UDC 004.8:519.2

Suprun O.,
candidate of physical and mathematical sciences
National Aviation University

ARTIFICIAL NEURAL NETWORK FOR THE BLIND METHOD OF JPEG STEGANOGRAPHY

Hiding messages in images (steganography) is used for both legitimate and illegitimate purposes. Detecting hidden messages in images stored on websites and computers (stegan analysis) is a top priority for cyber forensics personnel.

Models for describing data embedding and extraction processes can be represented as a communication channel, with the cover image acting as the communication channel through which the data is transmitted, and the embedded message acting as the data stream being sent. Thus, the cover image can be seen as noise; a simple model imitates image as a Gaussian noise implementation. Under these signal detection assumptions, information theoretic concepts can be applied to model embedding algorithms, extraction algorithms, and message detection algorithms. Pattern recognition models can also be applied, and in this study we apply an artificial neural network to classify feature data samples extracted from cover and stego image data [1].

In the operation of any blind algorithm for detecting embedded information, the following stages can be distinguished:

1) construction of a multidimensional space of image features;
2) analysis of the differences between the original images and the stego in the feature space;
3) classification of the database of source images and stego into two groups;
4) assignment of the analyzed image to the image-container or to the stego according to the results of items 2 and 3.

The selection of features is one of the most important stages of building a blind method of detecting steganographic information. The pixel space of the image is transformed into the feature space and the definition of the embedded message takes place already in the feature space.

Used sources

1. Yudin O., Barannik N., Ziubina R., Buchyk S., Frolov O., Suprun O. Efficiency Assessment of the Steganographic Coding Method with Indirect Integration of Critical Information: In.: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 36-40 (2019).