

|  |
| --- |
| **Steganography – Hidden in plain sight**    **Adam Board – 2005335@uad.ac.uk**  Introduction to Security– CMP110  BSc Ethical Hacking Year 1  2020/21 |

*Note that Information contained in this document is for educational purposes.*

Abstract

Throughout history, kings, criminals, and spies alike have used steganography to hide their messages from the public eye and interceptors in “Plain-sight”. They have communicated with their co-conspirators in this way to ensure that the message looks innocent to onlookers but not to the receiver. Artists and creators also use steganography to mark their intellectual property in case it gets used without their permission by others.

This paper shows how simple steganography can be implemented by using tools like Xiao Steganography and Hide’n’Send to encode a secret file inside of different medias to replicate examples of communication through steganography with an explanation of how each tool works. Furthermore the paper shows ways to make the message more secure using encryption and finally, the report explains methods of finding files with secret payloads within them, better known as steganalysis by using tools such as Hxd to investigate the Least significant bit to show the difference between the original and modified file to show where the information would be hidden within files.

Contents

[1 Introduction 1](#_Toc452904210)

[1.1 Background 1](#_Toc452904211)

[1.2 Aim 1](#_Toc452904212)

[2 Procedure 2](#_Toc452904213)

[2.1 Overview of Procedure 2](#_Toc452904214)

[2.2 Procedure part 1 2](#_Toc452904215)

[3 Results 3](#_Toc452904216)

[3.1 Results for part 1 3](#_Toc452904217)

[4 Discussion 4](#_Toc452904218)

[4.1 General Discussion 4](#_Toc452904219)

[4.2 Countermeasures 4](#_Toc452904220)

[4.3 Conclusions 4](#_Toc452904221)

[4.4 Future Work 4](#_Toc452904222)

[References 5](#_Toc452904223)

[Appendices 6](#_Toc452904224)

[Appendix A 6](#_Toc452904225)

[Appendix B 6](#_Toc452904226)

[Appendix C - Suggestions for formatting figures/tables/screenshots. 6](#_Toc452904227)

# Introduction

## Background

Steganography is a simple technique which has roots dating back to the Greek era during the Ionian uprising against the Persian empire, around 500BC. Herodotus, a classical writer of the Greek period, wrote in his book “*The Histories”* about Histiaeus, the ruler of Miletus and an adviser to the Persian king, and Aristagoras, the son-in-law of Histiaeus. Herodotus explained Histiaeus’ plan of tattooing a message onto a slave's head and then waiting for his hair to grow back to hide the message. Histiaeus then sent this slave all the way to his son-in-law with instructions to shave the slave’s head and read the message. However, Herodotus was also known for his unrealistic tales as well, for example “Snakes with Wings and Gold-digging Ants”. (Lake, 2020)

There are two examples from recent years, one of which includes a group of Russian spies who were sending American Government secrets to the SVR (Russian intelligence agency) through website images, this occurred in 2010. (Jackson Higgins, 2010). The other example is even used today, and it is to do with intellectual property; using steganography for digital watermarking (Dewan, 2017) which is “invisible” and encoded typically in the Least significant bit (LSB) so if the data is stolen then it can be linked back to the original owner.

The term Steganography came from the book, “*Steganographia*” by Johannes Trithemius. Steganography combines both Greek words “steganos,” which translates to concealed, and “Graphein,” translating to Writing; thus meaning concealed writing. The book seemed to talk about magic and occult to anyone who did not know how translate it, but to anyone who did know how to translate it, it was about steganography and cryptography (Lake, 2020). Modern Steganography is defined as “the practice of concealing messages or information within other non-secret data or text.”

This technique allows for hidden messages to be sent over a public space through different mediums, see figure 1.

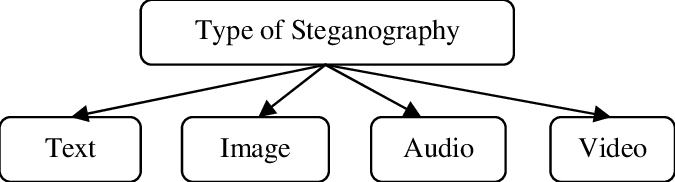


Figure ResearchGate, 2011

There could be an encoded message within any of these mediums, which is meant for another person to read.

Steganography often gets mixed up with cryptography due to their nature of both hiding information. The biggest difference is that steganography tries to do it in “plain-sight” using innocent looking files with a hidden message, while cryptography tries to scramble the message and alter the structure using ciphers and keys. See figure 2 for how steganography is done.

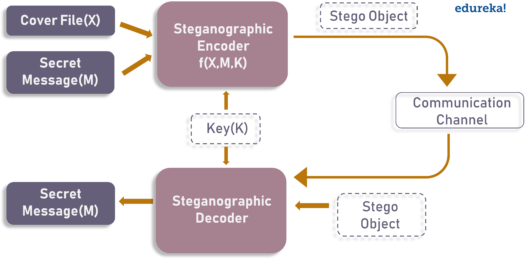


Figure edureka, 2020

Steganography uses a Cover medium and a message that is then encoded into one stego-medium using a key. The receiver has the decoder to decode the medium with the same key. For definitions of each term above see below.

Steganography has a list of terminology that are used when performing this technique, these include:

* Cover Medium/carrier
  + This is the medium within which we are hiding the data, for example images or video files.
* Stego-Medium
  + This is the finished steganographic file that observers see.
* Stego-Key
  + A piece of information required for the receiver, like a password or a cipher.
* Message/payload
  + This is the actual information that is meant to reach the receiver.
* Stego-Systems
  + The means and techniques used to create a hidden channel for sending information.
* Carrier
  + The object where the payload is embedded secretly.
* Steganalysis
  + The act of attacking stego-systems.

(Backdoor, 2020)

One of the problems with steganography alone is that it relies on being in “plain sight”, therefore a message encoded is only secure if anyone does not search for it. The Russian spies were smart and used cryptography on their data for another added layer of security.

An upside is that it can be difficult to know if a file contains a hidden payload or not without the use of steganalysis. Steganalysis can include checking the LSB since some of the data can be hidden inside of the binary code by changing a few of the bits to form sentences, for example 0110010 could be changed to 0110011 to form a different character and so on (Hiding Code Inside Images: How Malware Uses Steganography - SentinelOne, 2019). Using this method keeps the modified file very similar to the original, as no massive changes have been made - so long as the software does not edit too many LSBs. However, if the original file is present as well as the stego-medium, the change in LSB will be noticeable to an interceptor.

Another method is to check the file size, as they can be inflated due to steganography techniques (Hiding Code Inside Images: How Malware Uses Steganography - SentinelOne, 2019). The two images below are an example of the difficulty of spotting the difference with the human eye alone, see figure 3.

Steganography is easily accessible to everyone on the internet. Since there are hundreds of tools for steganography, they all have many similarities and differences between one another in terms of steganographic methods. The downside of this is that hackers, criminals, and terrorist groups also have access to these tools and can use them at their will to send messages.

Figure 3 Security on Demand

## Aim

This paper will show how any individual can create and share a hidden message through an image, Video file, or audio file by using different pieces of softwarewhich are all free. Two of the tools have built-in encryption methods as well.

Finally, this paper shows how to detect stego-mediums by comparing the cover-medium with the stego-medium by their file size or by checking the Least Significant bit for any changes.

Objectives of the report:

* Create a stego-medium for 3 mediums.
* Encrypt the files with the same tools.
* Show the extraction of files with the same tools to emulate passing data undetected.
* Detect the stego-medium’s payload using manual techniques.

# Procedure

## Overview of Procedure

The programs used for encoding the cover-mediums with the message into the stego-mediums include, Xiao Steganography, Hide’N’Send, Our Secret and Steghide. For steganalysis, manual methods like checking the LSB and the file size. Link to tools in the references.

## Procedure part 1

Part 1 aims at Xiao Steganography. After the tool is installed open Xiao Steganography and press ‘Add files’ to open the encoding file section. See figure 4 below for example of Graphical User Interface (GUI).

Graphical user interface, website

Description automatically generated

Figure

Select a BMP or WAV file type to hide your message in. Go to the next page and choose the file to encode; for this example, a song called ‘Return of the gods’ is the carrier for the message. Thereafter the program asks for the payload. Enter the payload to be encoded inside the carrier. It will then ask to select from encryption options that are available and allows a password to be added on as well, see figure 5 for encryption options.

Graphical user interface, application

Description automatically generated

Figure

Once selected, press ‘Next’ and ‘Finish’ and the files will be encrypted into a stego-medium.

For receiving the data, use the extraction function.

## Procedure part 2

This section focuses on Hide’N’Send. Once the tool is downloaded, open the launcher and it will bring up a GUI with the option to ‘Hide’ and ‘Extract’, see figure 6 below.

Graphical user interface, text

Description automatically generated

Figure 6

In Figure 6, in the settings, the method of concealment can be changed, for this example LSB is being used with a SHA512 hash and an AES encryption. In the image section shown in figure 6 a JPEG of a city at night is being used as a carrier file and a screenshot of Abertay university from google maps is the payload. The program requires a password to be set after pressing the ‘Hide’ button.

For extracting put in the same image with the password in the extraction half of the tool.

## Procedure part 3

Our Secret is the tool used in this part. Once the file is downloaded, open the software and add a carrier at the top right, a payload - which is in the center left of the software - and set a password just below the payload selection. For the carrier, the video ‘Ocean Storm tide’ has been used. See figure 7 for example.

Graphical user interface, application

Description automatically generated

Figure 7

Choose the file for the carrier, choose the payload and set a password, then press ‘Hide’. Once the stego-medium is created and sent, the receiver should open the same software and use the unhide function by selecting the stego-medium file and entering the password.

## Procedure part 4

Manual techniques are being used to compare the three stego-mediums to the original versions of the mediums. Hxd is the tool used to inspect the mediums down to the LSB and the standard file explorer is used for checking the files’ size.

Open Hxd and load all the original carrier files and the modified files. The binary and hex of the files can be checked through the main interface. When using file explorer for checking file size, find and check both files against each other by going to the properties tab and comparing the files.

# Results

## Results for part 1

Once the file is encoded and sent the receiver will open it using the same tool and password to reveal the payload file that has the information. See figure 8 below.

Graphical user interface, text, application

Description automatically generated

Figure 8

This shows that the file was successfully encoded within the carrier and sent to the receiver.

## Results for part 2

Once the receiver obtains the stego-medium, the receiver opens it with the same tool to reveal the payload. See figure 9 below.

Graphical user interface

Description automatically generated

Figure

Once the correct password has been entered, the payload will go to a spot selected by the receiver, then they will have successfully obtained the file.

## Results for part 3

When the receiver enters the password for the extraction on Our Secret, they will get the payload from the stego-medium sent to them. See figure 10 below.

Graphical user interface, application

Description automatically generated

Figure

The file that the receiver has been given is a text file called ‘secret.txt’. See contents of ‘secret.txt’ in figure 11 below.

Text

Description automatically generated

Figure

## Results for part 4

Hxd allows the comparison between the original carrier file and the stego-medium. See appendix A for comparison of the different mediums and their original carrier file’s hex text. From the comparison of the images and audio file there is a difference between the original and modified files, and the video file has data added onto the end of the hex text. For the file sizes, the compared file sizes are different by small bytes of data on them which could be a sign of steganography. The files’ sizes are in appendix B.

# Discussion

## General Discussion

From the results of procedure part one to three, it shows that all the tools can successfully create a stego-medium in a very simple and easy way, allowing two or more people to have a conversation. Procedure part 4 allows the detection of the steganograhic methods and can help identify what method has been used for each file, for example procedure part one and two’s tools, Xiao steganography and Hide’N’Send, both used LSB steganography methods since the bits are being edited as seen within the hex text. Xiao Steganography also allows the use of masking and filtering steganography as well, which is typically restricted to 24-bit images as it needs to select the specific pixels to input data into (Christaline, 2011).

The tool Our Secret, adds the data to the end of the hex file rather than hidden within it, so it would be easier to detect as it increases file size and can be easily cleared out of the file as it only needs the extra data erased.

The first two tools have encryption built into them which makes the payload more secure and harder to break into, even after interceptors have found the hidden payload. Both tools made the process of encryption easier since manual encryption was not required.

## Countermeasures

A countermeasure to Stego-mediums could be to create and implement a software that can detect multiple methods of steganography across all carrier types and remove them from the network. A second method would be to only allow trusted signatures from trusted sellers when purchasing any kind of software or downloading any kind of file. Finally, using examples from past exploits, check the past exploits against new incoming files to detect if any steganography techniques have been performed on the file (Mcafee, 2017).

## Future Work

Future work could be composed of creating a working stego-medium detector with a low false positive and negative rate that can detect LSB techniques as well as detecting inflated file sizes compared to an original file found off the internet, or creating a working stego-medium that can breach a firewall using only steganography to plant a reverse shell within the computer to allow control from a remote pc.

# References

2021. Image for types of steganography. [online] Available at: <https://www.researchgate.net/figure/Types-of-Steganography_fig4_228765086> [Accessed 24 April 2021].

Backdoor, Q., 2020. What Is Steganography?. [online] Medium. Available at: <https://medium.com/@.Qubit/what-is-steganography-92c9a611456b> [Accessed 6 May 2021].

Choudary, A., 2021. Steganography Tutorial | A Complete Guide For Beginners | Edureka. [online] Edureka. Available at: <https://www.edureka.co/blog/steganography-tutorial> [Accessed 24 April 2021].

Christaline, A., 2011. [online] researchgate.net. Available at: <https://www.researchgate.net/publication/252024904_Image_steganographic_techniques_with_improved_embedding_capacity_and_robustness> [Accessed 6 May 2021].

Dewan, C., 2017. Steganography - Don’t judge a book by its cover - Infosec Resources. [online] Infosec Resources. Available at: <https://resources.infosecinstitute.com/topic/steganography-dont-judge-book-cover/> [Accessed 1 May 2021].

Download.com. n.d. Hide'N'Send. [online] Available at: <https://download.cnet.com/Hide-N-Send/3001-2092_4-75728348.html> [Accessed 24 April 2021].

Jackson Higgins, K., 2010. Busted Alleged Russian Spies Used Steganography To Conceal Communications. [online] Dark Reading. Available at: <https://www.darkreading.com/risk/busted-alleged-russian-spies-used-steganography-to-conceal-communications/d/d-id/1133884> [Accessed 31 March 2021].

Lake, J., 2020. What is steganography and how does it differ from cryptography?. [online] Crime-research.org. Available at: <https://www.crime-research.org/articles/Stegano26/> [Accessed 31 March 2021].

Mcafee.com. 2017. [online] Available at: <https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-quarterly-threats-jun-2017-2.pdf> [Accessed 4 May 2021].

Oursecret.software.informer.com. n.d. Download OurSecret by SecureKit.net.. [online] Available at: <https://oursecret.software.informer.com/download/> [Accessed 28 April 2021].

Pixabay. 2021. [online] Available at: <https://pixabay.com/music/epic-classical-return-of-the-gods-dark-epic-free-soundtrack-2471/> [Accessed 25 April 2021].

Pixabay. 2021. [online] Available at: <https://pixabay.com/photos/city-bridge-night-river-lights-6156596/> [Accessed 25 April 2021].

Pixabay. 2021. [online] Available at: <https://pixabay.com/videos/waves-sea-ocean-storm-water-tide-71122/> [Accessed 25 April 2021].

Security On-Demand. n.d. Detecting Steganography in Your SOC | Security On Demand. [online] Available at: <https://www.securityondemand.com/detecting-steganography-in-your-soc/> [Accessed 18 April 2021].

SentinelOne. 2019. Hiding Code Inside Images: How Malware Uses Steganography - SentinelOne. [online] Available at: <https://www.sentinelone.com/blog/hiding-code-inside-images-malware-steganography/> [Accessed 28 April 2021].

Softonic. n.d. Xiao Steganography. [online] Available at: <https://xiao-steganography.en.softonic.com> [Accessed 20 April 2021].

# Appendices

## Text, table Description automatically generatedText Description automatically generatedAppendix A

Table

Description automatically generated

Info a Difference between the image carrier and the stego-medium

Table

Description automatically generatedTable

Description automatically generated

Info b Difference between the audio file carrier and the stego-medium

Graphical user interface, text, application

Description automatically generated

Info c Information at the end of the hex text for the video carrier file and the stego-medium

## Appendix B

Graphical user interface, application

Description automatically generated

Info All six files and their difference in file size for results part 4