Selection Image Points Method for Steganography Protection of Information

NASHAT ALBDOUR
Tafila Technical University
P.O.Box 179, Tafila, 66110, JORDAN
Dr.nashat82@yahoo.com

Abstract:- The method of effective extraction of image cells for realization of steganographic protection of information is proposed in the paper. On the basis of the proposed method, a method for constructing a container is proposed as represented by a graphic file. The main units of the steganographic system are developed on the basis of the proposed method of a graphic container constructing. To increase the number of the extracted cells, noise is added to the image. Noise cells are also used to embed message bits. The schemes and VHDL models of the cell extraction unit are developed.

Key-Words: - steganography, image, cellular automaton, extraction of isolated cells, image noise, container.

1 Introduction

The task of information security from unauthorized access has been solved throughout the history of humanity. There are two main ways to solve this problem: cryptography and steganography. The purpose of steganography is to hide the very existence of a secret message. In this case, both methods can be combined and used to improve the effectiveness of information security. Computer technologies have added a new impetus to the development and improvement of steganography. A new direction in the field of information security appeared - computer steganography [1-8].

Messages are embedded in digital data of an analog nature suc as au dio recordings, images, videos, texts, etc. In computer steganography, a secret message is embedded in a co ntainer, which is a graphic, audio or text file. The most common are graphic and audio files.

Containers can be of different volumes. The larger the container, the more information can be hidden in it. If the container is continuous (streaming), it is impossible to determine its beginning and end. Containers of a limited size limit the amount of the secret message. Here are the types of containers:

1. The container generated by the system itself [9, 10].
2. The container selected from a set of containers.
3. The container comes from outside.

The paper examines and explores the containers represented by graphic files. Typically, in each selected container, image cells are selected. Bits of the cells will be embedded with the bits of the secret message. These bits must be selected in such a way that the observer cannot determine them. The task of this work is to select and create a container and develop an efficient algorithm for selecting the cells of the container image to embed bits of the secret message.

2 Search for an approach for the formation of the necessary container

For successful steganographic protection of digital messages, different approaches are used to design the container. The container is designed in such a way that visual changes of embedding secret bits will not be observed. There are various ways of searching for such

cells (dots or pixels) on the image into which digital message bits are embedded without visible changes in the optical pattern. It is also necessary to take into account the use of mixed encryption, which increases resistance to unauthorized access.

The most common method of steganographic protection is the LSB method [6-8], which implements the replacement of the least significant bits of color bytes with message bits.

One approach is to select areas with the same color. In these areas, a p ointwise encrypted message is embedded in a sm aller (per unit brightness), or greater brightness values. An example of such an image with one area is shown in Fig. 1.

Fig. 1 An example of the embedding of an encrypted message in selected cells.

In the figure, no visual changes are observed. However, statistical analysis of images can easily identify selected cells in the entire image. To decrypt the message received in the container, the recipient must have knowledge that indicates the coordinates of the allocated cells with embedded bits of the secret message, along with the brightness level of the area containing them.

Since the opponent can assume that cells with a different color or brightness can exist on a solid background, an algorithm is used according to which the cells with the selected color are selected and the bits of the message are hidden in them. Such cells can be located in different places of the image. The extraction of such cells is easily accomplished with the help of cellular automata (CA) [11 - 15]. An example of a fragment of a graphic container with cells of the same color that are not located side by side, but form a single group is shown in Fig. 2.

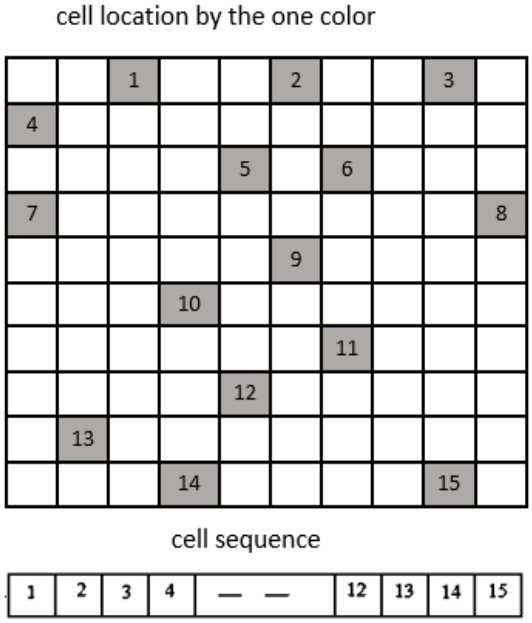

Fig. 2 Example of the distribution of one color cells in a container.

3 The method of extracting image cells for the embedding of message bits

In general, the method of steganographic protection of messages in a g raphic container consists of the following steps.

1. An image is selected as a container (color or grayscale).
2. All the points (cells) of the image are analyzed.
3. The cells of the image, in which you can embed the message according to the chosen algorithm, are selected.
4. The sequence of the selected cells according to the specified sequential search algorithm is indicated.
5. The digital secret message is

encrypted according to the selected algorithm.

6. Bits of the encrypted message are embedded into the selected cells with a given sequence.
7. The received steganogram is sent to the data transfer channel are sent.
8. The cell is extracted from the receiving side according to a predetermined sequential selection algorithm of selected cells.
9. A ciphertext is formed by extracting bits from the codes of the extracted cells.
10. The digital sequence is decrypted; and a secret message is obtained.

The key place in the method under investigation is the method of extraction cells into which bits of the secret digital message are embedded.

To implement such a method, the following actions are performed.

1. A color image is selected as a container.
2. The selected color image is transformed to a grayscale image.
3. The brightness threshold is chosen.
4. A gray image is binarized according to the chosen threshold.
5. Selected cells on a binary image are extracted.

An example of such a preliminary processing on Fig. 3 is shown.

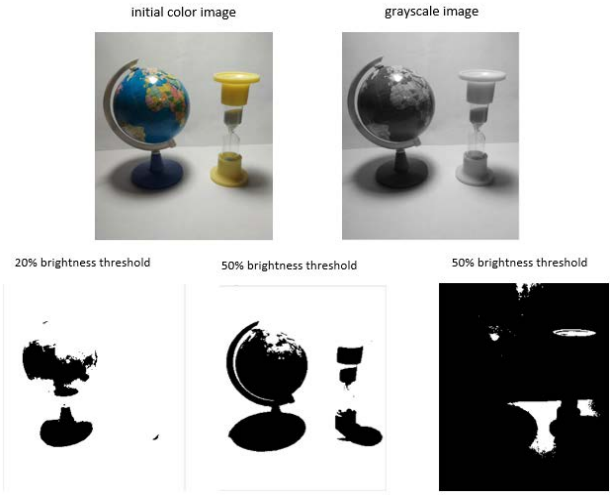

Fig. 3 An example of threshold processing of images for the extraction of isolated cells.

Fig. 3 shows the initial image, which is transformed into a multi-gradation gray image. The results of threshold processing of the resulting gray image are also shown. The threshold was set for different brightness values. For different values of the brightness threshold, there are different numbers of individual white cells inside black fields and isolated black cells on a white background. Having determined the coordinates of such cells, the corresponding bits of the secret message are embedded into the lower digits of the cell codes of the original image or message.

To determine the isolated cells on the opposite background, the theory of CA is used [11-15]. According to the theory of CA, each cell realizes a local transition function. Arguments of this function are the state signals from the neighborhood cell outputs. Each local function is chosen such that it satisfies the final result of the general state of the CA. For our case as a whole, the CA must leave the cells that are isolated on the corresponding background. An example of such a selection is shown in Fig. 4.

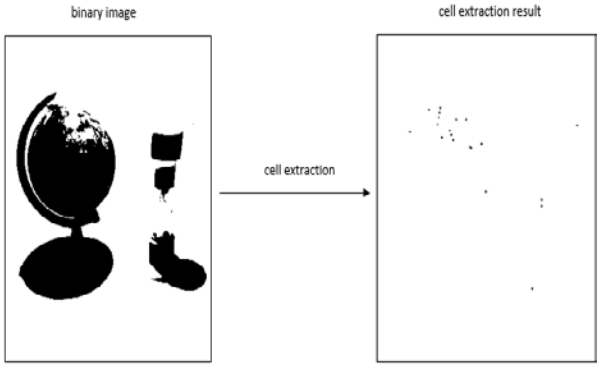

Fig. 4 An example of isolating unit cells of an image.

In the example shown in Fig. 4, a brightness threshold of 50% made it possible to extract 20 isolated cells. For different values of the brightness threshold, the number of extracted unit cells varies.

Each cell of the CA realizes the following logical function:

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

where $b_i(t)$ is the state of a cell at the time t; $x_i(t)$ is the state of the neighboring i-th cell at the time t.

This function implements an algorithm that does not take into account the state of cells located on diagonals with a control cell. An example of the operation of such a CA is shown in Fig. 5. We note that this function realizes the work of the CA in which the von Neumann neighborhood is chosen.

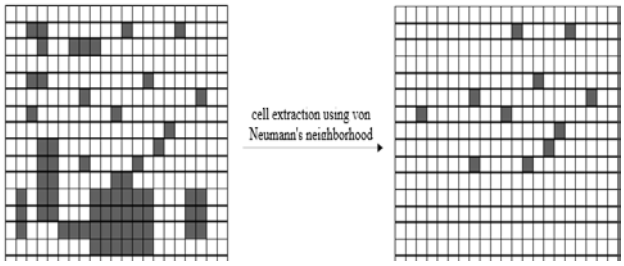

Figure 5 The CA work by the von Neumann neighborhood.

This example reflects the imperfection of using the von Neumann neighborhood for constructing a stegocontainer in construction steganography. On the resulting image, there are cells that are adjacent diagonally. This circumstance does not give completely isolated cells in the CA field. The best way to implement this method is to use Moore's neighborhood, which takes into account the neighborhood of the additional four cells that are located diagonally. According to the Moore neighborhood, each cell performs the following logical function:

$$b_i(t+1)=b_i(t)\wedge\overline{x_1(t)}\wedge\overline{x_2(t)}\wedge\overline{x_3(t)}\wedge\overline{x_4(t)}\wedge\overline{x_5(t)}\wedge\overline{x_6(t)}\wedge\overline{x_7(t)}\wedge\overline{x_8(t)}\vee$$
$$\vee\overline{b_i(t)}\wedge x_1(t)\wedge x_2(t)\wedge x_3(t)\wedge x_4(t)\wedge x_5(t)\wedge x_6(t)\wedge x_7(t)\wedge x_8(t) \quad (2)$$

The use of Moore's neighborhood makes it possible to eliminate the disadvantages of using the von Neumann neighborhood. An example of extracting unit cells in the neighborhood of Moore is shown in Fig. 6.

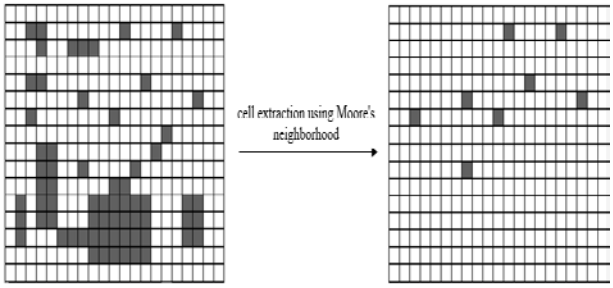

Fig. 6 The result of the work of the SC in extracting unit cells based on the Moore neighborhood.

Using Moore neighborhood makes it possible to completely extract isolated cells. The number of extracted cells is decreased. An example of the change (message bits embedding) of color and brightness when implementing a hidden message is shown in Fig. 7.

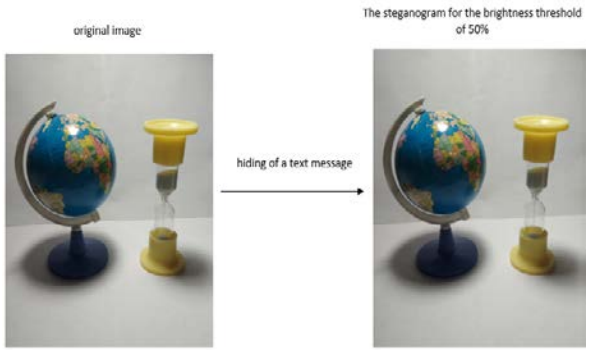

Fig. 7 An example of image changes when embedding a message into extracted cells for a 50% brightness threshold.

Message bits are embedded in 20 cells of image. The image is selected with a size of 300 × 370 with a resolution of 72 pixels / inch. The figure shows that no visual changes occurred. If there are not enough isolated cells in the selected containers, additional noise such as "salt" and "pepper" is introduced into the container. An example of the introduction of noise of this type is shown in Fig. 8.

Fig. 8 An example of the introduction of noise such as "salt" and "pepper".

Noises of this type are present in almost all images; and do not cause much suspicion in humans. For our example, the cells that belong to the noise are highlighted in Fig. 9. We see a different number of cells for different brightness thresholds.

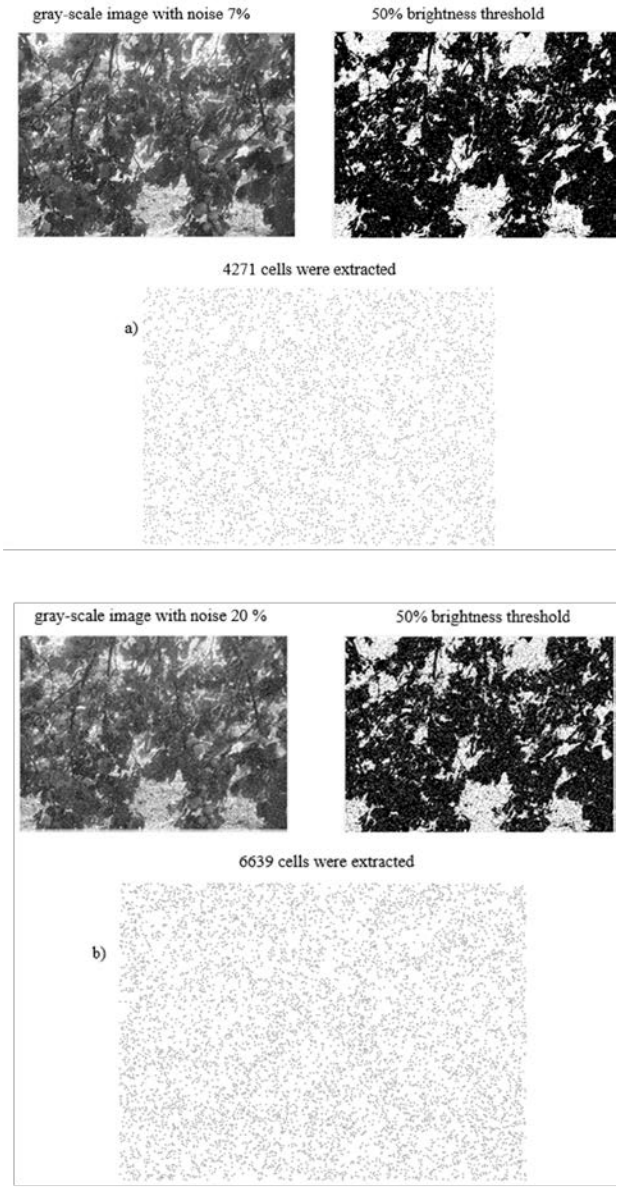

Fig. 9 Example of extracted cells at different brightness thresholds.

The initial image is shown in Fig. 8. In this image, changes are made by noise. Isolated noise cells are identified according to the described algorithm. Noise does not always give a result in percentage since noise cells can be located as adjacent cells.

This approach also does not provide visual changes in the original image since noise cells remain in the image area and are perceived as noise rather than as cells with embedded bits of the digital message. Thus, the use of this algorithm is possible. In this case, the opponent can guess that the bits are embedded in the noise pixels. Using the corresponding analysis can open the embedded message.

To eliminate the possibility of disclosing and detecting an embedded message, an additional bit sequence conversion (encryption) is used. This practically implements streaming encryption. The scheme of such encryption in Fig. 10 is shown.

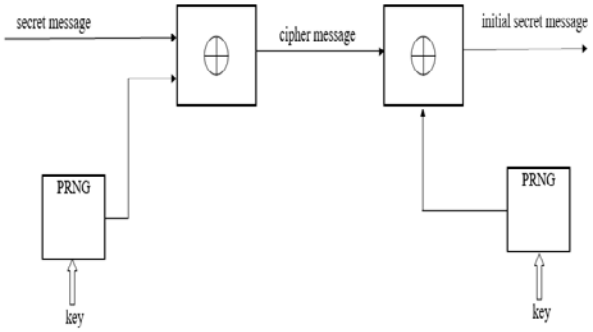

Fig. 10 Scheme for encrypting a secret message.

The main module of such a scheme is a pseudo-random number generator (PRNG), which forms a pseudo-random bit sequence. The resistance to cracking of the received shifrogram depends on the structure and properties of PRNG. The repetition period of the bit sequence is important. The length of the pseudo-random bit sequence limits the length of the embedded secret message. The most effective PRNGs are generators, which are described in detail in the papers [13 - 15]. These PRNGs are implemented on the basis of CA.

It is necessary to carry out random selection of cells. For a complete search of the selected cells, they are distributed in the form of a table in order to increase the coordinates according to the simplest search algorithm. Each filled cell of the table is coded by a corresponding number. Further sequential search of cell addresses is carried out. Such an algorithm can be an algorithm for enumerating every tenth number, then every ninth number, etc. It is also possible to sort through rows or columns and to perform a sequential search.

Consider an example for a small array of cells. The initial array with the extracted cells is shown in Fig. 11.

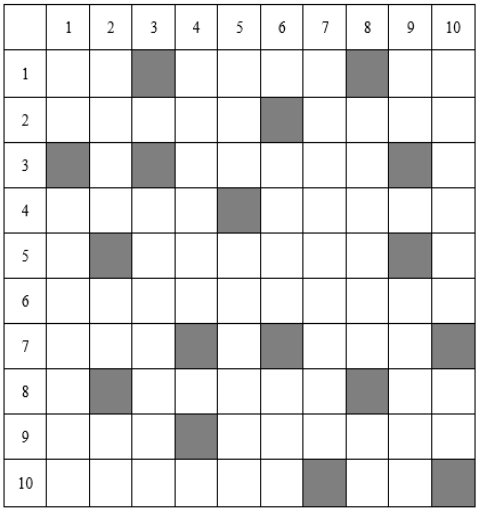

Fig. 11 An example of an array of 10 × 10 with extracted cells.

According to the obtained array (Fig. 11), Table 1 is constructed. The coordinates of the array cells are distributed in it. The last column of Table 1 shows the selection sequence of the extracted cells.

Table 1 Distribution of coordinates of the extracted cells.

№ of cell		Selected number

	X	y	according to the search
1.	1	3	10
2.	2	5	1
3.	2	8	11
4.	3	1	2
5.	3	3	12
6.	4	4	3
7.	4	9	13
8.	5	4	4
9.	6	2	14
10.	6	7	5
11.	7	10	15
12.	8	1	6
13.	8	8	16
14.	9	3	7
15.	9	5	17
16.	10	7	8
17.	10	10	9

Thus, all the moments for the reliable implementation of the method were taken into account. According to these provisions, a general scheme of the method of steganographic protection of messages based on design steganography is constructed (Fig. 12).

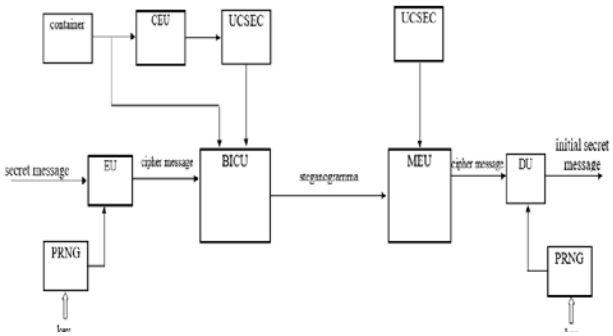

Fig. 12 Structural diagram of steganographic protection of messages based on design steganography.

The circuit is divided into transmitting and receiving parts. The transmitting part is embedded in the secret message. First, the secret message is encrypted with help PRNG and encryption unit (EU). The container is also constructed with the help of cell extraction unit (CEU). The coordinates of the isolated cells are transmitted to unit of consecutive selection of extracted cells (UCSEC). At the output of this unit, a sequence of selection of extracted cells is formed. The bits of the ciphertext are transmitted to the input of the bit introduction into the cell unit (BICU); the second input is transmitted to the container; and the third input is transmitted to the cells. BICU implements the insertion of the ciphertext bits into the least significant bits of the extracted cell codes. At the output of the BICU, a steganogram is formed.

Extraction of a se cret message on the receiving side is carried out in the reverse order. The steganogram is transmitted to the input of message extraction unit (MEU). The UCSEC sequentially determines the cells in which the message bits are embedded. At the output of the MEU, a ciphertext is generated, the bits of which are extracted from the least significant bits of the selected cells. The cryptogram is transmitted to the input of decryption unit (DU), at the output of which the original message is extracted.

Thus, to implement steganographic protection of digital messages, it is necessary for the receiving and transmitting parts to consider the following facts:

1. Encryption key (decryption).
2. Structure and algorithm of PRNG work.
3. The brightness threshold for image binarization.
4. The structure of the CA and the local function of one cell.
5. Selection algorithm of the extracted cells.

Such parameters are very difficult to select by analysts, so the method provides a high degree of protection.

4 Hardware Implementation of the method of constructing a container for creating a steganogram

The hardware implementation of the method of constructing a container gives a high quality for a whole set of indicators. First, the speed of the method is increased due to the use of CA. Since the hardware implementation of methods for the encryption of digital messages is sufficiently developed, the implementation of methods for constructing containers requires extensive attention. The structure that implements the method of constructing the container is shown in Fig. 13.

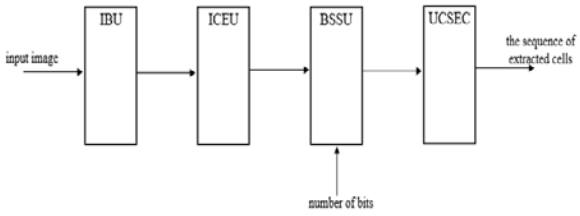

Fig. 13 Structure of the container preparation device.

The device contains an image binarization unit by brightness gradations (IBU), isolated cell extraction unit (ICEU), binary slice selection unit (BSSU) and unit of consecutive selection of extracted cells (UCSEC). Each block in this sequence performs an appropriate function, which indicates its complexity.

At the output of the device, the coordinates of the cells of the initial image of the container are formed and embedded in the bits of the message will be embedded. In the first step, the image is divided into binary slices. Each binary slice is an image consisting of black and white cells, which are obtained by performing threshold processing. An example of partitioning into binary slices is shown in Fig. 14.

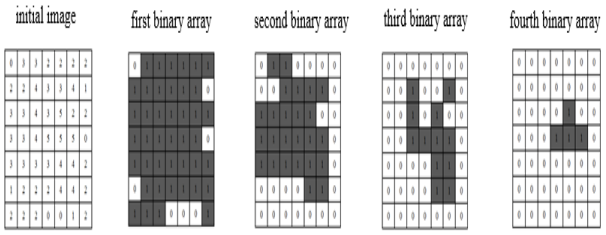

Fig. 14 An example of partitioning an image into binary sections.

ICEU extracts unit cells in each binary array. After extraction, each binary array has a d ifferent number of selected cells. BSSU selects a binary array based on the length of the binary message. UCSEC creates the necessary sequence of selected cells. At the output of UCSEC, a sequence of coordinates is formed in time. According to this sequence, bits of the binary message are embedded in the selected cells. The IBU structure is shown in Fig. 15.

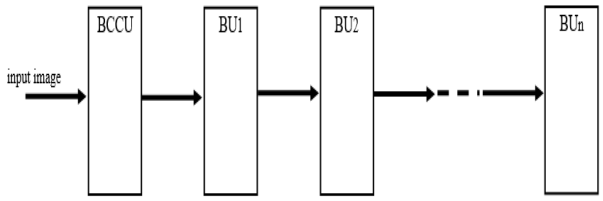

Fig. 15 Structure of the IBU.

The IBU consists of brightness - code conversions unit (BCCU) and n binarization units (BU_i). All the blocks BCCU and BU are cell arrays, which are arranged one by one sequentially. The output of each cell of the previous BU_{i-1} is connected to the input of the corresponding cell of the next BU_i. Each array that is formed in all BE is transmitted at its own BCCU or via a switch.

BCCU is a CA organized by Moore neighborhood. The functional diagram of such a cell is shown in Fig. 16.

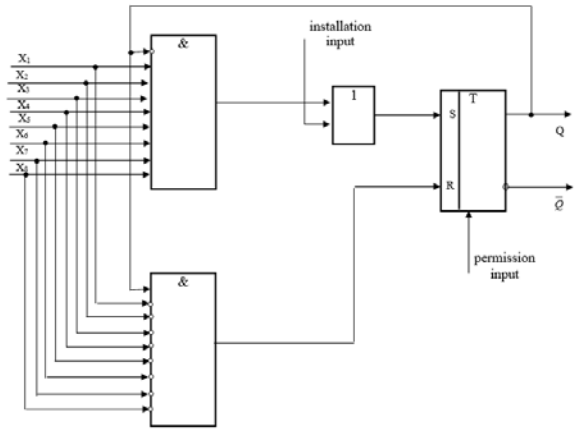

Fig. 16 Functional diagram of the CA cell for extracting unit cells in a binary image.

Fig. 17 shows the time diagrams of cell work obtained in CAD Active-HDL.

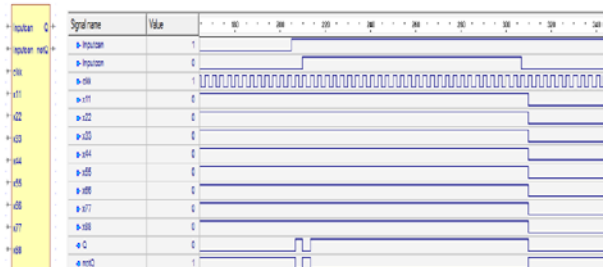

Fig. 17 Time diagrams of cell work obtained in Active-HDL CAD.

5 Conclusion

The paper considers approaches to the formation of containers. An algorithm for extracting image cells for embedding a message bit is presented. The algorithm was considered for extracting unit cells on the selected color background. In this case, the algorithm can be used to extract other cells (not only unit cells). The use of the theory of cellular automata allows you to specify different combinations of extracted cells. The conducted studies show that no visual changes occur after the introduction of the message. The implementation of the pseudo-random bit sequence generator based on cellular automata allows you to select different initial states from the container image. A structure for the extraction of unit cells has been developed and modelled in the Active-HDL environment, which makes it possible to implement the system on modern FPGAs.

References:

[1] Hedieh S. "Recent Advances in Steganography", *InTech;* 2012.
[2] Gregory K. "Investigator's Guide to Steganography", Auerbach; 2003.
[3] Eric C. Hiding in Plain Sight: Steganography and the Art of Covert Communication. Wiley; 2003.
[4] Petitcolas F, Anderson R, Kuhn M. Information Hiding: A survey. *Proceedings of the IEEE*. 1999; 87 (7): 1062–78.
[5] Fridrich J, Goljan M, Soukal D. Searching for the Stego Key. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. 2004. 5306: 70–82. [6] Shilpa G, Geeta G, Neha A. Enhanced Least Significant Bit Algorithm for Image Steganography. IJCEM International Journal of Computational Engineering & Management. 2012. 15 (4): 40-42.
[7] Raja K, Chowdary C, Venugopal K, Patnaik L. A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images. Proc. IEEE. 2005.
[8] Lokeswara V, Reddy S, Reddy C. Implementation of LSB Steganography and its Evaluation for Various File Formats. Int. J. Advanced Networking and Applications. 2011; 02 (05): 868-872.
[9] Sahoo G, Tiwari R. Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization. International Journal of Computer Science and Network Security. 2008; 8 (1): 228-233.
[10] Saha B, Shuchi S. Steganographic Techniques of Data Hiding using Digital Images. Defense Science Journal. 2012; 62 (1): 11-18.
[11] Wolfram S. Cellular automata. Los Alamos Science. 1983. 9 (1), 1983: 2-21.
[12] Stepan B. Models and hardware implementation of methods of Pre-processing Images based on the Cellular Automata. Advances in Image and Video Processing. 2014; 2 (5): 76-90.
[13] Stepan B. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities. IGI Global; 2017.
[14] Stepan B, Mykola B, Ruslan M, Andrii B, Sergii B. Designing of the Pseudorandom Number Generators on the Basis on Two-Dimensional Cellular Automata. Proceedings of the 1st International 62 Conference on Applied Physics, System 63 Science and Computers (APSAC2016). 2016: 137-143.
[15] Stepan B, Mykola B, Sergii B. Research of the method of pseudo-random number generation based on a synchronous cellular automata with several active cells. MATEC Web of Conferences, 2017: 1-6.