УДК 004.056.5

М.С. Ратушняк

Information Security by Means of Steganographic Methods

Вінницький національний технічний університет

Анотація

У доповіді розглянуто можливість використання стеганографічних методів приховування інформації та захист авторських прав за допомогою цифрових водяних знаків.

Ключові слова: стеганографія, вбудовування, водяні знаки.

Abstract

The report reviews the possibility of using steganographic methods of hiding information and protection of copyright by means of digital watermarks.

Key words: steganography, embedding, watermarks.

The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue nowadays. Some solution to be discussed is how to passing information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media. This report defines steganography as a science, underlines the importance of the technique used in implementing steganography [1].

Due to advances in ICT (information and communications technology), most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. Steganography is a technique of hiding information in digital media. In contrast to cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video, and images [2]. The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.

In addition, the rapid growth of publishing and broadcasting technology also require an alternative solution in hiding information. The copyright such as audio, video and other source available in digital form may lead to large-scale unauthorized copying. This is because the digital formats make possible to provide high image quality even under multi-copying. Therefore, the special part of invisible information is fixed in every image that could not be easily extracted without specialized technique saving image quality

simultaneously. All this is of great concern to the music, film, book and software publishing industries. Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography. All these applications of information hiding are quite diverse:

- in watermarking applications, the message contains information such as owner identification and a digital time stamp, usually applied for copyright protection;
- fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This is added to copyright information to makes it possible to trace any unauthorized used of the data set back to the user;
- steganography hides the secret message within the host data set and the presence of the message is imperceptible. In those applications, information is hidden within a host data set and is to be reliably communicated to a receiver [3].

To summarize, steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Карпінець В. В., Яремчук Ю. Є. Аналіз рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків / В.В. Карпінець, Ю.Є. Яремчук // Сучасний захист інформації. – 2011. – №2. – С.94 – 99

2. V. Karpinets, Ju. Yaremchuk, M. Prokofjev. Матеріали конференції, Technical University of Gabrovo. International scientific conference UNITECH'12. / V. Karpinets, Ju. Yaremchuk, M. Prokofjev. // Proceedings. Volume I, 16–17 November 2012, Gabrovo. – Pp. 348 – 352.

3. Johnson, N. F., Duric, Z., Jajodia, S. Information Hiding: Steganography and Watermarking - Attacks and Countermeasures. Kluwer Academic Press. Norwrll, MA, New York, The Hague, London, 2000. – 15p.

Ратушняк Марія Сергіївна – студентка групи УБ-12, факультет менеджменту, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: ratushnyak95@outlook.com;

Науковий керівник: ***Рудницька Тетяна Григорівна*** – викладач кафедри іноземних мов, Вінницький національний технічний університет, Вінниця.

Maria S Ratushnyak - Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, email: ratushnyak95@outlook.com;

Supervisor: ***Tatiana Rudnytska*** – teacher of English, the Foreigne Languages Department, Vinnytsia National Technical University, Vinnytsia.