Steganography in digital media

Pricope Stefan-Cristian
pricopestefancristian@gmail.com

Suciu Mihai
mihai-suciu@cs.ubbcluj.ro

Abstract

Steganography is the science of concealing a piece of information within another piece of information without affecting the latter in a noticeable way and therefore alerting any intruders of the existence of the former. This paper presents both existing and new ways of embedding computer files and data into different digital multimedia formats as covert as possible while still allowing the encoded information to be retrieved at a later time without any significant losses.

1 Introduction

The practice of hiding and securing information and messages between different parties has played a major part alongside human history, especially during times of war when it was vital that the enemy didn't intercept the strategies and even if they did, they would have no idea what to do with them and would have to dedicate a lot of time, money and personnel to decode the communications. Two of the most famous manifestations of this practice are cryptography and steganography[1].

Trying to differentiate between cryptography and steganography is not difficult, the only thing they have in common is their end goal - making sure that a piece of information sent from one place to another is secured and that only the right recipient will be able to read and understand the received information. But the methods they use and the time it takes to reach that goal are very different.

Cryptography chooses to focus on altering the information itself, encrypting it using a key only known by the receiver and sender[1], making it harder for any possible meddlers to alter the meaning of the message or even just understand it. Steganography is more concerned on hiding the fact that there even is any information being transmitted usually by embedding it in something else (hereby referred to as a cover), thus if any interlopers were to actually look at the cover, they wouldn't even be aware of the fact that it contained secrets.

In other words, both methods are meant to be used over an open and unsafe environment, and while cryptography tries to hide the contents of the message but not the fact that there is a message being sent, steganography tries to hide the communication altogether. The main advantage of these 2 methods is that they are not exclusive, they can be used together for maximum safety of the information.[2]

Given the evolution of the Internet and computers in general in the last 5 decades, there was a need for keeping the communications secure over all the networks, especially in the last 2 decades when computers became common household items. Thus, cryptography really got to shine and thousands of algorithms for encrypting the information were conceived and the very few remarkable ones are still being used[3]. But that doesn't mean steganography was left behind, quite on the contrary, researchers developed plenty of new algorithms for hiding information using digital files as cover.

Theoretically all types of digital files could be used as cover - shared libraries and executables can be edited to include the hidden data and then recompiled/rebuilt, text files and documents could be modified to enclose the information in secret places/paragraphs and multimedia such as images, music and video files can be changed to carry the digital data into their metadata, pixels, audio frequencies, motion vectors and many more. This paper will focus on the latter category of files and will

[1]This is only true in symmetric cryptography and is a gross oversimplification of cryptography as a science, but it is just meant to get a point across and help differentiate between the 2.

[2]The speed of encoding/decoding the information is greatly decreased when these 2 are combined which is the reason that nobody merges them, preferring to juse use encryption to keep the information safe.

[3]The reason cryptography is in the spotlight is because it is much faster, mathematically proven, and it hides all the data without leaving anything in plain sight(like steganography does with the cover)

attempt to explain different algorithms that can be used for implementing steganography using multimedia files as our cover.

References

[1] Petitcolas FAP, Anderson RJ and Kuhn MG. *Information Hiding - A Survey*. Proceedings of the IEEE, special issue on protection of multimedia content, 1999.

[2] Merriam-Webster dictionary.
`https://www.merriam-webster.com/dictionary/steganography`

[3] Johnson Neil and Jajodia Susil. *Exploring Steganography : Seeing the Unseen*. Los Alamitos, IEEE Computer Society, 1998.

[4] T. Morkel, J.H.P. Eloff and M.S. Olivier. *An overview of image steganography*. University of Pretoria, ICSA Research Group, 2005.

[5] Niels Provos and Peter Honeyman. *Hide and Seek: An Introduction to Steganography*. University of Michigan, IEEE Computer Society, 2003

2 Conclusion