Date of publication JUN-30, 2022, date of current version MAY-17, 2022.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.21.2.2591

Ensuring the Data Integrity in Infocommunication Systems

VLADIMIR PEVNEV, ALEKSANDR FROLOV, MIKHAIL TSURANOV, HEORHII ZEMLIANKO

National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, 61070, Ukraine (e-mail: v.pevnev@csn.khai.edu, a.frolov@csn.khai.edu, m.tsuranov@csn.khai.edu, g.zemlynko@csn.khai.edu)

Corresponding author: Vladimir Pevnev (e-mail: v.pevnev@csn.khai.edu).

This work is supported by the project STARC (Methodology of SusTAinable Development and InfoRmation Technologies of Green Computing and Communication) funded by Department of Education and Science of Ukraine.

ABSTRACT The article is devoted to the study of the perspectives of steganography to ensure integrity. The definition of information integrity is presented, which meets the new requirements and the definition of cybersecurity. Integrity is achieved through the control and recovery of information. The article provides a detailed analysis of existing approaches to the construction of modern steganometric systems. The greatest attention in the article was paid to the method of hiding information in graphic containers. The proposed method is a modification of the well-known method of replacing the least significant bits. The main difference from the known method is that not all least significant bits are changed. The selection of the bits to be changed is carried out using a pseudo-random sequence generator, while, thanks to the proposed algorithm, no more than 3.12 percent of the bits are changed, which is the limit of visibility for the steganalyst. There are 6.25 percent of information bits in such a message.

KEYWORDS Integrity of information; steganography; container; adder.

I. INTRODUCTION

THE higher development of information technologies imposes stringent requirements for ensuring information security (IS) on various systems. One of the main and most acute is the problem of ensuring the integrity of information (IoI) [1]. The integrity of information in [2] is defined as the impossibility of unauthorized modification, deletion, copying and creation of new data of this type. At that, the system shall provide indication of specified unauthorized actions or their attempts.

However, this definition does not match any of the classical works on information theory, which describe the properties of information. These properties include availability, timeliness, relevance, completeness, objectivity, etc. As it can be seen, the concept of integrity of information in these documents is missing.

It should be noted that it would be correct to attribute integrity to the properties of the system in which information circulates. In this case, integrity should be defined as a property of the system with the help of built-in means for a given time to counteract unauthorized change of information and/or restore distorted information. Based on the presented definition of IoI, we can distinguish the following effects on information [3]:

- modification of information;
- substitution of information;
- destruction of information.

Modification supposes changes to any part of the information. These changes can be both accidental and intentional. In the second case, they may be authorized or unauthorized. Substitution supposes the imposition of false information by replacing the true (original) information. Destruction is most often associated with the destruction of a physical information carrier and/or demagnetization (formatting) of electronic media [1].

In solving the problem of ensuring IoI the following stages may be noted:

- direct integrity provision;
- integrity control;
- recovery of integrity.

Direct integrity provision can be achieved due to the reliability of technical means, reduction of the volume of transmitted information, concealing the fact of information transfer and organizational measures.

Integrity control is achieved through a checksum or digital signature.

Recovery of the integrity of information is carried out through the use of methods of noiseless coding, antivirus protection and the use of backup copies. It should be noted that any recovery method starts working after and/or together with integrity monitoring. It is also worth noting antivirus protection, which can recover files by removing the virus body embedded in these files.

All the presented methods are described in detail in [1].

II. LITERATURE REVIEW

Despite the high demand for means of providing IoI in modern realities, at present there are practically no works that would reflect the results of a comprehensive study of methods and techniques. After the publication of the famous article [4], a new direction in cryptography appeared – the use of a digital signature. At that time, it was a truly revolutionary decision. Many countries have introduced their own standards, which have been revised and improved many times. The bottleneck in all proposed systems is keys. Their crypto resistance increases due to an increase in size or the use of new mechanisms (e.g., elliptic curves). The use of traditional symmetric keys in a digital signature leads to possible compromise of the document.

Much attention was paid to steganography at the end of the last century. However, recently there have been no significant works on the theory of steganography. The last theoretical works are dated to 1995-2005 years. These include [5-8]. Unfortunately, there is little work on integrated research to ensure the integrity of information. There are several articles that deal with CI issues, but overwhelmingly they deal with integrity issues in databases [9, 10] or computer networks [11].

The purpose of the article is to analyze the possibility of using steganography methods to provide CIs during its life cycle.

III. BASIC PART OF THE STUDY

A. ANALYSIS OF STEGANOGRAPHY METHODS

The possibility of applying the methods of steganography for ensuring IoI is justified in [1].

Computer steganography techniques use text, graphic, audio, or video files to hide the fact that a message needs to be transmitted. These methods are based on [8, 12-14]:

– using the properties of computer formats that are specifically designed for data storage and transmission;

– redundancy of audio, visual or textual information from the standpoint of psychophysiological features of human perception.

Today there is a great variety of steganography algorithms. Methods of computer steganography are divided into three main groups, each of which has several implementations that use different mechanisms of information concealment [8, 12-21]:

a) methods of hiding information in audio containers:
   1) the method of hiding in the smallest significant bits;
   2) the method of concealment based on the distribution of the spectrum;
   3) the method of concealment based on the use of the echo signal;
   4) the method of hiding in the signal phase;
b) methods of hiding information in text containers:
   1) the method of concealment on the basis of gaps;
   2) the method of concealment based on the syntactic features of the text;
   3) the method of concealment on the basis of synonyms;
   4) the method of concealment based on the use of errors;
   5) the method of concealment based on the generation of quasi-text;
   6) the method of hiding based on the use of font features;
   7) the method of hiding based on the use of document code and file;
   8) the method of concealment based on the use of alternating the length of words;
   9) the method of concealment based on the use of the first letters;
c) methods of hiding information in graphic containers:
   1) the method of hiding in the smallest significant bits;
   2) the method of concealment based on the modification of the index format of the presentation;
   3) the method of concealment based on the use of autocorrelation function;
   4) the method of concealment based on the use of nonlinear modulation of the embedded message;
   5) the method of concealment based on the use of sign modulation of the built-in message;
   6) concealment method based on wavelet transform;
   7) the method of concealment based on the use of discrete cosine transform.

The greatest development and application today acquire methods of hiding information in graphic containers. This is due to the large size of graphics files, the large amount of information that can be placed in such containers without noticeable distortion of the image, the existence in most real images of areas that have a noise structure and are well suited for embedding information, a variety of image processing methods and digital image representation formats used in steganography. Classification of steganography methods in which graphic containers are used is shown in Fig. 1.

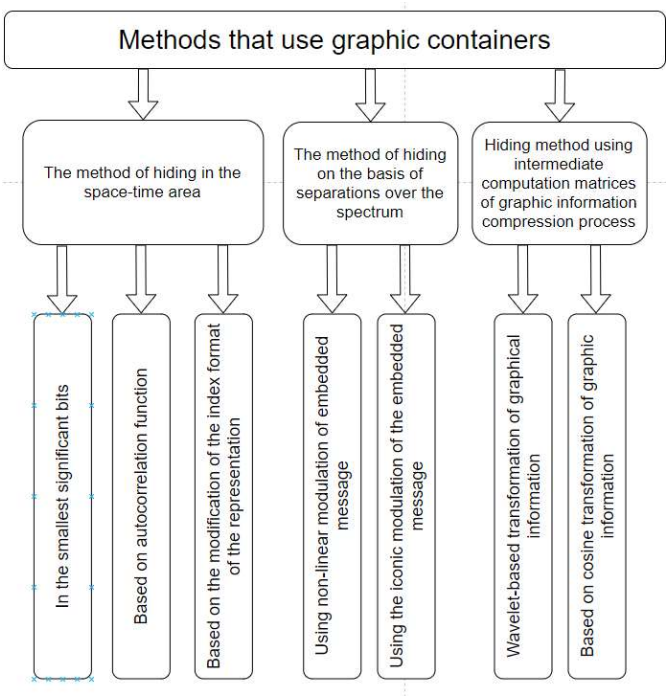


Figure 1. Classification of steganography methods that use graphic containers

One of the most common is the method of hiding in the least significant bits (LSB). The essence of this method is to replace the last significant bits in the container with bits of the hidden message [13]. The difference between empty and filled containers will be imperceptible to human perception. There are a large number of implementations of this method [8, 22, 23].

The disadvantage of the LSB method is its instability to the processing of the container file, which makes it impossible to use it in hiding data in the file, which is subsequently compressed [23, 24].

More resistant to distortion, including compression, are methods that use spectrum allocation to hide information because they use data that has already been converted through communication channels.

There are several ways to represent an image in the frequency domain. In this case, a certain decomposition of the image is used as a container. For example, there are methods based on discrete cosine transform (DCP), discrete Fourier transform (DFT), wavelet transform, Karunen Loev transform, or eigenvector expansion, and others [15, 25-28]. Such transformations can be applied both to individual parts of the image and to the image as a whole.

Wavelet transforms and DCTs are the most widespread among all orthogonal transformations in steganography. This is due to the significant spread of their use in image compression. In addition, to hide the data, it is advisable to use exactly the transformation of the container, which will be subjected to this in the known compression algorithms. For example, the DCT algorithm is basic in the JPEG standard, and the wavelet transform in the JPEG2000 standard [29, 30].

One of the most famous steganography methods is the method of Koch and Zhao method of relative substitution of DCT coefficients [31, 32]. This algorithm implements a watermark bit into 8 x 8 pixel image blocks (1 bit per block). A monochrome image or a sequence {0, 1} consisting of any number of numbers can be used as a message.

When applying this algorithm, it is assumed that the recipient must know in addition to the container with embedded data and its dimensions, the algorithm for hiding data, the dimension of the segments into which the container was divided, and the matrix coordinates of the cosine functions used for hiding. When receiving data from the image, the DCT is repeated and the selected coefficients are compared according to the rule used when hiding the data.

Thus, the original image is distorted by making changes to the DCT coefficients, if their relative value P does not correspond to the bit that is hidden. The larger the P value, the more resistant it is to compression, but the image quality deteriorates significantly. Conversely, the smaller P is, the less noticeable the presence of information in the container, but the greater is the number of errors in the extracted information.

Another steganography method is the Friedrich method [8]. In contrast to the previous Koch and Zhao algorithm, in which DCT is performed in blocks, in Friedrich's algorithm DCT occurs for the entire image that is protected. The hidden message is a sequence of {-1, 1}. In this algorithm, the data is embedded in the image in two different ways, depending on which DCT coefficients are hidden in medium-frequency or low-frequency. This algorithm has the same disadvantage: the resistance of the algorithm to compression decreases with increasing container capacity.

A similar shortcoming is characteristic of other algorithms [33, 36], which use concealment in the coefficients of spectral transformations.

It should also be noted the inherent algorithms described above significantly deteriorate the accuracy of the recovered data with increasing compression ratio.

B. METHOD DEVELOPED

The proposed work does not set the task to consider the essence of the analyzed methods of steganography. The result of the analysis should be the choice of a method that can be used to ensure IoI. One of the simplest and most effective methods of hiding information, according to the authors, is a graphical method using the low-order bits of the transmitted image data. This results from the fact that in the presence of 8-16 bits on one color for each pixel change of the younger of them practically does not affect the quality of the transmitted image.

At the present stage of development there is a sufficiently large number of algorithms that allows to find the embedded message in the container. To neutralize such algorithms, it is necessary to reduce the number of changeable bits, but at the same time even unchangeable bits must carry some information. To implement such a scenario, an algorithm is proposed that uses a pseudo-random sequence generator (PRSG). This idea is realized with the help of the scheme shown in Fig. 2.

Consider the work of the proposed scheme. The input of the adder-distributor (AD) receives a message that we want to pass and a pseudo-random sequence (PRS) from the PRSG. The resulting sequence AD converts by overlaying a message on the unit bits of the PRS. Fig. 3 shows the receipt of the output sequence (third row), which must be transmitted to the input of the container using the transmitted message (upper row) and PRS (second row).

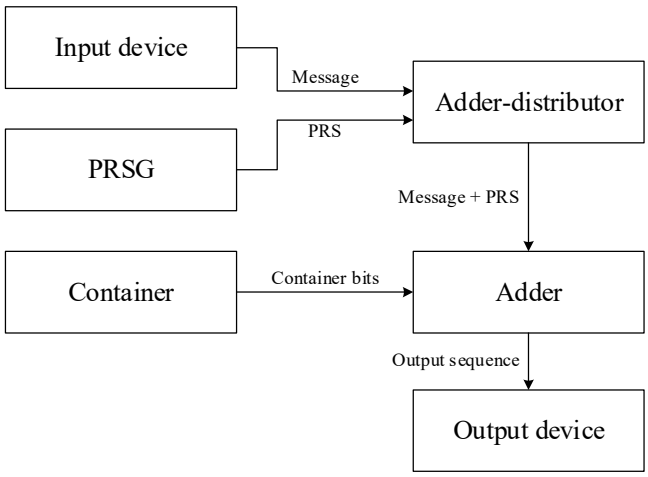


Figure 2. IoI ensuring scheme

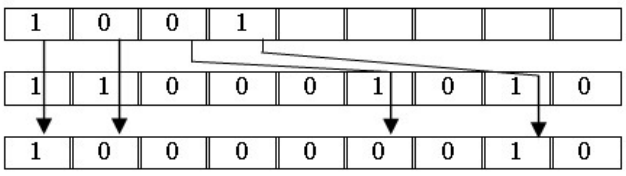


Figure 3. Matching of message bits with container bits

In the adder, modulo-2 addition (XOR) occurs between the corresponding bits of the container and the sequence received from the AD. See Fig. 4.

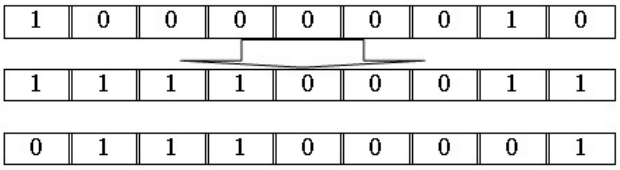


Figure 4. The process of embedding message bits in a container using XOR operation

The first line in Fig. 3 corresponds to the output of the AD block, the second line – the values of the corresponding bits of the container, the third line – the transmitted message embedded in the corresponding bits of the container.

It should be noted that the part of the unchanged bits of the container conveys information that contains the message. Due to this, there is an increase in stealth, and additional difficulties are created for the opposing side. With the structure of the message taken as an example, only two of the eight bits involved in the transmission of the message were changed.

If we consider the PRS, which is involved in the process of converting information, then it should be noted that CSPs described in [35] comply with the requirements set forth in [37] and have the properties of a random sequence.

When considering the original transmitted message, it may turn out that it contains more units than zeros. In this case, we can invert the bit sequence, thereby reducing the number of changed bits in the container. Such bits will be less than 25 percent of the number of low bits of each color of the graphic image.

The scheme and description of the algorithm. The scheme of the proposed algorithm is shown in Fig. 5.

Step 1. The low bits that are responsible for each color of each pixel in the container are stand out.

Step 2. Generated by the PRS using the generator.

Step 3. The message pointer is set to zero.

Step 4. If the number of ones in the message exceeds the number of zeros, then all bits of the message are inverted. The sum of the number of ones and zeros in the message is written to the message length counter.

Step 5. The bits of the container obtained in step 1 are matched with PRS bits obtained in step 4. "1" is written to the match counter.

Step 6. If the PRS bit is "1", then modulo-2 addition (XOR) occurs between the corresponding bit of the container and the bits of the message pointed to by the message pointer. The value of the message pointer is incremented by one.

Step 7. If the PRS bit is "0", then the corresponding container bit does not change.

Step 8. The value of the counter is incremented.

Step 9. If the value of the message length counter is greater than the value of the message pointer, then go to step 6.

Step 10. Completion of the algorithm.

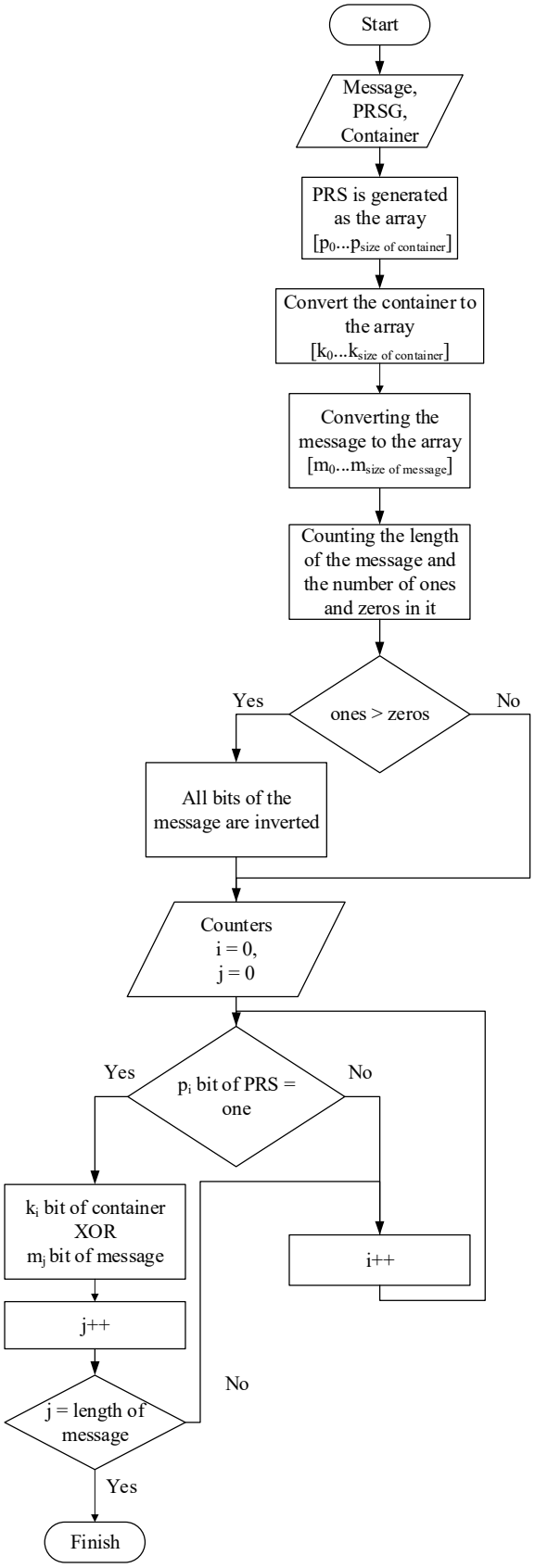


Figure 5. Scheme of algorithm

IV. CONCLUSION

Information integrity in the face of widespread information technology is playing an increasingly important role in ensuring cybersecurity in the modern world. In the present

work, the possibility of using steganographic methods to ensure integrity in infocommunication systems is considered. Based on the analysis of steganography methods, the classification of these methods is presented. The paper proposes a modification of the well-known LSB method due to the use of a pseudo-random sequence generator, allowing us to reduce the number of variable characters in the container. Such symbols become no more than 25 percent, which greatly complicates the adversary's activities in detecting and imposing information, which contributes to the solution of the main task of ensuring integrity. In order to further improve the proposed method, consideration should be given to placing the transmitted message in the most "variegated" places of the pictures that are used to transmit the message.

References

[1] V. Pevnev, M. Tsuranov, H. Zemlianko, O. Amelina, "Conceptual model of information security," In *Integrated Computer Technologies in Mechanical Engineering, ICTM 2020, Lecture Notes in Networks and Systems*, Springer, Cham, Switzerland, 2021, vol. 188, pp. 158–168. https://doi.org/10.1007/978-3-030-66717-7_14.

[2] ITU-T Rec. Y.2701, Security requirements for NGN release 1, April 2007, 44 p. [Online]. Available at: https://www.itu.int/rec/T-REC-Y.2701-200704-I/en.

[3] V. Pevnev, V. Torianyk, V. Kharchenko, "Cyber security of wireless smart systems: channels of intrusions and radio frequency vulnerabilities," Radioelectronic and Computer Systems, no. 4, pp. 79–92, 2020. https://doi.org/10.32620/reks.2020.4.07. (in Ukrainian)

[4] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, issue 2, pp. 120-126, 1978. https://doi.org/10.1145/359340.359342.

[5] J. Reeds, "Solved: The ciphers in book III of trithemius's steganographia," AT&T Labs New Jersey, 1998, 28 p. [Online]. Available at: http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/Trithemius.pdf

[6] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, "Information hiding – A survey," *Proc. of the IEEE (special issue)*, vol. 87, issue 7, pp. 1062–1078, 1999. https://doi.org/10.1109/5.771065.

[7] M. D. Swanson, Z. Bin, B. Chau, A. H. Tewfik, "Multiresolution video watermarking using perceptual models and scene segmentation image processing," Proceedings of the IEEE International Conference on Image Processing, 1997, vol. 2, pp. 558-561, https://doi.org/10.1109/ICIP.1997.638832.

[8] J. Fridrich, M. Goljan, R. Du, "Reliable detection of LSB steganography in color and grayscale images," Special Sessions on Multimedia Security and Watermarking Applications: Proceedings of the 2001 Workshop on Multimedia Security: New Challenges, Ottawa, Canada, October 5, 2001, pp. 27-30. https://doi.org/10.1145/1232454.1232466.

[9] Z. Li, Y. Xilan, L. Hongsong, C. Minrong, "A dynamic multiple watermarking algorithm based on DWT and HVS," *Int. J. Communications, Network and System Sciences*, vol. 5, no. 8, pp. 490–495, 2012. https://doi.org/10.4236/ijcns.2012.58059.

[10] E. A. Brewer, "Pushing the CAP: Strategies for consistency and availability," *IEEE Computer*, vol. 45, issue 2, pp. 23–29, 2012. https://doi.org/10.1109/MC.2012.37.

[11] A. Serkov, V. Tkachenko, V. Kharchenko, V. Pevnev, K. Trubchaninova, N. Doukas, "Method of increasing security of spatial intelligence in the industrial internet of things systems," *Proceedings of the 24th International Conference on Circuits, Systems, Communications and Computers, CSCC'2020*, 2020, pp. 283–289. https://doi.org/10.1109/CSCC49995.2020.00058.

[12] B. Girod, "The information theoretical significance of spatial and temporal masking in video signals," *Human Vision, Visual Processing, and Digital Display: Proc. of the SPIE*, Los Angeles, January 18-20'1989, vol. 1077, pp. 178-187. https://doi.org/10.1117/12.952716.

[13] E. Adelson, *Digital Signal Encoding and Decoding Apparatus*, U.S. Patent, No. 4,939515, 1990.

[14] D. S. Taubman, M. W. Marcellin, *JPEG 2000: Image Compression Fundamentals, Standards and Practice*, Kluwer Academic Publishers, 2001, 776 p. https://doi.org/10.1007/978-1-4615-0799-4.

[15] S. J. Gibbons, F. Ringdal, T. Kværna, "Joint seismic-infrasonic processing of recordings from a repeating source of atmospheric explosions," *J. Acoust. Soc. Am.*, vol. 122, issue 5, pp. 158-164, 2007. https://doi.org/10.1121/1.2784533.

[16] D. Simitopoulos, D. E. Koutsonanos, M. G. Strintzis, "Robust image watermarking based on generalized radon transformations," *Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 732–745, 2003. https://doi.org/10.1109/TCSVT.2003.815947.

[17] Y.-C. Chiu, W.-H. Tsai, "Copyright protection against print-and-scan operations by watermarking for color images using coding and synchronization of peak locations in frequency 95 domain," *Journal of Information Science and Engineering*, vol. 22, no. 3, pp. 483–496, 2006.

[18] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, A. Piva, "A DWT-based technique for spatio-frequency masking of digital signatures," *Proceedings of the 11th SPIE Annual Symposium, Electronic Imaging, Security and Watermarking of Multimedia Contents*, 1999, vol. 3657, pp. 31-39. https://doi.org/10.1117/12.344689.

[19] T. H. Manjula Devi, H. S. Manjunatha Reddy, K. B. Raja, K. R. Venugopal, L. M. Patnaik, "Detecting original image using histogram, DFT and SVM," Intern. Journal of Recent Trends in Engineering, vol. 1, no. 1, pp. 367–371, 2009.

[20] M. Sheikhan, M. S. Moin, M. Pezhmanpour, "Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform," *Proceedings of the 10th Int. Conf. on Intelligent Systems Design and Applications*, 2010, pp. 368–372. https://doi.org/10.1109/ISDA.2010.5687236.

[21] M. Topkara, U. Topkara, M. J. Atallah, "Words are not enough: Sentence level natural language watermarking," *Proceedings of the 4th ACM International Workshop on Contents Protection and Security MCPS'06*, October 2006, pp. 37–46, https://doi.org/10.1145/1178766.1178777.

[22] B. Pfitzmann, *Information Hiding Terminology*, Springer Lecture Notes of Computer Sciense, 1996, pp. 347-350. https://doi.org/10.1007/3-540-61996-8_52.

[23] A. Westfeld, A. Pfitzmann, *Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools – and Some Lessons Learned*, [Online]. Available at: https://users.ece.cmu.edu/~adrian/487-s06/westfeld-pfitzmann-ihw99.pdf.

[24] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, no. 6, pp. 441-444, 2005. https://doi.org/10.1109/LSP.2005.847889.

[25] X. Chen, Q. Dai, C. Li, "A fast algorithm for computing multidimensional DCT on certain small sizes," *IEEE Transactions on Signal Processing*, volume 51, issue 1, pp. 213–220, 2003. https://doi.org/10.1109/TSP.2002.806558.

[26] C.-H. Chen, B.-D. Liu, J.-F. Yang, "Condensed recursive structures for computing multidimensional DCT/IDCT with arbitrary length," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 52, no. 9, pp. 1819-1831, 2005. https://doi.org/10.1109/TCSI.2005.852935.

[27] S. Zhou, B. Tang, R. Chen, "Comparison between non-stationary signals fast fourier transform. and wavelet analysis," *Proceedings of the International Asia Symposium on Intelligent Interaction and Affective Computing*, 8-9 December 2009, Wuhan, pp. 128-129. https://doi.org/10.1109/ASIA.2009.31.

[28] A. Jaber, R. Bicker, "Real-time wavelet analysis of a vibration signal based on Arduino-UNO and LabVIEW," *International Journal of Materials Science and Engineering*, vol. 3, no. 1, pp. 66-70, 2015. https://doi.org/10.12720/ijmse.3.1.66-70.

[29] J. Li, "Image compression: The mathematics of JPEG 2000," *Modern Signal Processing, MSRI Publications*, vol. 46, pp. 185-221, 2003. [Online]. Available at: https://www.msri.org/people/staff/levy/files/Book46/08li.pdf.

[30] ISO/IEC 15444-1:2019 Information Technology – JPEG 2000 Image Coding System – Part 1: Core Coding System

[31] J. Zhao, E. Koch, "Embedding robust labels into images for copyright protection," *Proceedings of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, Munich, Vienna, 1995, pp. 242–251.

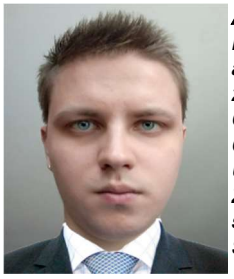
[32] J. Zhao, E. Koch, "Towards robust and hidden image copyright labeling," *Proceedings of the IEEE Workshop on Nonlinear Signal and Image Processing*, Greece, 1995, pp. 123–132.

[33] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, no. 7, pp. 674-693, 1989, https://doi.org/10.1109/34.192463.

[34] Y. Jadav, "Comparison of LSB and subband DCT technique for image watermarking," *Proceedings of the Conference on Advances in Communication and Control Systems*, Mumbai, India, 2013, pp. 398-401.

[35] M. J. Shensa, "The discrete wavelet transform: wedding the a trous and Mallat algorithms," *IEEE Trans. on Signal Processing*, vol. 40, pp. 2464–2482, 1992. https://doi.org/10.1109/78.157290.
[36] N. Urbanovich, "Development, analysis of efficiency and performance in an electronic textbook methods of text steganography," *Proceedings of the Printing future days: 4th International Scientific Conference on Printing and Media Technology*, Chemnitz, Germany, 07–10.11.2011, pp. 189–193.
[37] J. Soto, *Statistical Testing of Random Number Generators*, National Institute of Standards & Technology, 2009, p. 3.

***VLADIMIR PEVNEV**, graduated Kharkiv Higher Military Command School in 1975. An Associate Professor of Dept. of Computer Systems, Networks and Cybersecurity, National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine since 2014. Scientific interests: cryptography, generation prime number.*



***ALEKSANDR FROLOV**, graduated National Aerospace University named after N. Ye. Zhukovsky "KhAI" in 2018. A PhD student of Dept. of Computer Systems, Networks and Cybersecurity, National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine since 2018. Scientific interests: Steganography, Cybersecurity.*

***MIKHAIL TSURANOV**, graduated National University of Internal Affairs in 2006. A Senior lecturer of Dept. of Computer Systems, Networks and Cybersecurity, National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine since 2015. Scientific interests: Cybersecurity.*

***HEORHII ZEMLIANKO**, graduated National Aerospace University named after N. Ye. Zhukovsky "KhAI" in 2019. A PhD student of Dept. of Computer Systems, Networks and Cybersecurity, National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine since 2020. Scientific interests: cybersecurity Smart Systems, game concept in information technology, UX/UI Design, Internet of Things and Smart-technologies.*