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..

Types of Steganography

1. Text steganography

Text steganography conceals a secret message inside a piece of text. The simplest version of text steganography might use the first letter in each sentence to form the hidden message. Other text steganography techniques might include adding meaningful typos or encoding information through punctuation.

2. Image steganography

In image steganography, secret information is encoded within a digital image. This technique relies on the fact that small changes in image color or noise are very difficult to detect with the human eye. For example, one image can be concealed within another by using the least significant bits of each pixel in the image to represent the hidden image instead.

3. Video steganography

Video steganography is a more sophisticated version of image steganography that can encode entire videos. Because digital videos are represented as a sequence of consecutive images, each video frame can encode a separate image, hiding a coherent video in plain sight.

4. Audio steganography

Audio files, like images and videos, can be used to conceal information. One simple form of audio steganography is "backmasking," in which secret messages are played backwards on a track (requiring the listener to play the entire track backwards). More sophisticated techniques might involve the least significant bits of each byte in the audio file, similar to image steganography.

5. Network steganography

Network steganography is a clever digital steganography technique that hides information inside network traffic. For example, data can be concealed within the TCP/IP headers or payloads of network packets. The sender can even impart information based on the time between sending different packets.

More recently, digital steganography has emerged as a practice with both legitimate and criminal uses. The different algorithms in digital steganography include:

- **Least significant bit (LSB):** In the LSB algorithm, the least significant bit in each byte of a multimedia file (e.g., an image or audio) is modified to convey a hidden message.
- Multi-access edge computing can also help save on bandwidth costs and improve security by processing data locally instead of sending it over the network to central servers.
- **Discrete Fourier transform (DFT):** In the DFT algorithm, information is hidden inside a multimedia file using the mathematical technique of discrete Fourier transformation.