Method of Applying (t,n)-Threshold Scheme in Steganography

Anton N. Mironenko, Mikhail D. Velichko
Computer Sciences Faculty
Dostoevsky Omsk State University
Omsk, Russia
MironenkoAN@omsu.ru; mihailvelichko23@gmail.com

***Abstract*—This work is devoted to the development of the method of information concealment, in the raster image using steganography together with cryptography the solving the problem of recovering a message if the image which contains hidden data is damaged. It proposes a method of implementing the steganography for insert data on digital image not in its entirety, but previously using (t, n)-threshold scheme and inserting each of the parts received independently. The software was developed for approbation of the proposed method. A series of experiments confirming the possibility of applying the proposed method was carried out. Text information is inserted into the raster image. Further, the image was subjected to modification, simulates container damage when it was transmitted through the communication channel or as a result of intentional actions of an intruder. As a result of the experiments, it can be said about the possibility of applying the proposed method.**

***Keywords*— cryptography; secret sharing; stegnographic inser; raster image; data concealing; increased reliability; LSB .**

I. Introduction

The issue of maintaining and ensuring the confidentiality of information is relevant. The software, allowing transferring data securely, is encrypted. If an open channel is used, a man in the middle (MITM) attack is possible, and the attacker, if not able to decrypt the data, may violate their integrity. The solution to this problem can be the use of steganography, i.e. concealment of the fact of the transfer of classified information. A lot of scientific works are devoted to this topic, for example [1-4].

The article [5] discusses the main trends in steganography.

The [6] paper introduces work on developing secure data communication system. It includes the usage of two algorithms RSA and AES used for achieving cryptography along with LSB for achieving steganography both on Android platform. The joining of these three algorithms helps in building a secured communication system on ‘Android’ platform which is capable of withstanding multiple threats.

In [7] proposed steganography system of information protection on the basis of the proposed original algorithm for embedding information with overlapping blocks of images in rows and columns. It is shown that this steganography system retains its resistance to passive stegoanalytic attacks with block overlapping up to 24x24 pixels and at this overlap value is more stable than the standard and improved steganography method based on direct spreading of the spectrum.

In the article [8] the author proposes a new steganography method based on the compression standard according to the Joint Photographic Expert Group and an Entropy Thresholding technique. The algorithm uses a pair of keys: public and private, to generate a pseudo-random sequence that indicates where the secret information will be embedded. The insertion takes eventually place at the first seven AC coefficients in the transformed DCT domain. Before the insertion of the message the image undergoes several transformations. After the insertion the inverse transformations are applied in reverse order to the original transformations. The insertion itself takes only place if an entropy threshold of the corresponding block is satisfied and if the pseudorandom number indicates to do so.

In steganography, the following problems can be distinguished:

1. detection of a steganography inserts (stegoanalysis);

2. reliability of information concealment during its transmission.

The first problem is solved in [9].

The solution of the second problem is proposed in [10], in this work studying focuses on integrating schemes like OFDM, CDMA and MC-CDMA with steganography and image encryption techniques to develop wireless systems with inbuilt information security feature.

In the article [11] the authors consider the method of unifying cryptography and steganography. Encryption is performed on images with subsequent embedding of secret data

This work is also devoted to the problem of increasing the reliability of information hiding when it is transmitted, i.e. the task of restoring information in case the image which contains hidden data is damaged (image-container).

Consider the possibility of combining the steganography method and the (t, n)-threshold scheme. The analysis of existing steganography algorithms and threshold schemes is carried out.

II. Statement of the Problem and Its Solution

We will analyze the existing methods of steganography and find which one is most suitable.

Next, we will consider algorithms for embedding information in the part of the original image. The advantage of these algorithms is that for implementation, you do not need to perform complex linear transformations of the image. Information will be introduced by manipulating the brightness or the color components of the image.

1. Kutter's algorithm.

In this algorithm, the information will be embedded in the blue channel because the changes in this color are less visible to the human eye. A pseudo-random position is selected in the image into which the information will be inserted and further into the blue channel. This information is introduced by modifying the brightness.

In work [12], the possibility of using the steganographic method Kutter-Jordan-Bossen allowing hiding the information of the video sequence is considered. In addition, the criterion for selecting a container image is proposed in the work.

2. Langelaar's algorithm.

This algorithm works with blocks of 8x8 pixels from the original image. Initially, a pseudo-random mask of 8x8 pixels is created, consisting of zeros and ones. At the first stage, each block is divided into a pair of subblocks, depending on the value of the mask. Then, for each of them, the average brightness value is calculated. At the second stage, some arbitrary threshold is selected, after which the embedded information bit will be built in the following way: 1 is written if the difference between the average brightness values is greater than the selected threshold; 0 is written if the difference between the average brightness values is less than the selected threshold. If this condition is not met, the changes will occur in the pixel values of the second subblock.

3. Rongen's algorithm.

The embedded information is a two-dimensional matrix, which consists of ones and zeros. Their number is almost equal to each other. On the basis of some characteristic function, computed locally in the course of analyzing neighboring pixels, those pixels in which information can be embedded are recognized. The number of these pixels is about 0.01 of the total number, so not all units will be embedded in these pixels. To increase the number of these pixels initially proposed to carry out a slight distortion of the image.

4. Least significant bit (LSB).

The essence of this method is that the least significant bit of the image carries in itself the least information. When you change them to the bits of the hidden message, the difference from the original object is almost insignificant for human perception. This method allows you to embed large amounts of information, which is a significant plus, as well as it is easy to implement [13-15].

In this article [16] the authors proposed method divides the cover image into some m×n blocks and partitions the binary secret data into some vectors with the length of m*n. For each block, one Hamiltonian path is first found such that the LSB of pixels of the block along this path have the maximum similarity to the corresponding vector of data. Then this part of data is embedded into the first LSB of pixels of the block along the best path using the modified LSB matching and the code of this path is embedded into the second LSB of the pixels using a novel method such that the minimum MSE value between the block of the cover image and the block of the stego-image is achieved.

After analyzing known methods of data concealment in raster images to achieve the goal and studying works [17-18], it was decided to use the LSB method, which was suitable for describing the problem, since it splits the image into parts and then records the information in them.

We analyze the existing threshold schemes.

1. Shamir's secret sharing scheme [19].

Briefly, this algorithm can be described as follows. Let a finite field G be given. We fix n different non-zero non-secret elements of this field. Each of these elements is assigned to a certain member of the group. Next, an arbitrary set of t elements of the field G from which the polynomial f (x) is composed over the G field of degree t-1, $1<t\leq n$. After obtaining the polynomial, we calculate its value at non-secret points and report the results to the corresponding members of the group.

To restore the secret, you can use the interpolation formula, for example, the Lagrange formula.

2. Blackley's scheme.

The secrets to be solved in the Blackley's scheme are one of the coordinates of a point in an m-dimensional space. The shares of secret, distributed to the sides, are the equations of (m-1) -dimensional hyperplanes. To restore the point, it is necessary to know the m equations of hyperplanes. Less than m sides cannot recover the secret, since the intersection set of m-1 planes is straight, and the secret cannot be recovered.

3. Secret sharing using the Chinese remainder theorem (Mignotte's threshold secret sharing scheme, Asmuth-Bloom's threshold secret sharing scheme).

For a certain number (in Mignotte's scheme this is the secret itself, in the Asmuth-Bloom's scheme-some derived number), the remainders from dividing by the sequence of numbers that are distributed to the sides are calculated. Due to the restrictions on the sequence of numbers, only a certain number of sides can restore the secret.

For the further analysis, two schemes were chosen: 1 and 3.

The Blackley's scheme was not included in the analysis because it is less effective than Shamir's scheme: in the Shamir's scheme, each share is the same size as the secret, and in the Blackley's scheme, each share is t times larger.

The results of comparison schemes are presented in the Table 1. The Shamir's secret sharing scheme was chosen.

TABLE I. RESULTS OF THE EXPERIMEN

	t=5,n=3, |M|=512	**t=n=32, |M|=512**	**t=n=128, |M|=512**
Shamir's secret sharing scheme			
• **Secret separation time:** • **Secret recovery time:** • **Amount of memory required:**	5 ms 1 ms 1560 byte	7 ms 2 ms 6720 byte	75 ms 27 ms 100608 byte
Asmuth-Bloom's threshold secret sharing scheme			
• **Secret separation time:** • **Secret recovery time:** • **Amount of memory required:**	130 ms 1 ms 3456 byte	1145 ms 4 ms 274432 byte	3032 ms 97 ms 4243456 byte

The idea of the proposed method is to combine the steganography method LSB with the (t, n) -threshold scheme, which allows for damage to the stack container to n-t parts, where t≤n and n - is the total number of shares of the secret, and t - is the minimum number of shares of the secret for its successful recovery, all the same ensure a reliable recovery of secret.

The proposed approach can be described in two stages:

1. embedding information in the image container (Fig. 2);

2. information recovery (Fig. 1).

The embedded information is processed according to the selected (t, n) -threshold scheme, i.e. secret shares are formed.

The original image into which the insert will be inserted is divided into n parts in width, according to the secretion (t, n) - threshold scheme used to form the shares of the secret. Further, each of the obtained parts is considered as an independent image. The image is represented as an array of bits in which for each of the colors of the pixel is encoded with 8 bits. Write the secret by making changes to the low-order bits. The first pixel of the image will record the length of the secret part, and the next part of the secret itself. Such changes will occur with all n blocks. After finishing the embedding procedure, the image-container is formed from n parts that already contain the secret parts.

To retrieve information, you need to know the number of parts to which the original image and its length were divided.

Next, from each of the parts of the container image, the first pixel is read, and the presence of the length record of the secret portion from the hidden message is checked. If such information is present, then the secret share is read. Then checksums are checked. They will be counted again from each part of the image and will be compared to those that were recorded in the file. In case of their coincidence, the share of the secret will be written into the array, which will be transferred to the input of the secret recovery function.

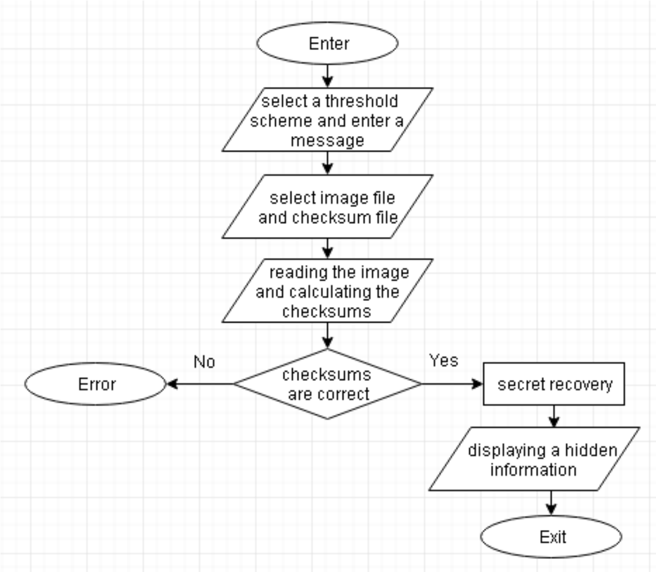
Enter
select a threshold scheme and enter a message
select image file and checksum file
reading the image and calculating the checksums
checksums are correct
No
Error
Yes
secret recovery
displaying a hidden information
Exit

Fig. 1. Block scheme for recovery of information

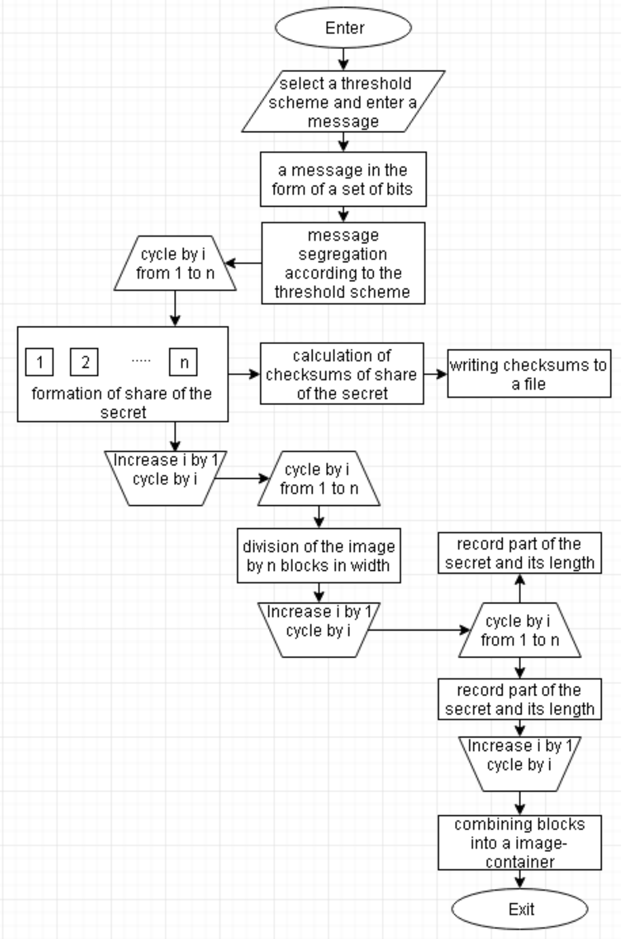
Enter
select a threshold scheme and enter a message
a message in the form of a set of bits
message segregation according to the threshold scheme
cycle by i from 1 to n
1
2
.....
n
formation of share of the secret
calculation of checksums of share of the secret
writing checksums to a file
Increase i by 1 cycle by i
cycle by i from 1 to n
division of the image by n blocks in width
Increase i by 1 cycle by i
record part of the secret and its length
cycle by i from 1 to n
record part of the secret and its length
Increase i by 1 cycle by i
combining blocks into a image-container
Exit

Fig. 2. Block scheme for embedding information.

III. APPROBATION

To approbate the proposed method, a C # program was implemented. As a (t, n) -threshold scheme, the Shamir's secret sharing scheme [19] was chosen.

Block scheme of the program can be seen in Figures 3, 4.

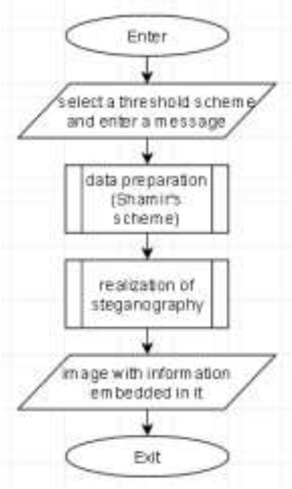
Enter
select a threshold scheme and enter a message
data preparation (Shamir's scheme)
realization of steganography
image with information embedded in it
Exit

Fig. 3. Block scheme of program operation (embedding information).

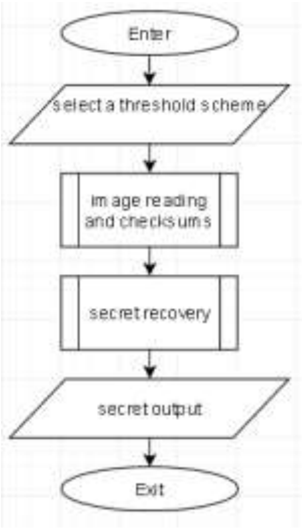

Fig. 4. Block scheme of program operation (secret recovery).

A set of experiments were carried out. For a greater probability of recovering a secret, it is best to choose as small as possible t, and n as much as possible. In the first experiment, the values were chosen 4 and 10, respectively. As the embedded information, the phrase "Тестирование программы!!!".

The information was embedded in Fig. 5.

Fig. 5. Original image.

After cutting the image-container by ~ 30%, in order to simulate damage or attack, the original message was restored. If the container is damaged by more than 60%, it will be impossible to restore the secret. Improve the results by decreasing the threshold or increasing the number of parts.

Then experiments were conducted in which various changes were made to the image-container, imitating damage to the container during transmission or deliberately assigning it to an attacker: imposing "noise", cutting out a part of the picture, imposition of extraneous images.

In cases where the image was damaged by cutting out its part or imposing foreign images (Fig. 7), the experiments were successful, i.e. the image was restored, if the damage is less than 60% of the container.

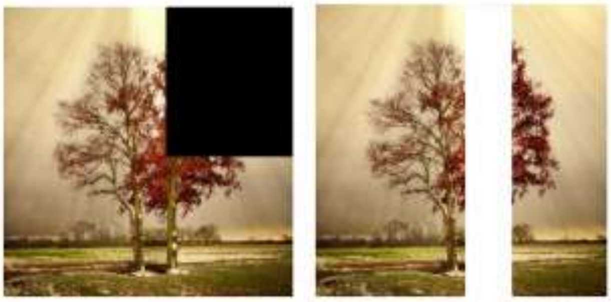

Fig. 6. Damage to the image-container.

In experiments, when the damage was done by applying "noise", the results were worse. The result is presented in Table 2, where "+" - it was possible to restore the information, "-" - it was not possible to recover the information.

TABLE II. RESULTS OF THE EXPERIMEN

(t, n) - threshold scheme **the level of "noise" (%)**	**(3,10)**	**(6,10)**	**(8,10)**	**(10,100)**
0,05	+	+	+	+
0,10	+	+	+	+
0,15-0,19	+	+	+	+
0,2	-	-	-	-

Overcoming the threshold of 0.2% noise, the message was not restored when selecting any threshold scheme. This meant that the maximum Gaussian noise that could be applied and the message could be recovered was 0.19%. Significantly improve the results can be by selecting the shares to restore information for a particular algorithm. The task of finding the algorithm for choosing the shares was not set in this paper. It was necessary to test the hypothesis of the possibility of combining the steganography method LSB with the (t, n) -threshold scheme. The search for a choice algorithm for shares can be a direction for further work on this topic.

IV. Conclusion

The work presented a method that solves one of the problems of steganography, namely, increasing the reliability of information hiding during its transmission, as well as increasing the resistance to attacks aimed at corrupting the image-container. The essence of the method consists in combining the steganography method LSB and (t, n) -threshold scheme. The software was developed and approbated. As a (t, n) -threshold scheme, the Shamir's secret sharing scheme was chosen. A set of experiments was carried out: a steganography insertion of the text was made to the original image. Then the image-container was modified, thereby simulating damage during transmission or deliberate actions by the attacker. During the experiments it was revealed that:

1. In case of damage by imposition of an extraneous image or by deleting part of the image-container, the threshold for successful recovery of the embedded information is 60%;

2. In case of damage to the image-container by imposing "noise", the threshold of successful recovery is 0, 19%.

The low threshold of successful recovery when the container is damaged by superimposing "noise" is explained by the unsuccessful choice of the sampling scheme of shares for recovery. In general, we can talk about the possibility of applying the proposed method to improve the reliability of information concealment during its transmission or damage to the container.

References

1. Al-Afandy K., Faragallah O., Elmhalawy A. High security data hiding using image cropping and LSB least significant bit steganography. Information Science and Technology (CiSt), 2016 4th IEEE International Colloquium on, 24-26 Oct. 2016. DOI: https://doi.org/10.1109/CIST.2016.7805079

2.Chitradevi B., Thinaharan N., Vasanthi M. Data Hiding Using Least Significant Bit Steganography in Digital Images. 2017. DOI: http://doi.org/10.5281/zenodo.262996

3. Al-Dmour H, Al-Ani A, Nguyen H. An efficient steganography method for hiding patient confidential information. Conf Proc IEEE Eng Med Biol Soc. 2014; 2014:222-5. DOI: https://doi.org/10.1109/EMBC.2014.6943569

4. Kaur S., Bansal S., Bansal R.K. Steganography and classification of image steganography techniques. Computing for Sustainable Global Development (INDIACom), 2014 International Conference on, 5-7 March 2014. DOI: https://doi.org/10.1109/IndiaCom.2014.6828087

5. E. Zielinska, W. Mazurczyk and K. Szczypiorski, “Trends in Steganography,” Communications of the ACM, no. 03, issue 57, 2014, pp. 86–95. DOI: http://dx.doi.org/10.1145/2566590.2566610

6. Kandul A., More A., Davalbhakta O., Artamwar R., Kulkarni D. (2015) Steganography with Cryptography in Android. In: Satapathy S., Biswal B., Udgata S., Mandal J. (eds) Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Advances in Intelligent Systems and Computing, vol 328. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-12012-6_7

7. Baltaev R.H., Lunegov I.V. Algoritm vstraivanija i izvlechenija informacii v nepodvizhnye cifrovye izobrazhenija stojkij k passivnym stegoanaliticheskim atakam . Voprosy bezopasnosti., 2016, no. 6, pp. 24-35. DOI: https://doi.org/10.7256/2409-7543.2016.6.21252. Available at: http://e-notabene.ru/nb/article_21252.html (accessed 10 January 2018) (in Russian).

8. Soria-Lorente A., Berres S. A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information. Security and Communication Networks Volume 2017 (2017), Article ID 5397082, 14 p. https://doi.org/10.1155/2017/5397082

9. Belim S. V., Vilkhovskiy D. E. Usage of analytic hierarchy process for steganographic inserts detection in images. Dynamics of Systems, Mechanisms and Machines (Dynamics), 2016. 15-17 Nov. 2016. DOI: https://doi.org/10.1109/Dynamics.2016.7818977

10. Padmapriya Praveenkumar, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan, 2017. Inbuilt Image Encryption and Steganography Security Solutions for Wireless Systems: A Survey. Research Journal of Information Technology, 9: 46-63. DOI: http://dx.doi.org/10.3923/rjit.2017.46.63

11. Padmapriya Praveenkumar, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan, 2014. Cryptic Cover for Covered Writing: A Pre-Layered Stego. Information Technology Journal, 13: 2524-2533. DOI: http://dx.doi.org/10.3923/itj.2014.2524.2533

12. Lysenko N., Labkov G. Applying of Kutter-Jordan-Bossen steganographic algorithm in video sequences. Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian, 1-3 Feb. 2017. DOI: https://doi.org/10.1109/EIConRus.2017.7910651

13. Zeeshan M., Ullah S., Anayat S., Hussain R.G., Nasir N. A Review Study on Unique Way of Information Hiding: Steganography, International Journal on Data Science and Technology. Vol. 3, No. 5, 2017, pp. 45-51. DOI: http://dx.doi.org/10.11648/j.ijdst.20170305.11

14. Thangadurai K., Sudha Devi G. An analysis of LSB based image steganography techniques. Computer Communication and Informatics (ICCCI), 2014 International Conference on, 3-5 Jan. 2014. DOI: https://doi.org/10.1109/ICCCI.2014.6921751

15. Liu, J., Tian, Y., Han, T. et al. Stego key searching for LSB steganography on JPEG decompressed image. Sci. China Inf. Sci. (2016) 59: 32105. DOI: https://doi.org/10.1007/s11432-015-5367-x

16. Iranpour M. LSB-Based Steganography Using Hamiltonian Paths. Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on, 16-18 Oct. 2013. DOI: https://doi.org/10.1109/IIH-MSP.2013.151

17. Fkirin A, Attiya G. and El-Sayed A. Steganography Literature Survey, Classification and Comparative Study.Communications on Applied Electronics 5(10):13-22, September 2016. DOI: https://doi.org/10.5120/cae2016652384

18. Dr. Simon R Wiseman. Defenders Guide to Steganography. Deep Secure Technical Report DS-2017-2. DOI: https://doi.org/10.13140/rg.2.2.21608.98561

19. Luo P, Yu-Lun Lin A, Wang Z. Hardware Implementation of Secure Shamir's Secret Sharing Scheme. High-Assurance Systems Engineering (HASE), 2014 IEEE 15th International Symposium on, 9-11 Jan. 2014. DOI: https://doi.org/10.1109/HASE.2014.34