***Humeniuk I., Cand. Tech. Sc., Assoc. Prof.**,*
Lahodnyi O., Cand. Tech. Sc.,
Kosheva I.
Korolov Zhytomyr Military Institute

INFORMATION ENCRYPTION METHOD IS BASED ON A COMBINATION OF CRYPTOGRAPHIC AND STEGANOGRAPHIC PROPERTIES OF ALGORITHMS

Problem statement. With the beginning of a full-scale invasion of Russian Federation in Ukraine, the objects of cyber influence were primarily the government, energy, military and financial sectors of the state. In the current conditions, the task of improving existing methods of protecting information at the data, host and network levels, synthesis of cryptographic and steganographic encryption algorithms is becoming relevant. That is why the purpose of this work is to ensure high cryptographic stability of encrypted information during its transmission through the channels of the network of information and communication systems and reduce the level of threat of unauthorized access to it or attack on the cipher.

Research method. The main properties of information, the maintenance of which is one of the tasks of ensuring cybersecurity, include confidentiality, data integrity and accessibility to electronic information resources. Their complex set is called the security model (triad).

To achieve this goal, it is proposed to improve the method of information protection, which is based on the use of the alphabet of a monochrome image. The proposed method consists of three stages: primary, main (encryption) and final (decryption). Detailed scheme of the method functioning is given in Fig. 1.

In the first step, each character that can be used in the message is assigned a certain static range of values [000; 255], which corresponds to the brightness scale of the image pixels. If you select a color bitmap, this range is tripled by using all channels (R, G, and B). As a result, the number of alphabet variants increases, for example, the value for English characters is selected from [0; 255] the R channel, for punctuation marks and special characters – the G channel and digits – B, etc.

It is worth noting that the alphabet is synthesized on one side of the information exchange and sent to the other by closed channels of data transmission, or agreed without any third party.

Another step of the current stage is the formation of a pixel map. It arbitrarily selects an image with the same color model and the number of blocks to which it will be distributed and numbered.

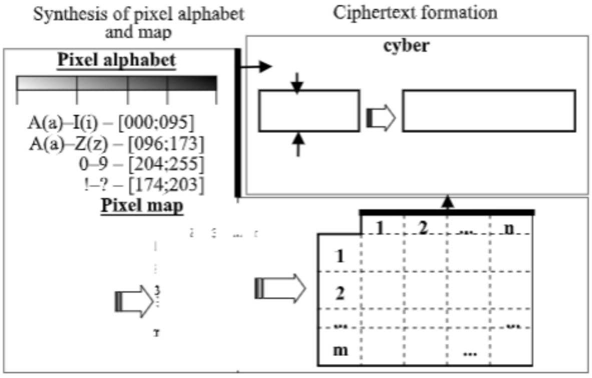

Fig. 1. Method operation scheme

For each block, average pixel brightness values are calculated and recorded in the table. The alphabet, the image should be changed with a certain periodicity.

The main stage is intended directly for encrypting the message of the original message, transmitting by the sender and receiving by the addressee. Its essence lies in the following: the message using the synthesized alphabet is replaced by the corresponding value from the range assigned to it. Further, pixel map block numbers and corresponding average pixel brightness values are randomly selected. Accordingly, these numbers determine the encryption key. Using the formulas given in the scheme, a ciphertext is formed. A feature of the method is that several characters can be assigned the same block.

The result is a ciphertext that looks like a sequence of pairs of values and for each character of the message.

Conclusion. The proposed method is advisable to use during the organization of the transfer of confidential information and in the presence of a potential threat of unauthorized access to it.

References

1. R. Hryschuk, Yu. Danik Fundamentals of Cybernetic Security : monograph, Zhytomyr. : ZhNAEU, 2016. 636 p.

2. V. Trysnyuk, K. Smetanin, I. Humeniuk, O. Samchyshyn, T. Trysnyuk Information Encryption Method based on a Combination of Steganographic and Cryptographic Algorithm's Features: Cybersecurity Providing in Information and Telecommunication Systems II, Kyiv, Ukraine, October 26, 2021. pp. 150–159.