**steganography technology and countermeasures-**

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

**Difference Between Steganography, Cryptography, and Obfuscation**

Steganography, cryptography, and obfuscation are three related terms; they all refer to practices that make data more difficult to understand. However, these words are not interchangeable — subtle yet crucial distinctions exist between them.

Below are the differences between steganography, cryptography, and obfuscation:

Cryptography attempts to encode a message, making it difficult or impossible for anyone except the intended recipient to decrypt it. The encoding and decoding process is accomplished using cryptographic keys that translate back and forth between the true message and its encrypted version.

Steganography attempts to hide a message within another object. Not only does steganography seek to make this information harder to understand, but it also seeks to conceal that a message is being sent in the first place.

Obfuscation is any technique that prevents third parties from understanding a message. For example, a program’s source code may be obfuscated by removing the whitespace, making the message difficult for humans to read.

Note that steganography and cryptography are not mutually exclusive. For example, steganography could hide a message inside another file using encryption for extra security. The recipient could then extract the encrypted message and decrypt it using a given key.

Examples of Steganography

Steganography has been in use for centuries. Basic physical forms of steganography include invisible ink that can only be read by exposing it to heat and messages written under the postage stamps of an envelope.

However, clever practitioners of steganography have developed a range of more sophisticated techniques that work in various mediums. One example is a laser printer’s Machine Identification Code (MIC), a unique identifier encoded on any printed document using tiny yellow dots that are invisible to the naked eye. Secret messages can even use the letters of a crossword or the numbers of a sudoku puzzle.

More recently, digital stenography 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.

The good news for users of steganography is that they don’t have to code these algorithms from scratch. Instead, different programming languages come with pre-built steganography libraries and frameworks. For example, the Python Stegano module can hide messages within an image (PyPI), while the ImageSteganography library does the same for C++ programmers (GitHub, 2022).

In the next section, we’ll go over five of the most common types of digital stenography.

What Are the 5 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

Last but not least, 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.

Steganography Tools and Techniques

There are many different types of steganography — so how can you get started? Fortunately, there are a number of tools for using steganography online.

OpenStego is an open-source steganography tool that offers two main functionalities: data hiding and watermarking (i.e., hiding an invisible signature). As of this writing, OpenStego works only for image files (Vaidya, S).

Another free steganography tool (though not open-source) is OpenPuff. The OpenPuff software supports steganography in image, audio, and video files and can even split a message across multiple files (EmbeddedSW).

How Do Malicious Hackers Use Steganography?

As you might imagine, steganography can be used for both good and ill. For instance, dissidents living under oppressive regimes can use steganography to hide messages from the government, passing sensitive information within a seemingly innocuous medium.

However, digital steganography is also a tool for malicious hackers. An attacker can hide the source code for a malware application inside another supposedly harmless file (such as a text file or an image). A separate program can then extract and run the source code.

In June 2020, for example, security researchers at Malwarebytes discovered that malicious actors had hidden code for a web skimmer inside the EXIF metadata of an image file. When executed, this code silently captured the details of users as they entered their names, addresses, and payment card information on e-commerce websites (Segura, 2020).