**Digital Steganography: The art of hiding information in plain sight**

RADU ȘTEFAN IONESCU

Department of Economic Informatics and Cybernetics

2Bucharest University of Economic Studies

Calea Dorobanților Ave. No. 15-17, District 1, Bucharest

ROMANIA

E-mail: ionescu.radu.18@gmail.com

*Abstract:* Digital steganography is the practice of using some digital formats, such as image files or sound files, as a cover for hiding messages, without altering the original files in terms of human perception. This method of concealing data may use any computer file type as a container in which we can embed the same or another digital file type. For example, we can hide: a plain text file into an image file, a picture into a sound recording or an image into a text file. However, it is not always possible to do this due to the sizes of the files, so hiding some text into an image file may be far easier than the other way around because, generally, an image file is bigger in size than a text file. For this reason, this paper focuses on the two digital file types that suit best the steganographic process: image files and audio files. These two computer mediums are generally large enough that we can alter them, by embedding the secret information inside, but to the human eye or ear they will appear the same. This is a clever way to send sensitive information because, while cryptography ensures the message is not readable, steganography does not reveal the existence of the message at all. For a better security, cryptography will also be used to encrypt the messages before embedding them into the cover.

*Key-Words:* image steganography, audio steganography, digital steganography, data hiding,

cryptography, steganalysis

**1 Introduction**

For as long as we have known ourselves as humans, besides other problems such as food, water or shelter, we have also had the difficulty of communicating sensitive information. While this dilemma existed in our minds since the birth of humankind, rudimentary solutions started to be implemented back in the ancient times. Nowadays, in an era of information technology, where virtually anybody owns some kind of device connected to the internet, which provides access to lots of data, digital steganography is the modern way of concealing messages or other delicate information. As opposed to ancient steganography techniques, which were implemented in a physical manner, using special ink, writing the message in an unobservable area of a letter or using certain rules for extracting the concealed information from an otherwise normal looking text, the modern implementations makes use of the digital form in which information circulates now.

Digital steganography is the process of embedding sensitive pieces of data into another computer file in such a manner that human perception cannot detect the difference between the original file and the one containing added information. For the purpose of this paper, the confidential data will be referred to as the secret message and the container which embeds it will be called the cover file. Generally, both the secret message and the cover file can be of any computer file type. That means we can hide a text file into an image file, but we can do it the other way around too, although that would be harder because of the generic size difference between the two types.

Image and audio files are appropriate mediums for the steganographic process due to the large size and high redundancy [1]. For the purpose of this paper we will use images and sound recordings as the cover file types and plain text as the secret message type.

Additionally, we will use encryption to ensure better security for the message. Cryptography is different than steganography because, while encrypting a message ensures its transformation into a form that an eavesdropper would not understand, steganography tries to hide the existence of a hidden message at all [2].

Other similar processes tightly coupled with steganography are fingerprinting and digital watermarking. A fingerprinting algorithm is used to generate a unique mark for a piece of data and embed it into that specific file. This is very useful when you want to supply some files and protect them from ongoing distribution. Watermarking also embeds a mark of the files with the purpose of signifying ownership. As opposed to steganography, in fingerprinting and watermarking the existence of the embedded data is publicly known, whereas steganography tries to completely hide that there is any information hidden inside. While a successful attack concerning a watermarking or fingerprinting algorithm consists of removing the watermark or fingerprint, basically removing the ownership protection, an attack on a steganographic system should detect and eventually extract the hidden data [3].

**2 Problem Formulation**

[to-do]

**3 Problem Solution**

[to-do]

**4 Conclusion**

[to-do]

# *References:*

|  |  |  |  |
| --- | --- | --- | --- |
| [1] | M. S. MEGHA, "Methods of Audio Steganography," *International Journal of Engineering and Management Research,* vol. 4, no. 3, pp. 154-156, 2014. | | |
| [2] | N. HAMID, A. YAHYA, B. AHMAD and O. M. AL-QERSHI, "Image Steganography Techniques: An Overview," *International Journal of Computer Science and Security,* vol. 6, no. 3, pp. 168-187, 2012. | | |
| [3] | T. Morkel, J. Eloff and M. Olivier, "An Overview Of Image Steganography," *Proceedings of the Fifth Annual Information Security South Africa Conference,* 2005. | | |
| [4] | M. ZAMANI, A. MANAF, R. AHMAD, F. JARYANI, H. TAHERDOOST and A. M. ZEKI, "A Secure Audio Steganography Approach," *International Conference for Internet Technology and Secured Transactions,* 2009. | | |
| [5] | M. S. SHAHREZA, "Stealth Steganography in SMS," *International Conference on Wireless and Optical Communications Networks,* 2006. | | |
| [6] | P. POCATILU, I. IVAN, A. VIȘOIU, F. ALECU, A. ZAMFIROIU and B. IANCU, Programarea Aplicațiilor Android, Bucharest: Editura ASE, 2015. | | |
| [7] | C. MAITI, D. BAKSI, I. ZAMIDER, P. GORAI and D. R. KISKU, "Data Hiding in Images Using Some Efficient Steganography Techniques," *Communications in Computer and Information Science,* vol. 260, pp. 1-9, 2011. | | |
| [8] | N. F. JOHNSON, Z. DURIC and S. JAJODIA, Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, Boston, MA: Springer, 2001. | | |
| [9] | | R. CHANDRAMOULI and N. MEMON, "Analysis of LSB based image steganography techniques," *Proceedings 2001 International Conference on Image Processing,* vol. 3, pp. 1019-1022, 2001. | |
| [10] | | R. G. BALDWIN, "Steganography 101 using Java," [Online]. Available: https://www.developer.com/java/ent/article.php/10933\_3530866\_2/Steganography-101-using-Java.htm. [Accessed 12 March 2020]. | |
| [11] | | R. G. BALDWIN, "Processing Image Pixels Using Java: Controlling Contrast and Brightness," [Online]. Available: https://www.developer.com/java/other/article.php/3441391. [Accessed 12 March 2020]. | |
| [12] | | R. G. BALDWIN, "Processing Image Pixels using Java, Getting Started," [Online]. Available: https://www.developer.com/java/other/article.php/3403921. [Accessed 12 March 2020]. | |
| [13] | | S. K. ARORA, "Audio Steganography : The art of hiding secrets within earshot (part 2 of 2)," [Online]. Available: https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-2-of-2-c76b1be719b3. [Accessed 11 March 2020]. | |
| [14] | | S. K. ARORA, "Audio Steganography : The art of hiding secrets within earshot (part 1 of 2)," [Online]. Available: https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-1-of-2-6a3bbd706e15. [Accessed 11 March 2020]. | |
| [15] | | “Steganography,” [Online]. Available: https://en.wikipedia.org/wiki/Steganography. [Accessed 9 March 2020]. | |
| [16] | | "Documentation | Android Developers," [Online]. Available: https://developer.android.com/docs. [Accessed 10 March 2020]. | |
| [17] | | "What is Steganography? Webopedia Definition," [Online]. Available: https://www.webopedia.com/TERM/S/steganography.html. [Accessed 25 April 2020]. | |
| [18] | | N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm," *Journal of Computer Science,* vol. 3, pp. 223-232, 2007. | |
| [19] | | | M. Fortrini, "Steganography and digital watermarking: A global view.," 2011. |
| [20] | | | N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," *IEEE Security and Privacy Journal,* vol. 1, pp. 32-44, 2011. |