic Publishing, 2012.

[17] U. Dewangan, M. Sharma, S. Bera, *Development and Analysis of Stego Images Using Wavelet Transform*, LAP LAMBERT Academic Publishing, 2015.

[18] M. Hegarty, A. Keane, *Steganography, The World of Secret Communications*, CreateSpace Independent Publishing Platform, 2019.

[19] S. Bilan, M. Bilan, R. Motornyuk, A. Bilan, S. Bilan, "Designing of the pseudorandom number generators on the basis on two-dimensional cellular automata," *Proceedings of the 1st International Conference on Applied Physics, System Science and Computers*, Dubrovnik, Croatia, 2017.

[20] L. Roberts, *Machine Perception of Three-Dimensional Solids, Optical and ElectroOptical Information Processing*, MIT Press, 1965.