

Learn to code – free 3,000-hour curriculum

JULY 13, 2023 / #CRYPTOGRAPHY

What is Steganography? How to Hide Data Inside Data



Daniel Iwugo

Ladies and Gentlemen, welcome to the world of Spies



In the movie Uncharted (great movie by the way), Tom Holland and his brother have a secret form of communication. They would write a message on a plain postcard with special ink that became invisible and then send it to the other person.

On the outside, it seemed like another plain old postcard. But if a lighter was lit just behind the paper, the ink would reappear, and a new message would be found 🔥 .

This is one of the coolest hidden information tricks seen in movies. But what if we could do this on computers?

Well, turns out we sorta can. Using Steganography.

Disclaimer: This concept can be used for both good and bad. The content of this article is for educational purposes only and is not to be used to play pranks, or harm people and infrastructure.

Learn to code – free 3,000-hour curriculum

1. What is Steganography?
2. Types of Steganography – Text, Image, Video, Audio, Network
3. Image steganography using Steghide

What is Steganography?

Steganography is the art of hiding secret data in plain sight. It sounds kind of counter-intuitive, but you'd be surprised how effective it is.

Hiding things such as source code, passwords, IP addresses, and other confidential information in pictures, music, or other random files tends to be the last place anyone would think of finding them.

You should note that steganography and cryptography are not mutually exclusive from each other. One may contain elements of the other or both. For example, you could perform steganography with an encryption algorithm or password, as you'll find out soon.

Types of Steganography

There are various types of steganography, and we'll look at five of them in this tutorial.

Text Steganography

This form involves hiding a message within a text. A common way to do this is substitution. It involves replacing certain characters with others and then substituting them back to retrieve the original data.

Learn to code – free 3,000-hour curriculum

Thi follow eng tixt contaens a sicrit missagi

Doesn't really make sense right? But what if we replace the i's with e's and the e's with i's?

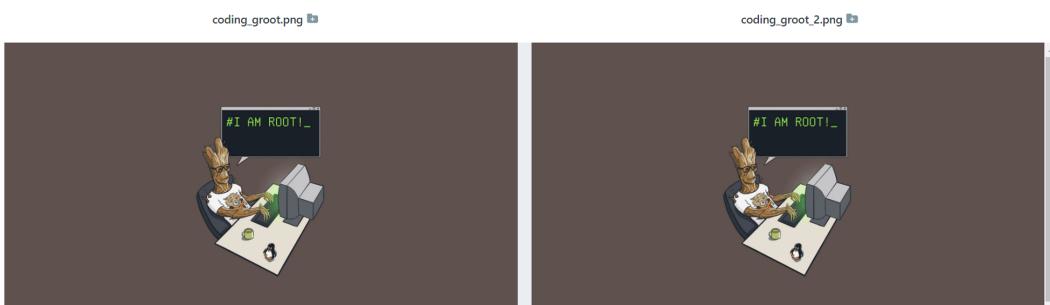
The follow ing text contains a secret message

I think that's a little easier on the eyes. This is a pretty easy example, but there are much more complicated ones and even some you could come up with on your own.

Image Steganography

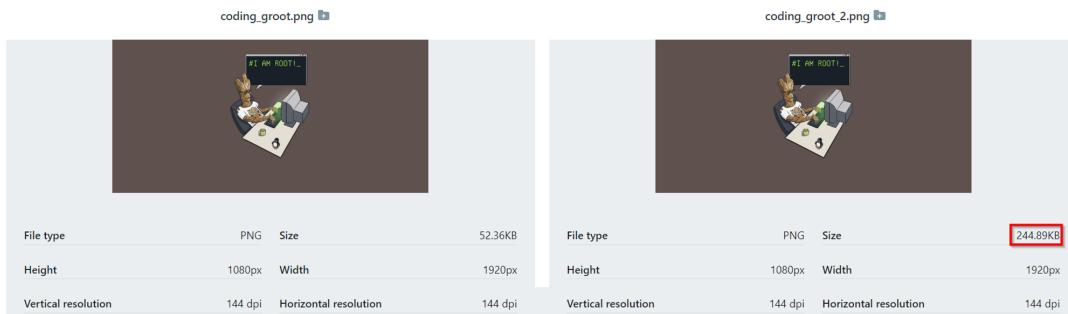
Frankly, this is my favourite. It involves hiding data behind digital images. There are various techniques for image steganography which include the Least Significant Bit technique, Masking and Filtering, and Coding and Cosine Transformation.

Take a look at the two images below and spot the difference:



Groot on Linux | Credit: Mercury

Learn to code – free 3,000-hour curriculum



Comparing the images | Credit: Mercury

The only difference is the size of the images. That's because the one on the right is hiding 260 words of text in it. How cool is that?

Video Steganography

In Video steganography, you can literally hide entire videos inside another video. Videos are basically a sequence of images with audio playing as the sequence progresses. This type of steganography allows each video frame to encode an image of the one you want to hide.

This technique can also be used to hide text as demonstrated in the software [Steganosaurus](#) by James Ridgeway. He shows how it works in this [video](#).

Audio Steganography

This type of steganography enables hidden messages to be encoded inside an audio file. A common technique used in this is called Backmasking. Backmasking is hiding a message in the audio file and it can only be heard when played backwards.

[Learn to code – free 3,000-hour curriculum](#)

Network Steganography

This is relatively rare, but nevertheless, it is a technique in which messages are passed by hiding them in network traffic. The messages could be found in the payload or headers of data packets when captured and analysed by the receiver.

Now let's take a look at how to do some image steganography.

Steganography using Steghide

Steghide is an open source image steganography tool that uses the least significant bit (LSB) method to hide data in images.

Images are made up of pixels, which are made up of bits. The bit depth determines how many colours are present in an image. The higher the bit depth, the more colourful the image tends to look.

What LSB does is change the last bit of each byte (or pixel) in the image to one that represents the data you want to hide. This changes the image data, but if done properly is not perceivable. The higher the bit depth and resolution, the more data can be stored in the image.

Now that you understand how it works, let's play a little hide and seek (no pun intended 😊).

First we'll be needing a few things:

1. A Linux OS
2. An Internet Connection

Learn to code – free 3,000-hour curriculum

Install Steghide

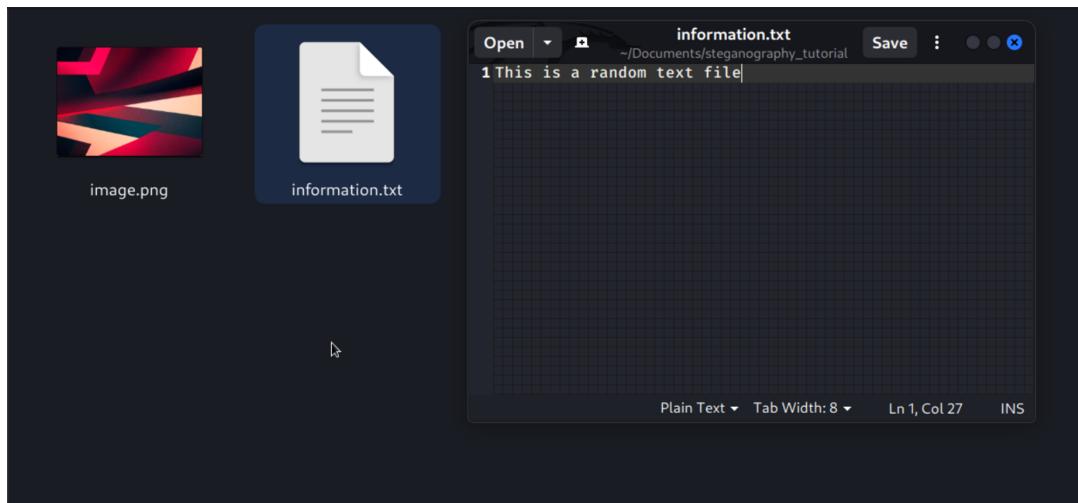
First we need to install Steghide. Open your terminal and run the following command to do that:

```
sudo apt install steghide
```

You can always run `steghide --help` to get the command list to see all your options.

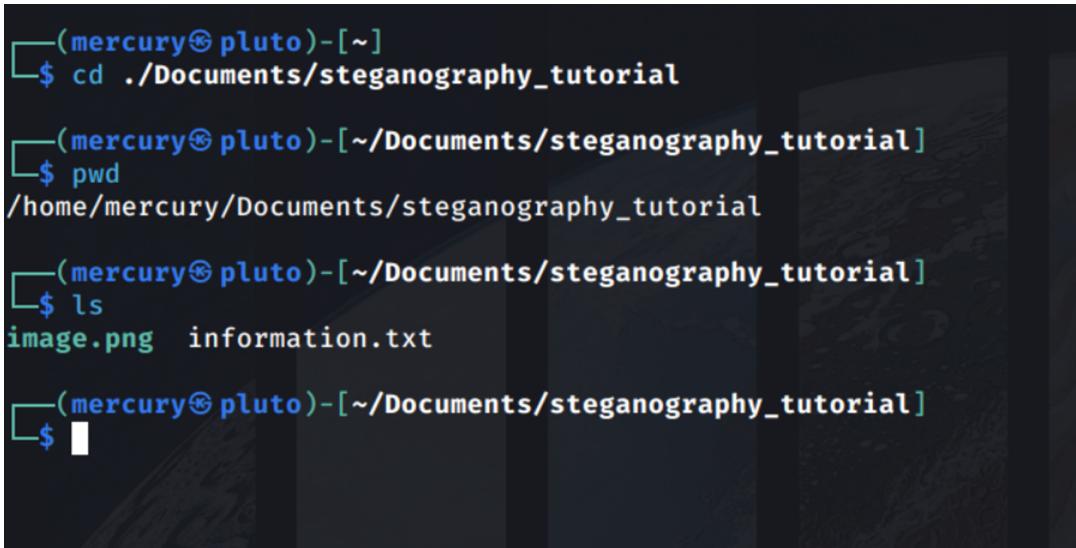
Get your image ready

Next, have an image and a text file in a directory. My files are ‘information.txt’ and ‘image.png’. I’ve also put some text in the file to hide in the image later.



Setting up files | Credit: Mercury

Learn to code – free 3,000-hour curriculum



```
(mercury@pluto)@[~]
$ cd ./Documents/steganography_tutorial

(mercury@pluto)[~/Documents/steganography_tutorial]
$ pwd
/home/mercury/Documents/steganography_tutorial

(mercury@pluto)[~/Documents/steganography_tutorial]
$ ls
image.png  information.txt

(mercury@pluto)[~/Documents/steganography_tutorial]
$ 
```

Looking for the files | Credit: Mercury

Create a new image

Next, run the following command to create a new image that contains the text file you want to hide.

```
steghide embed -ef <data> -cf <image> -sf <stego_image> -v
```

Let's take a look at the command:

- **steghide** – We specify the tool to use
- **embed** – Tells the tool we want to embed data
- **-ef** – Embed file, specifies the file to hide
- **-cf** – Cover file, specifies the cover image
- **-sf** – Stego file, creates a duplicate of the original image with the embedded file in it

Learn to code – free 3,000-hour curriculum

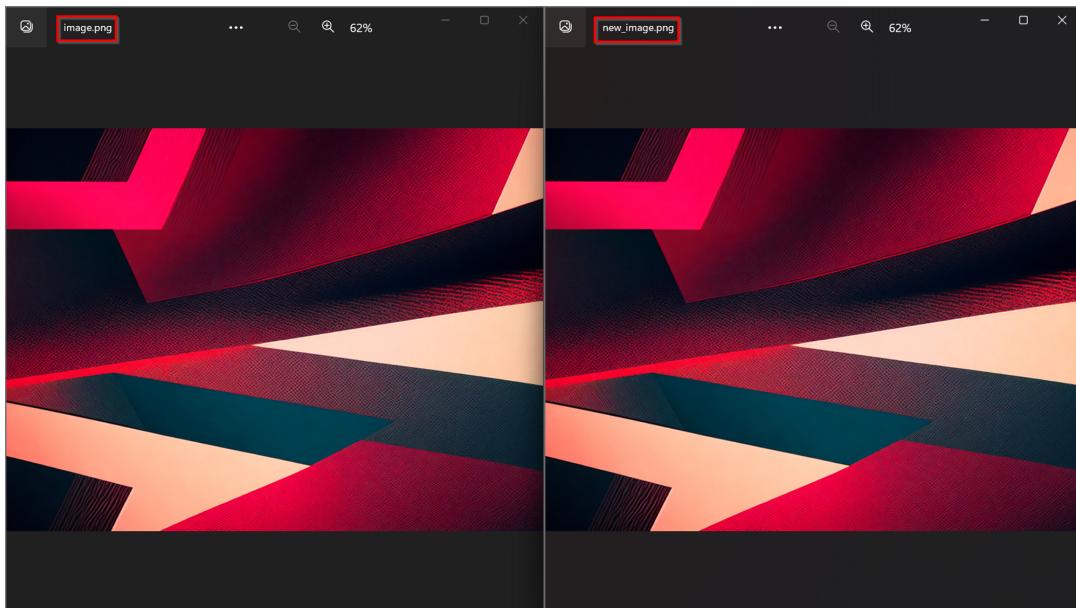
When the command is run, you will be asked to enter a password. If you want an extra layer of security, you might want to do this. If you don't, just hit enter twice. Here's the result of what I ran:

```
(mercury@pluto)-[~/Documents/steganography_tutorial]
$ steghide embed -ef information.txt -cf image.png -sf new_image.png -v
Enter passphrase:
Re-Enter passphrase:
reading secret file "information.txt"... done
reading cover file "image.png"... done
creating the graph... 102 sample values, 298 vertices, 37393 edges
executing Static Minimum Degree Construction Heuristic... 100.0% (1.0) done
writing stego file "new_image.png"... done
```

Embedding the information | Credit: Mercury

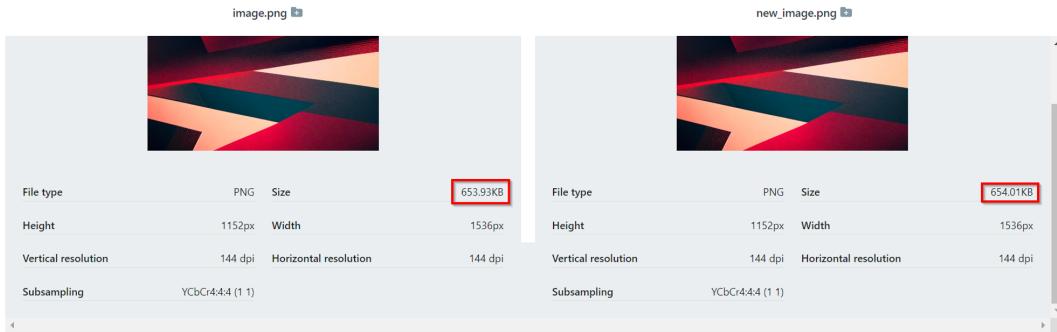
Inspect the new file

Now let's take a look at the new file.



Comparing the images side by side | Credit: Mercury

Learn to code – free 3,000-hour curriculum



Comparing the images details | Credit: Mercury

Extract the data

The stego file is slightly bigger than the original because it contains information. We can extract the data from the stego file using the command below.

```
steghide extract -sf <stego_image> -xf <extracted_data>
```

Let's review the command above:

- **-sf** – stego file, the image containing hidden data
- **-xf** – extract file, the file with extracted data

Below is the screenshot from running the command. The extracted text is also shown below.

Learn to code – free 3,000-hour curriculum

```
(mercury@pluto)-[~/Documents/steganography_tutorial]
$ cat extracted_data.txt
This is a random text file
```

Extracting the information | Credit: Mercury

If you extracted the text, Congratulations 🎉. You have successfully hidden and extracted the text from the image. You can do this with a number of things, even whole books.

Using a different tool called Stegcore, I hid a text file containing Quincy Larson's new book, "[How to Learn to Code & Get a Developer Job](#)", behind an image of the book 📚.

Here's an excerpt from the book.

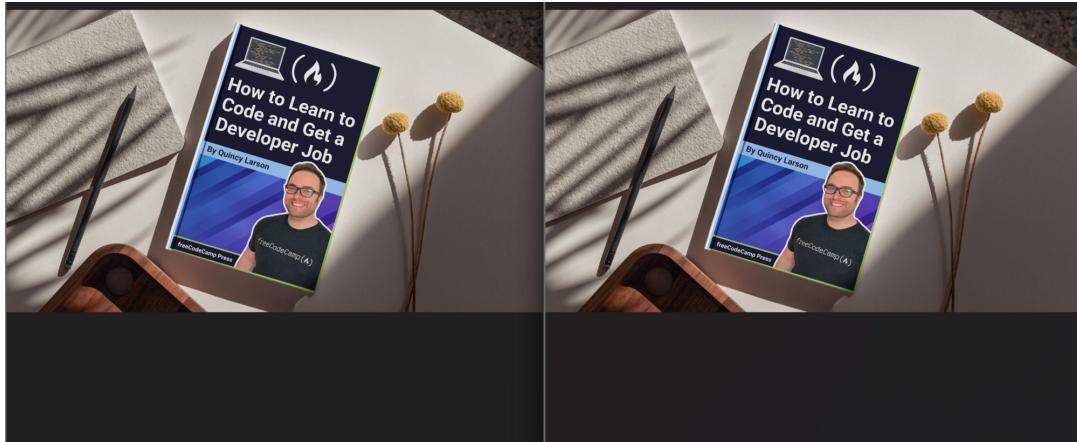
```
January 6, 2023 /#Learn To Code
How to Learn to Code & Get a Developer Job [Full Book]
Quincy Larson

If you want to learn to code and get a job as a developer, you're in the right place. This book will show you how.
And yes this is the full book - for free - right here on this page of freeCodeCamp.
Update June 19, 2023: By popular request, I've added more insights throughout the book about Generative AI tools like GPT-4, and how they're affecting software development.
A few years back, one of the Big 5 book publishers from New York City reached out to me about a book deal. I met with them, but didn't have time to write a book. Well, I finally had time. And I decided to just publish this book for free, right here on freeCodeCamp.
```

An excerpt from the book | Credit: Quincy Larson

And just like before, the text was embedded into a new image. Here is the original and the stego image side by side.

Learn to code – free 3,000-hour curriculum



The original image compared to the stego image | Credit: Mercury

And as expected, the stego image is slightly larger in size than the original.

learn_to_code.png				stego image.png			
File type	PNG	Size	1.31MB	File type	PNG	Size	1.44MB
Height	720px	Width	1280px	Height	720px	Width	1280px
Vertical resolution	144 dpi	Horizontal resolution	144 dpi	Vertical resolution	144 dpi	Horizontal resolution	144 dpi
Depth	8-bit	Format	RGB	Depth	8-bit	Format	RGB
Filter	Adaptive	Interlace	Noninterlaced	Filter	Adaptive	Interface	Noninterlaced

The image details side by side | Credit: Mercury

Talk about hiding a book behind a book (bad joke, I know 😂). If you want to try it out, you can check out the Github [repository](#) or the [app](#).

Conclusion

You've learned what steganography is and how to implement it using tools. Keep in mind that steganography is a tool and can be

Learn to code – free 3,000-hour curriculum

Once again, this tutorial is for educational purposes only and is to be used to help and defend information from black hat hackers. Stay safe in the online jungle and happy hacking 😊.

Acknowledgements

Thanks to [Anuoluwapo Victor](#), [Chinaza Nwukwa](#), [Holumidey Mercy](#), [Favour Ojo](#), [Georgina Awani](#), and my family for the inspiration, support and knowledge used to put this together. I appreciate all of you.

If you want articles similar to this one, hit me up on [Upwork](#) or read more of my articles [here](#).

Cover image credit: Abstract Data Cube | Credit: [Shubham Dhage](#).



Daniel Iwugo

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet

If you read this far, tweet to the author to show them you care.

[Tweet a thanks](#)

Learn to code for free. freeCodeCamp's open source curriculum has helped more than 40,000 people get jobs as developers.

[Get started](#)