Steganography: Steganography Process, watermarking. Steganography Methods and Attacks, Steganography tools

What Is Steganography?

- It comes from the Greek words steganos, which means “covered” or “hidden,” and graph, which means “to write.” Hence, “hidden writing.”
- A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection.
- “Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data” .So, the sentence is saying that you can combine encryption (to make data secure with decryption key) with steganography (to make the fact that data is being concealed less obvious) as an additional layer of protection for sensitive information.
- You can use steganography to hide text, video, images, or even audio data

Steganography Process :

The process of steganography involves hiding data within another file or medium in a way that makes the presence of the hidden data difficult to detect. Here's a general overview of the steganography process:

1. **Select Data to Hide**: Choose the data you want to hide. This could be a message, a file, or any information you wish to keep confidential or covertly transmit.

2. **Select Cover Medium**: Choose a cover medium, which is the file or object in which you will hide the data. Common choices include images, audio files, videos, or even text documents. The cover medium will carry the hidden data.

3. **Choose Steganography Tool/Method**: Select a steganography method or tool that suits your purpose and is compatible with the cover medium you've chosen. There are various steganography techniques, including LSB replacement, frequency domain methods, and more.

4. **Embed Data**: Use the steganography tool to embed the selected data into the cover medium. The process of embedding involves altering the cover medium in a way that hides the data. The specific steps for embedding will depend on the steganography method you've chosen.

5. **Key/Password (Optional**): Some steganography tools allow you to use a key or password to enhance security. Without the key or password, it should be difficult or impossible to extract the hidden data.

6. **Verify the Process**: After embedding the data, verify that the process was successful. Make sure that the cover medium still appears normal to the human eye or ear and that the hidden data can be extracted correctly.

7. **Transmit or Store:** Depending on your purpose, you can now transmit the steganographically altered cover medium, store it securely, or share it as needed.

8. **Extract Hidden Data:** To retrieve the hidden data, you or the intended recipient need access to the steganography tool and, if applicable, the key or password. Use the tool to extract the concealed data.

9. **Decryption/Decoding (If Applicable):** Depending on the steganography method used, you might need to decrypt or decode the extracted data to obtain the original information.

10. **Maintain Security:** Ensure the security of the hidden data and be mindful of who has access to the steganographically altered cover medium and any associated keys or passwords.

It's important to note that steganography can be used for both legitimate and malicious purposes. Ethical and responsible use is essential. Additionally, some applications or platforms may have mechanisms in place to detect or prevent steganography, so consider the context and legality of your actions when using steganography techniques.

Watermarking:

Digital Watermarking is use of a kind of marker covertly embedded in a digital media such as audio, video or image which enables us to know the source or owner of the copyright. This technique is used for tracing copyright infringement in social media and knowing the genuineness of the notes in the banking system.

Types of Watermarks :

1. **Visible Watermarks –** These watermarks are visible.
2. **Invisible Watermarks –** These watermarks are embedded in the media and use steganography technique. They are not visible by naked eyes.
3. **Public Watermarks –** These can be understood and modified by anyone using certain algorithms. These are not secure.
4. **Fragile Watermarks –** These watermarks are destroyed by data manipulation. There must be a system which can detect all changes in the data if fragile watermarks are to be used.

Digital watermarking process (Life cycle) : The information needs be embedded in the media. The signal which is embedded is the host signal and the information is called digital watermark. The process has 3 main parts:

1. **Embed –** In this part, the digital signal is embedded with the digital watermark.
2. **Attack –** The moment when the transmitted media is changed, it becomes a threat and is called an attack to the watermarking system.
3. **Protection –** The detection of the watermark from the noisy signal which might have altered media (JPEG compression, rotation, cropping, and adding noise) is called Protection.

Applications :

- Watermarks are used in forensics. Tampered evidence is unacceptable in forensics and Watermarked images are acceptable.
- This is used by brands. The Digital Watermarking is done so that the authority of the digital media is intact.
- Digital Watermarking prevents copying of the data.
- Video editing software use watermarks so that people buy the full version of it.
- It is used in video authentication. News channels often show videos of other agencies which are watermarked. It is also used for ID card security.
- It is used for content management in social media.

Advantages :

- It is used in detecting copyright infringements of digital content.
- Watermarking is a very secure technique. The embedding of watermarks is done by a key. Anyone who wants to remove the watermark can only do this with the knowledge of the keys involved in embedding.
- The embedded version of a file is also digital in nature which can be transmitted and used easily. No change in file format ensures that there is no error or difficulty in using watermarked media.

Disadvantages :

- Watermarks that are visible are easily removed or overlayed by other watermarks.
- There still needs to be invention of more robust techniques to watermark pictures. The pictures with watermarks are easily resized and the watermarks can be cropped.
- The owners can remove watermarks easily. This means that if anyone on the owner side can easily manipulate the image and alter the watermark.

Steganography Methods:

Steganography methods involve techniques for hiding information within other data in a way that is difficult to detect. Here are some common steganography methods:

1. **Image Steganography:** Concealing data within images is one of the most popular forms of steganography. There are various techniques for image steganography, including:

a. **LSB (Least Significant Bit) Replacement**: This method involves replacing the least significant bits of the pixel values in an image with the hidden data. This change is often imperceptible to the human eye.

b. **Frequency Domain Methods:** Transforming the image into the frequency domain (e.g., using Fourier transforms) and embedding data in the frequency components, such as the amplitude or phase of the image.

c. **Spread Spectrum:** This method spreads the hidden data across the entire image to minimize the chances of detection.

2. **Audio Steganography:** Similar to image steganography, audio steganography hides information within audio files. Techniques include altering the amplitude of audio samples, modifying the phase of audio signals, or using spread spectrum methods within the audio data.

3. **Text Steganography:** Concealing data within text documents by subtly manipulating the text or introducing hidden characters or spaces. This method is less common but can be used for covert communication.

4. **Video Steganography:** Embedding data within video files, which is a combination of image and audio steganography techniques applied to video frames and the associated audio stream.

5. **File Steganography:** Hiding data within any type of file, such as documents, PDFs, or executable files, by subtly altering their content or structure.

6. **Network Steganography:** Concealing data within network protocols, headers, or payloads to covertly transmit information over a network. This can involve manipulating packet headers or using specific communication channels that are less likely to attract attention.

7. **Social Media Steganography:** Using social media platforms and websites to hide information within images, comments, or posts. This can involve embedding data in the images or using subtle encoding in text.

8. **Printer and Scanner Steganography:** Manipulating the printed or scanned output of documents to hide data through variations in printing or scanning processes.

It's important to note that steganography can be used for both legitimate purposes, such as digital watermarking, copyright protection, and covert communication for security reasons, as well as for malicious activities like data exfiltration or cyber-espionage. As a result, it's crucial for security professionals to be aware of steganography and employ techniques to detect and counteract it when necessary.

Steganography Attacks:

Use of Steganography in Cyberattacks

Cybercriminals are now leveraging steganography as an attack vector to hide malicious JavaScripts and malware within the images and distribute them to targets. When the victim clicks the malicious image, the malware embedded in the image automatically downloads the malicious code or malware, infecting the targeted system.

Types of Steganography Attacks

Based on the targets, the attackers use different types of steganography attacks, which include:

1. Text Steganography

In a Text Steganography attack, hackers conceal information (malware code) inside the text files. Bad actors do this by altering the text format in the existing file, such as changing words, creating random characters or sentences.

2. Image Steganography

Attackers hide malicious data in images in an Image steganography attack. They exploit the large number of bits or pixels in an image and replace them with malware codes. Threat actors leverage different tactics to establish image steganography attacks, including the

Least significant bit insertion, Masking and Filtering, Pattern encoding, Coding, and Cosine transformation methods.

3. Audio Steganography

In an Audio steganography attack, threat actors exploit WAV audio files to hide their customized malware. Attackers embed the malicious code within the WAV audio files that contain a loader component to decode and execute malicious content embedded in audio files.

4. Video Steganography

Video steganography is a combination of both text and image-based steganography attacks. Adversaries embed a large amount of malicious data inside the moving stream of images and audio files.

How Do You Prevent Steganography Attacks?

- Avoid employees downloading software and other applications from unknown sources as they may contain steganographic codes.
- Never click/open/download suspicious text/audio/image files from unknown sources.
- Closely monitor the software distribution procedures in your organizations to identify malicious insiders.
- Train employees on various phishing and social engineering lures.
- Use anti-malware tools to identify the presence of malware in the files, text docs, images received from unknown sources.

Steganography tools :

There are various steganography tools available for embedding and extracting hidden data within cover media. Here are some popular steganography tools:

1. **OpenStego**: OpenStego is an open-source steganography software that allows users to hide data within images and other files. It provides several steganography techniques and is available for Windows, macOS, and Linux.

2. **Steghide**: Steghide is a command-line tool that specializes in hiding data in image and audio files. It is available for various platforms, including Linux, Windows, and macOS.

3. **OutGuess**: OutGuess is a steganography tool that can hide data within images. It is known for its robustness and ability to withstand various steganalysis techniques. It is available for Windows and Linux.

4. **Steganography Studio**: Steganography Studio is a user-friendly Windows-based tool for hiding data within images. It supports several steganography methods and encryption for added security.

5. **S-Tools**: S-Tools is a classic steganography software that can hide data in images and audio files. It's available for Windows and is known for its simplicity.

6. **Hide and Reveal**: Hide and Reveal is a user-friendly steganography tool for Windows. It allows users to easily hide text within images and reveal hidden messages.

7. **Xiao Steganography**: Xiao Steganography is an open-source steganography tool for Windows that supports image and audio file hiding. It also offers the option to password-protect hidden data.

8. **QuickStego**: QuickStego is a simple steganography tool for hiding text within images. It's available for Windows and is known for its ease of use.

9. **Image Steganography**: Image Steganography is a web-based steganography tool that allows users to hide text within images online without the need for software installation.

10. **StegFS**: StegFS is a steganography tool that takes a different approach by creating a virtual file system within an encrypted container. It's available for Linux and is designed for secure data storage.

Please note that the use of steganography tools should always adhere to legal and ethical standards. Misuse of steganography for malicious purposes is illegal and unethical. Additionally, be aware that some security systems and forensic tools are capable of detecting steganography, so it's important to consider the context and legal implications of using such tools.