DEVELOPMENT OF THE TECHNIQUE FOR DETERMINING THE IMPORTANCE OF STEGANOGRAPHIC ALGORITHMS CHARACTERISTICS

Olesia Vovk, Andrii Astrakhantsev
Communication Networks Department, Kharkiv National University of Radioelectronics, Lenin Ave., 14, Kharkiv, 61000, UKRAINE, E-mail: olesia.vovk@gmail.com

With the advent of global computer networks, access to information has become incredibly easy. The simplicity and speed of such access are much improved. The threats of compromised data have also increased. Steganography is one of the ways to support information security. It is a method of communication that conceals the existence of secret messages. Today steganography is used for protecting of information from unauthorized access, network resources monitoring systems, as well as for the protection of copyright in certain types of intellectual property and in the authentication of digital objects.

Currently a very large number of different steganographic methods are proposed, part of them are universal, or designed for a wide range of tasks. At the same time, each steganographic task has different requirements for characteristics such as robustness, capacity, complexity of embedding information and others.

In this paper, methodology of analysis that allows determining the importance (weight) of each of the qualitative characteristics of the methods of hiding information during transmission by communication networks in objective way was proposed.

All the most common fields of using steganography were analyzed and evaluated, such as: covert communication, copyright protection of images (authentication), fingerprinting (traitor-tracing), adding captions to images, adding additional information, such as subtitles to videos, image integrity protection (fraud detection), copy control in DVD recordings and intelligent browsers, automatic copyright information.

Based on the requirements put forward the most common areas using the steganography principles, the most important characteristics of algorithms for all major areas of application of steganography were defined according to the developed methodology. So for protection image integrity the greatest weight values are stability and security, for covert communication are once three characteristics - bandwidth, security and invisibility. Scientific novelty lies in identifying the most influential of all characteristics for steganographic applications, which proved to security, stability and complexity of detection.

There is also scientific novelty in the proposed technique of evaluating the steganoalgorithm effectiveness based on the above characteristics. The technique allows providing equally weighted algorithm estimation, and also considering coefficients obtained during the evaluation of the characteristics importance. Studies have shown that during general evaluation methods the best results was demonstrating by the method of replacing the least significant bit (A1, metric = 0.266). While more detailed analysis considering the importance of the various factors of performance, the best result was shown by integrating methods based on discrete wavelet transform (DWT, A6, metric = 0.240).

On the basis of the research we plan to develop a proprietary method that will be highly resistant to the certain attacks , but generally the above assessment would not be lower than the results for DWT methods.

Keywords – steganography, characteristics, methodic, weight, algorithm, robustness, multiobjective choice.