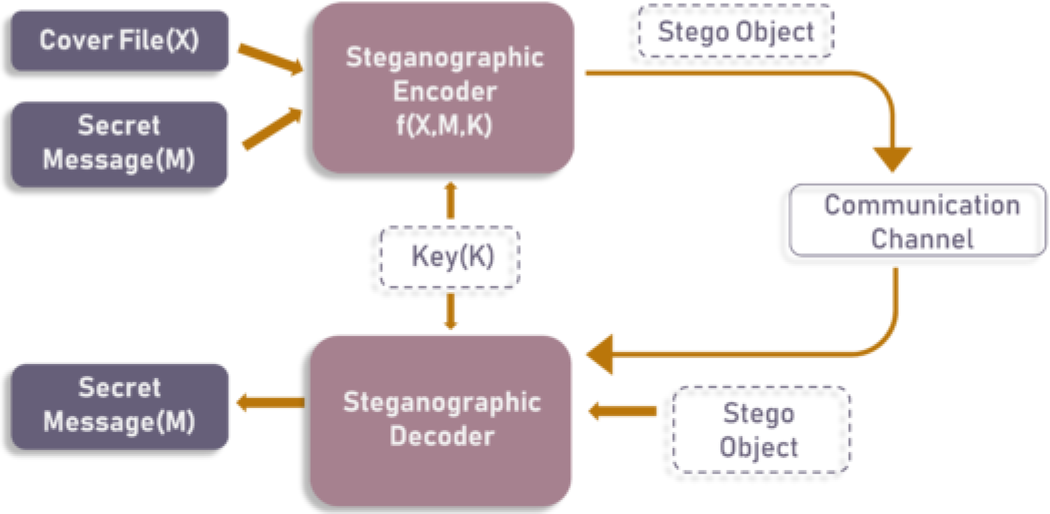
Steganography

What is Steganography?

Steganography is the art and science of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message

The diagram below depicts a basic steganographic model.



As the image depicts, both cover file(X) and secret message(M) are fed into steganographic encoder as input. Steganographic Encoder function, f(X,M,K) embeds the secret message into a cover file. Resulting Stego Object looks very similar to your cover file, with no visible changes. This completes encoding. To retrieve the secret message, Stego Object is fed into Steganographic Decoder.

Steganography Tutorial: Historical Background

Steganography is the practice of concealing a secret message behind a normal message. It stems from two Greek words, which are *steganos*, means covered and *graphia*, means writing. Steganography is an ancient practice, being practiced in various forms for thousands of years to keep communications private. For Example:

- The first use of steganography can be traced back to 440 BC when ancient Greece, people wrote messages on wood and covered it with wax, that acted as a covering medium
- Romans used various forms of Invisible Inks, to decipher those hidden messages light or heat were used
- During World War II the Germans introduced microdots, which were complete documents, pictures, and plans reduced in size to the size of a dot and were attached to normal paperwork
- Null Ciphers were also used to hide unencrypted secret messages in an innocent looking normal message

Now, we have a lot of modern steganographic techniques and tools to make sure that knows our data remains secret. Now you might be wondering if steganography is same as cryptography. No, they are two different concepts

How is Steganography different from Cryptography?

At their core, both of them have almost the same goal, which is protecting a message or information from the third parties. However, they use a totally different mechanism to protect the information.

Cryptography changes the information to ciphertext which cannot be understood without a decryption key. So, if someone were to intercept this encrypted message, they could easily see that some form of encryption had been applied. On the other hand, steganography does not change the format of the information but it conceals the existence of the message.

	STEGANOGRAPHY	**CRYPTOGRAPHY**
Definition	It is a technique to hide the existence of communication	It's a technique to convert data into an incomprehensible form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn't alter the overall structure of data	Alters the overall structure of data

Key	Optional, but offers more security if used	Necessary requirement
Failure	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext

So, in other words, steganography is more discreet than cryptography when we want to send confidential information. The downside being, the hidden message is easier to extract if the presence of secret is discovered. For the remainder of this steganography tutorial, we will learn about different steganography techniques and tools.

Steganography Techniques

Depending on the nature of the cover object(actual object in which secret data is embedded), steganography can be divided into five types:

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

Text Steganography

Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts. Various techniques used to hide the data in the text are:

- Format Based Method
- Random and Statistical Generation
- Linguistic Method

Image Steganography

Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used cover source because there are a huge number of bits present in the digital representation of an image. There are a lot of ways to hide information inside an image. Common approaches include:

- Least Significant Bit Insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Coding and Cosine Transformation

Audio Steganography

In audio steganography, the secret message is embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a much more difficult process when compared to others, such as Image Steganography. Different methods of audio steganography include:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding
- Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files.

Video Steganography

In Video Steganography you can hide kind of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds. You can think of this as the combination of Image Steganography and Audio Steganography. Two main classes of Video Steganography include:

- Embedding data in uncompressed raw video and compressing it later
- Embedding data directly into the compressed data stream

Network Steganography (Protocol Steganography)

It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you can find in the OSI model. For Example, you can hide information in the header of a TCP/IP packet in some fields that are either optional.

In today’s digitalized world, various software tools are available for Steganography. In the remainder of this Steganography Tutorial, we will explore some of the popular steganographic tools and their capabilities.

Best Tools to Perform Steganography

There are many software available that offer steganography. Some offer normal steganography, but a few offer encryption before hiding the data. These are the steganography tools which are available for free:

- ***Stegosuite*** is a free steganography tool which is written in Java. With Stegosuite you can easily hide confidential information in image files.
- ***Steghide*** is an open source Steganography software that lets you hide a secret file in image or audio file.
- ***Xiao Steganography*** is a free software that can be used to hide data in BMP images or in WAV files.
- ***SSuite Picsel*** is another free portable application to hide text inside an image file but it takes a different approach when compared to other tools.
- ***OpenPuff*** is a professional steganographic tool where you can store files in image, audio, video or flash files