IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 14, Issue 5 Ser. II (Sep. – Oct. 2019), PP 06-11
www.iosrjournals.org

A Novel Methods For Image Steganography By Effective Image Points Selection

Nashat Albdour
Department of Communication, Electronics and Computer Engineering
Tafila Technical University P.O.Box 179, Tafila, 66110, JORDAN

Abstract: - *In this paper, a steganographic method for selecting cells of a container image is proposed for efficiently embedding bits of a secret message. Based on the conducted studies, the optimal number of low-order bits was chosen to embedding a secret message. In this case, the cell codes were arranged in descending order (ascending). To increase the volume of the introduced message, it is suggested to introduce noise into the original image and embed additional bits into the codes of the noise cells. Studies were carried out to change the visual characteristics when embedding a secret message into the codes of selected cells. Studies are presented to select noise cells at different thresholds of image binarization with noise, which made it possible to determine the optimal binarization threshold. Based on the research conducted and the results obtained, a scheme of steganography protection of information is built.*

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

Date of Submission: 02-10-2019 Date of Acceptance: 18-10-2019

I. Introduction

Among all the known methods and means of information protection gained wide popularity steganographic methods [1-3]. The peculiarity of steganographic methods is the concealment of the very fact of the existence of a secret message. Increase the degree of information security allows the use of cryptographic methods. Initially, the secret message is encrypted by known methods, and then it is injected into the container using steganographic methods.

As containers, various digital data are used, which can be represented by graphic, audio or text files. Containers come in different volumes. Containers of limited volumes are vulnerable. It is impossible to crack messages of unlimited value embedded in streaming containers. In containers of unlimited size (stream containers), it is difficult to determine the beginning and end of an embedded secret message.

In modern steganography, graphic containers are most often used, which can be generated by the steganographic system itself and can be selected inside the system, as well as those that come from outside.

One of the main tasks of steganography is the task of selecting image cells, in the bits of which will be embedded the bits of the secret message. The cells of the image must be chosen in such a way that the observer cannot identify them from the whole set of cells (pixels) that form the image of the container. In this case, the task is also to select such image cells that do not cause significant visual distortions of the container.

This approach limits the number of pixels used by the image, and therefore limits the length of the secret message. In this connection, the task is to increase the number of used cells, into which bits of the secret message can be embedded. The solution of this problem requires additional studies in the field of visual characteristics of images.

If the container is designed by the user of the system, then the solution of this problem is simplified since the used cells are set initially. If the container is not created but comes from other sources, then the solution of this problem requires searching for optimal approaches and developing new methods for solving it.

In this paper, the task is solved of developing an efficient algorithm for selecting the cells of the container image into which the bits of the secret message are embedded. In this case, the container can come from other sources, and the user can make changes as an additional noise.

II. System Implementation

All methods of computer steganography are based on the embedding or addition of bits of digital messages to binary codes of digital containers. The most popular method is the LSB method [2, 4-6]. This method is based on replacing the lower bits of the pixel codes by the bits of the message. In this case, the embedding in all bits of the container does not always give effective protection. Therefore, the study and search of algorithms for sequential selection of container cells is carried out, for which no visual changes occur. Much attention is paid to the preliminary introduction of such cells into the image [7, 8]. In this case, the container is generated by the system itself.

One of the most effective methods of forming the information cells of a container is to introduce noise (for example, noises like "salt" and "pepper"). Noises of this type are present in almost all images and do not cause suspicion in the observer. An example of an image of a container with added noise in Fig. 1 is shown.

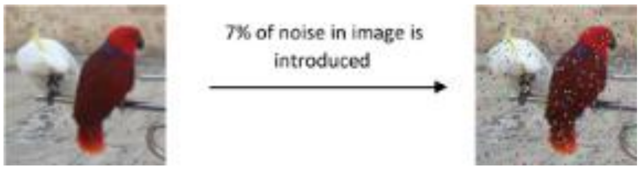


Fig. 1. An example of the introduction of noise (7%) such as "salt" and "pepper" when forming a container.

To select the cells of the image of the container, methods are used that are based on the theoretical foundations of cellular automata (CA) [9-12]. Local logic functions are assigned to each image cell, according to which only noise cells are allocated. For our example (Figure 1), the isolated noise cells in Fig. 2 are shown. Before you select cells, the image is binarized by the specified brightness threshold. In this image, no additional artificial noise was introduced.

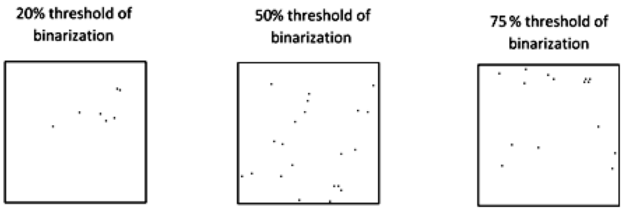


Fig. 2. An example of extracted cells for different brightness thresholds in the image of the container "Parrots".

As can be seen from Fig. 2 the number of cells extracted is different for different brightness thresholds. In this case, different cells are selected for different brightness thresholds. Can be selected cells that do not belong to noise, but belong to the original image. Such cells are isolated from neighboring cells at appropriate brightness thresholds. The embed of a secret message bit into these cells can change the visual characteristics of the container image. However, in the codes of cells belonging to noise, it is possible to embed secret bits not only in the lower order bits. This will not affect the visual characteristics of the container image.

Disadvantages of this method is a small number of image cells, in which secret bits can be embedded. In addition, the method does not give a good result when there is a need to use a container image that came from outside. Especially if one knows about this image. This situation can lead to a problem, which is that the volume of the container is less than the volume of the secret message. To solve the emerging problems, there is a need to search for new methods that make it possible to use almost all cells of the image without changing its visual characteristics.

The investigated method of steganographic protection of messages in a graphic container consists of the following steps.

An image as a container are selected (color or multi-gradation).The codes of all points (cells) of the image are analyzed. The cells from the maximum to the minimum code are enumerated. The cell arrays with equal codes are looking for. The arrays of cells of the first code are selected. The sequence of cell numbering in the selected array (line by line from left to right and from top to bottom) are specified).

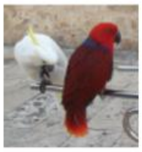
The input image are analyzed. A sequence of writing the ni bits of the message into a selected array of cells are selected. After the selected array of cells is filled, the next cell array is selected in which the code is more one per unit from the previous one.

The following bits of the message are inserted into this array, etc. The recording is performed until the secret message is fully implemented. The received steganogram to the data transfer channel is transferred. The digital sequence and receive a secret message are decrypted.

In accordance with this algorithm, the selected message is embedded in the image codes of the container in ascending order (decreasing) the value of the number represented by the code of each cell. It is important to determine the number of least significant bits of the codes of each cell, which do not give visual image distortions as a result of the introduction of the message bits. Such information can be obtained as a result of experimental studies of the method. In connection with this, an experiment was conducted, which is aimed at determining the image cells into which as many as possible of the bit of the secret message are embedded.

To analyze the method, we used an image of 100 × 100 cells with a resolution of 96 pixels / inch,in Fig. 3 is shown.

Original image



Fragment of the image in the codes

	0										10
0	7440539	7506075	7769504	7242905	7571353	7965340	8624553	8228769	9348023	9414588	993938
	7768217	8033184	8230566	8032931	7900316	8097186	8426662	8360097	8886959	9348795	101372
	9347245	9084845	8361382	9018027	8426914	8163487	8557477	9478834	9676214	9610939	961119
	9874361	9414326	9282741	8625071	8296107	7967396	7901861	7967141	8164006	9216951	921823
	9281970	9084849	9414070	9020084	8691379	8493485	8033192	7638694	7702429	9741233	980779
	9018281	9281196	9018797	9151412	9283259	9283002	8822708	8296364	7571100	9278887	107276
	8426402	8953002	9150382	9545656	9415100	9414587	8822449	7965599	7899807	8884901	107944
	7966369	8163747	8886694	9742521	9546685	9546427	8492711	7702168	8161691	8951463	993989
	7703453	7571355	8360096	9348019	9415868	9546168	8951975	8687515	9674666	10005947	100059
	7901090	8097441	9412779	9940670	9547198	10070969	9609129	10267572	10531261	10203069	104664
	7637918	8097439	9215144	9349047	9481407	10005175	10794428	11189701	10400962	9545909	100714
	7703709	8492453	8558501	8953265	9021116	8953266	10532031	10598594	10269890	9940667	994015
	8492967	8361380	8163230	8623784	8889531	9019829	9480375	9546170	9743803	9743804	101380
	7901342	8230307	8624294	8492710	8626616	9085621	9939898	10203325	10071741	9415610	888772
	8361381	8033186	8163230	8492454	8692151	8756912	9808051	9742774	8953519	8164517	770294
	8096927	8097695	7965078	9215400	8690606	9085106	8886950	9216944	8427431	7901087	790057
	8624038	7767961	8556959	9478572	8755624	8690348	9346732	8623265	8361123	8294817	849168
	7570842	8360357	8821678	8491942	8622756	8954033	8557990	9544111	9347246	8294300	829455
	7967145	8756399	9347504	9018539	9018023	8492708	9150379	9610416	9611702	9020083	856004
	8953523	8953004	9675952	8624293	8754854	8623270	8622754	9149865	9346733	9084335	901957
	9084848	8756139	9215149	8426146	8754856	8557991	8820648	8953003	8360614	8557732	921540
	8953006	8756141	8689573	8755367	8360353	8492455	8952749	8426662	7570585	8820391	888669
	8360354	8755625	8030616	8425887	8623525	8492711	8229026	8426661	8229025	8558246	836035
23	7964824	8624038	8819613	9478569	8755364	8360352	8096924	7965338	7900317	7373976	803139

Fig. 3. The original image of "Parrots".

The color and brightness of each image cell is determined by a 24-bit binary code (3 bytes). As a result of the analysis, it was determined that 10,000 codes are used to represent the Parrot's control image (the minimum value corresponds to 987961, the maximum value is 16709610). Different codes used only 7700. The remaining codes formed groups with the same codes.A fragment of the binary code that was embedded in the container represented by the image of "Parrots" is shown in Fig. 4.

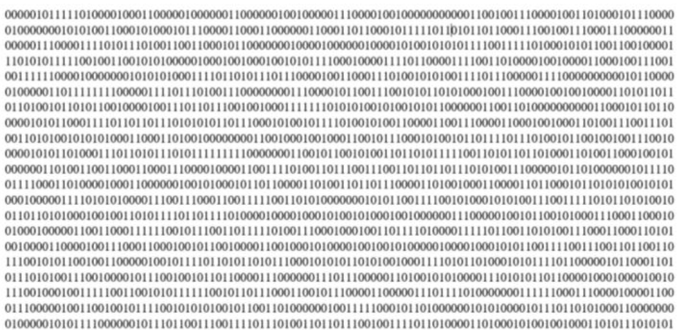


Fig. 4. Example of a message fragment represented by a binary code.

For insertion into the least significant bits (one least significant digit) of the container, 10,000 bits are used from the message. The more junior bits are allocated to the introduction of message bits, the more message volume can be embedded in the container. The secret message was embedded in one low-order bit, two low-order bits, three low-order bits, etc., of all the cells in the container. The image of "Parrots" (Figure 3) with an embedded message (Figure 4) for a different number of low-order bits is shown in Fig. 5.

Fig. 5. Images of "Parrots" with the embedded message in a different number of low-order bits.

As a result of the visual analysis, noticeable differences from the initial one begin with the container, in which more than 3 minor bits of cells are amended. The result indicates that a message can be inserted into the selected container with a length of 30000 bits without changing the visual characteristics. Fragments of images of "Parrots" measuring 10 × 10 with embedded messages (Figure 5) in Fig. 6 are shown.

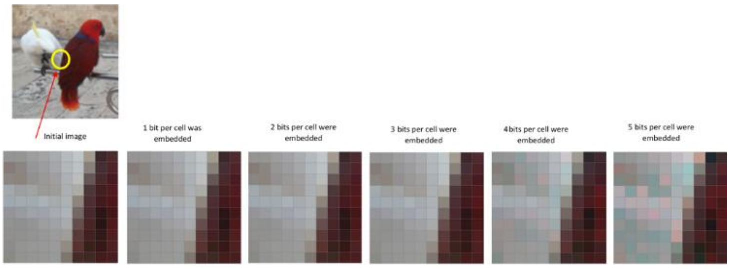


Fig. 6. Fragments of images "Parrots" size 10 × 10 with embedded messages in a different number of low-order bits of code for each cell.

Increased fragments of images with embedded messages do not display visual changes, in cases of changes 1, 2, 3 lower bits of codes in each cell.Thus, in a container image of 100 × 100 cells we can inject 30,000 bits of a secret message without significant visual changes. To increase the volume of a secret message, you can use a larger container. In this case, the visual picture of the image changes, and the volume of the graphic image is increased.

There are tasks in which it is necessary to use the same container image without increasing its size and memory size. In such situations it is necessary to look for such cells of the container image in which more bits of the secret message can be embedded. As such cells can be used cells that make cells of noise such as "salt" and "pepper" [13, 14]. These cells can be extracted using the theory of cellular automata [9, 10]. For this, the necessary local function of the state of the cell is given, with the help of which all the neighborhood cells are analyzed. Additional bits can be embedded in noise cells beginning with the 4th bit. In addition to the three embedded bits in the least significant bits, it is also possible to embed more of the message bits into the noise cell codes. At the same time there are no visual changes in the container.

The number of additional cells for embedding additional bits can be increased in several ways. The first way is to increase the percentage of noise. However, it greatly distorts the image. The second way is based on the choice of the necessary brightness threshold for image binarization in the noise cells extraction algorithm. Since the increase in noise cells does not satisfy the desired requirements, the studies were carried out for the second variant of increasing the information cells.

In the initial image of the container, noise such as "salt" and "pepper" was introduced. The studies were carried out for brightness thresholds of 20%, 50%, and 75%. For each threshold, a different number of cells are extracted. The greatest number of cells was obtained for the binarization threshold of 50%. For the initial image without embedded noise, 21 cells were extracted for the binarization threshold of 50%. In this case, the situation was taken into account when messages were embedded into the code of each cell in the three least significant bits.

Initially, the message to the three least significant bits of the code of each cell was introduced into the initial image of the Parrot on the algorithm described above, and this image was used as the initial one in the experiment. In the container with the embedded message, cells were extracted for the specified brightness thresholds. For the 20% threshold, 73 cells were highlighted, for the 50% threshold - 214 cells and for 75% of the threshold - 91 cells were highlighted. In the codes of the selected cells 3, 4, 5, ..., 10 bits of the additional message are embedded. Since the bits of the message are already embedded in the three least significant bits of the codes of each cell in the container, the bits of the additional message were embedded in the codes of the selected cells starting from the 4th lower order (Fig. 7).

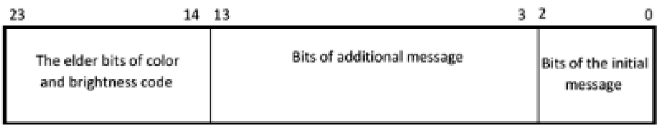


Fig. 7. Format of the fields of the code of the selected cell with embedded bits of the initial and additional message.

The code for the additional message was divided into groups of 3, 4, 5, 6, ..., 10 and embedded in the codes of the selected cells. The results of embedding the additional message code in Fig. 8 are shown.

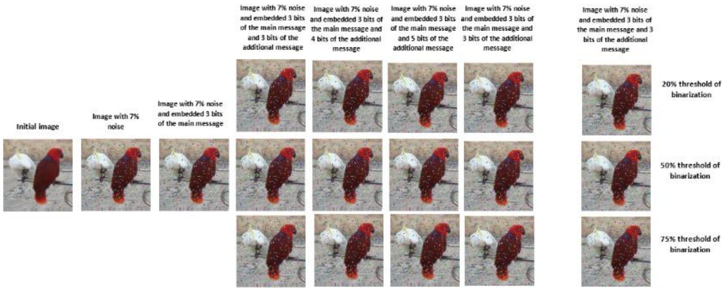


Fig. 8. The image of "Parrots" with embedded three bits in the lower bits of each cell code and with a different number of bits of embedded additional message.

The results show that the number of embedded bits in the noise cells does not result in significant visual distortions. In this example, 30000 bits of the main message and 2140 bits of the additional message was embedded.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. To eliminate the possibility of disclosing and detecting an embedded message, an additional bit sequence conversion (encryption) is used which practically implements streaming encryption [15].

The device for forming the key gamma is a pseudorandom bit sequence generator (PRNG). PRNG, which form a key gamma of a long length, allow you to embed large amounts of messages and are most resistant to unauthorized intervention. The most effective PRNG are generators, which are described in detail in the works [11, 12, 15, 16]. These PRNGs are implemented on the basis of CA and give a key gamut of high quality.

III. Developed system

According to these provisions, a general scheme of the method of steganographic protection of messages based on design steganography is constructed (Fig. 9).

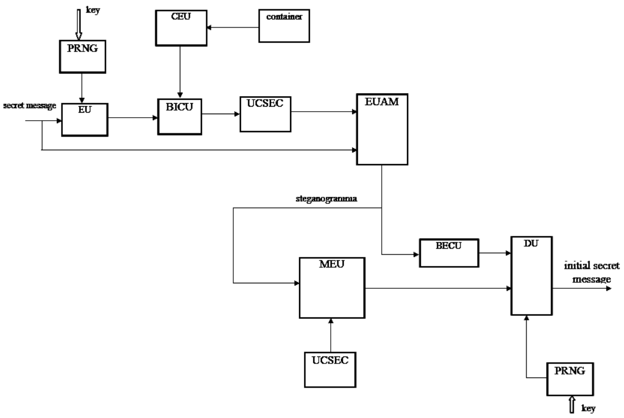


Fig. 9. Structural diagram of steganographic protection of messages based on design steganography.

The circuit is divided into transmitting and receiving parts. The transmitting part embeds the secret message. First, the secret message is encrypted based on PRNG and encryption unit (EU). The container is also designed using a cell extraction unit (CEU). At this stage, noise cells are embedded into the image of the initial container. The ciphertext bits are came to the bit introduction into the cell unit (BICU), and at the second input is came with a constructed container. BICU analyzes the codes of the cells of the container and arranges them in ascending order (decreasing). According to the proposed algorithm, BICU embedes three bits of the input message into the three least significant bits of the codes of all the cells in the container image.

In the unit of consecutive selection of the extracted cells (UCSEC), the binarization threshold is set and cells that are isolated in the image field. The coordinates of the selected cells are came to the input of the embedded unit of the additional message (EUAM). At the output of this block, a steganogram is formed, which is came into the transmission channel.

Extraction of a secret message on the receiving side is carried out in the reverse order. The steganogram is came to the input message extraction unit (MEU). The UCSEC sequentially determines the cells into which the bits of the additional message are embedded. At the MEU output, a ciphertext is generated, the bits of which are taken from the bits of the extracted cells beginning with the 4th LSB of the code. The cipher message is came to the additional input decryption unit (DU), at the output of which the initial additional message is extracted. At the same time, the steganogram enters at the input of the bit extraction cell unit (BECU), which performs a sequential search of cells, extracts from the codes of these cells the three least significant bits of the cipheredgram and generates it at the output. The received cipher message of the main original secret message is received at the main input DU. The DU output generates the main and additional messages.

In fact, the primary and secondary messages represent one whole secret message. During the implementation, it is divided into two. The additional message begins after the insertion of the initial message into the cells of the entire container, per three bits into each cell.To perform steganographic protection of digital messages, it is necessary that both the receiving and transmitting parts know the following data. The encryption key (decryption), which specifies the initialization vector PRNG. Structure and algorithm of work of PRNG.Brightness threshold for image binarization.

Local function of one cell of the CA to select cells in the container image.Algorithm for sorting out selected cells (Algorithm of cell distribution by code size). The number of additional bits for the embedding of bits of additional messages into extracted cells.Such parameters constitute a large data set, which is very difficult to select by analyst, so the method provides a high degree of protection.

IV. Conclusion

The paper presents an experimental technique for determining cells into which the maximum number of bits of a secret message can be embedded. An algorithm is proposed that determines the sequence of cells and the number of least significant bits of the message embedding injected in each cell. Also, an algorithm for embedding a bit of an additional message was proposal. The proposed algorithms and the conducted experiment allowed to increase the volume of the embedded secret message without changing the volume of the image of the container. The use of the theory of cellular automata allows you to specify different combinations of isolated cells. The conducted studies show that visual changes do not occur after the insertion of the message into the three least significant bits of the code of each cell of the container image. The introduction of noise into the image of the container allowed to increase the volume of the embedded message. The optimum binarization threshold is also determined, in which the number of additional embedded bits is maximally.

References

[1]. Recent Advances in Steganography. Edited by Hedieh Sajedi, ISBN 978-953-51-0840-5, 100 pages, Publisher: InTech, Chapters published November 07, 2012

[2]. Gregory Kipper. Investigator's Guide to Steganography. – 2003.- Auerbach Publications.- 240 pages.

[3]. Eric Cole. Hiding in Plain Sight: Steganography and the Art of Covert Communication.- 2003.- Wiley.- 360 pages.

[4]. V. Lokeswara Reddy, Dr.A.Subramanyam, Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, - 2011. - P. 868-872.

[5]. Shilpa Gupta, Geeta Gujral and Neha Aggarwal. Enhanced Least Significant Bit algorithm For Image Steganography.// IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 – P. 40-42.

[6]. K.B.Raja, C.R.Chowdary, Venugopal K R, and L.M.Patnaik," A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" Department of Computer Science Engineering, Bangalore 2005 IEEE.

[7]. G. Sahoo and R. K. Tiwari. Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization.- IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008.- P. 228-233.

[8]. Babloo Saha and Shuchi Sharma. Steganographic Techniques of Data Hiding using Digital Images.- Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18.

[9]. Wolfram S., Cellular automata. Los Alamos Science, Vol. 9, 1983, pp. 2-21.

[10]. Stepan Bilan. Models and hardware implementation of methods of Pre-processing Images based on the Cellular Automata.- Advances in Image and Video Processing, Vol 2, No 5 (2014), P. 76-90, ISSN 2054-7412, DOI: 10.14738/aivp.25.561, URL: http://dx.doi.org/10.14738/aivp.25.561.

[11]. Stepan Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities.- (2017).- IGI Global, USA.- P. 301. https://www.igi

[12]. global.com/book/formation-methods-models-hardware-implementation/178719.

[13]. Stepan Bilan, Mykola Bilan, Sergii Bilan. Research of the method of pseudo-random number generation based on asynchronous cellular automata with several active cells.- MATEC Web of Conferences, - Vol. 125,- 02018 (2017), - P. 1-6. https://www.matec-conferences.org/articles/matecconf/pdf/2017/39/matecconf_cscc2017_02018.pdf

[14]. S. Bilan and S. Yuzhakov, Image Processing and Pattern Recognition Based on Parallel Shift Technology, CRC Press, 2018.

[15]. S. Belan, and S.Yuzhakov, Machine Vision System Based on the Parallel Shift Technology and Multiple Image Analysis, Computer and Information Science, Vol. 6, No 4, Published by Canadian Center of Science and Education, 2013, pp. 115-124.

[16]. B. Schneier, Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C, Wiley Computer Publishing, John Wiley & Sons, Inc,. 784 (1996).

[17]. Stepan Bilan, Mykola Bilan, Ruslan Motornyuk, Andrii Bilan and Sergii Bilan. Designing of the Pseudorandom Number Generators on the Basis on Two-Dimensional Cellular Automata.- Applied Physics, System 60 Science and Computers. Proceedings of the 1st International 62 Conference on Applied Physics, System 63 Science and Computers (APSAC2016), 64 September 28–30, Dubrovnik, Croatia. Lecture Notes in Electrical Engineering. Volume 428. Springer International Publishing AG, P. 137-143. DOI 10.1007/978-3-319-53934-8_3. https://www.springerprofessional.de/en/designing-of-the-pseudorandom-number-generators-on-the-basis-of-/13318374.