Digital Steganography

Dr. Shubhangi Sapkal

Information hiding: History

- The idea of communicating secretly is as old as communication itself. In this section, we briefly discuss the historical development of information hiding techniques such as steganography/ watermarking.
- Early steganography was messy. Before phones, before mail, before horses, messages were sent on foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger.
- While information hiding techniques have received a tremendous attention recently, its application goes back to Greek times. According to Greek historian Herodotus, the famous Greek tyrant Histiaeus, while in prison, used unusual method to send message to his son-in-law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-inlaw.

Information hiding: History

- The second story also came from Herodotus, which claims that a soldier named Demeratus needed to send a message to Sparta that Xerxes intended to invade Greece.
- Back then, the writing medium was written on wax-covered tablet. Demeratus removed the wax from the tablet, wrote the secret message on the underlying wood, recovered the tablet with wax to make it appear as a blank tablet and finally sent the document without being detected.
- Invisible inks have always been a popular method of steganography. Ancient Romans used to write between lines using invisible inks based on readily available substances such as fruit juices. When heated, the invisible inks would darken, and become legible.

Information hiding: History

- Later chemically affected sympathetic inks were developed. Invisible inks were used as recently as World War II.
- Modern invisible inks fluoresce under ultraviolet light and are used as anti-counterfeit devices. For example, "VOID" is printed on checks and other official documents in an ink that appears under the strong ultraviolet light used for photocopies.

Information hiding: History

- During World War II, null ciphers (unencrypted message) were used to hide secret messages. The null cipher, which often appeared to be innocent message about ordinary occurrences, would not alert suspicion, and would thus not be intercepted.
- For example, the following message was sent by German spy during WWII.
- Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.
- Decoding this message by taking the second letter in each word reveals the following secret message.

What is Steganography?

- Steganography or Stego as it often referred to in the IT community, literally means, “Covered writing” which is derived from the Greek language.
- Steganography is defined as follows, “Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present”.
- In a digital world, Steganography and cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security.

Steganography Vs Cryptography

- The term Steganography means, “cover writing” whereas cryptography means “secret writing”.
- Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message.
- The message we want to send is called plain text and disguised message is called cipher text. The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption.
- Encryption protects contents during the transmission of the data from sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is the clear.
- Steganography hides messages in plain sight rather than encrypting the message; it is embedded in the data (that has to be protected) and doesn’t require secret transmission. The message is carried inside data.

Steganography Vs Cryptography

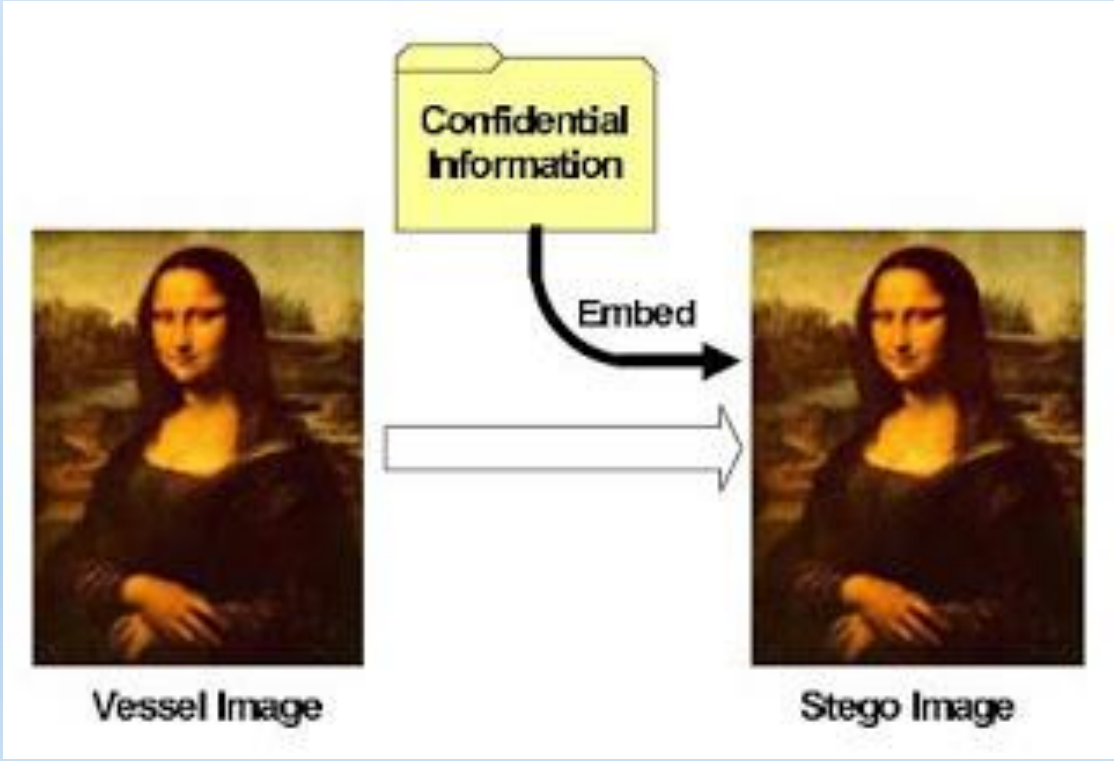
- Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as Internet.
- Steganographic research is primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment. Many Governments have created laws that either limit the strength of cryptosystems or prohibit them completely.
- This unfortunately leaves the majority of the Internet community either with relatively weak and a lot of the times breakable encryption algorithms or none at all. This is where Steganography comes in.

Steganography Vs Cryptography

- Steganography can be used to hide important data inside another file so that only the parties intended to get the message even knows a secret message exists. It is a good practice to use Cryptography and Steganography together.
- Neither Steganography nor Cryptography is considered “turnkey solutions” to open systems privacy, but using both technologies together can provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems.

Steganography

- The art of hiding data in a file so that only the sender and intended recipient suspect the presence of hidden data
  - A form of security through obscurity
- Very easy to accomplish
- Harder to detect and decrypt
- BMP, JPG, TXT, HTML/XML, PDF, PNG, GIF, AU, WAV, MP3, AVI, TIF, TGA, DLL, EXE



Steganography

- As cryptanalysis is the counterpart of cryptography, steganalysis is the counterpart of steganography.
- A *steganalyst* tries to determine the existence of a covert communication channel between two parties and either break or alter their communication.
- While cryptology states that a cipher is broken when the attacker is able to gain information on the content of the payload, a steganography technique is considered broken when its mere existence is proven.

Steganography

- The main purpose of Steganography, which means ‘writing in hiding’ is to hide data in a cover media so that others will not be able to notice it.
- While cryptography is about protecting the content of messages, steganography is about concealing their very existence

Steganography

- Steganography equation is ‘Stego-medium = Cover medium + Secret message + Stego key’.
- The general model of data hiding can be described as follows. The embedded data is the message that one wishes to send secretly. It is usually hidden in an innocuous message referred to as a cover-text or cover-image or cover-audio as appropriate, producing the stego-text or other stego-object.
- A stego-key is used to control the hiding process so as to restrict detection and /or recovery of the embedded data to parties who know it.

Steganography

- While steganography can be achieved using any cover media, we are concerned with hiding data in digital images.
- The features expected of a stego-medium are imperceptibility and robustness, so that the secret message is known only to the intended receiver and also the stego-medium being able to withstand attacks from intruders.
- The amount of secret message embedded should be such that it doesn’t reduce the quality of the stego image.
- The goal of steganography is to embed secret data into a cover in such a way that no one apart from the sender and intended recipients even realizes there is secret data.

Steganography - Applications

- The applications of information hiding systems mainly range over a broad area from military, intelligence agencies, online elections, internet banking, medical-imaging and so on.
- These variety of applications make steganography a hot topic for study. The cover medium is usually chosen keeping in mind the type and the size of the secret message and many different carrier file formats can be used.
- In the current situation digital images are the most popular carrier/cover files that can be used to transmit secret information.

Classification of Steganographic methods

- Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.
- Secret key steganography where the stego key is exchanged prior to communication.
- Public key steganography where a public key and a private key is used for secure communication.

CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

1. Spatial Domain Techniques
2. Transform Domain Techniques
3. Spread Spectrum
4. Statistical Method
5. Distortion Technique

Spatial Domain

- These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity.
- The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image.
- Moreover these embedding algorithms are applicable mainly to lossless image compression schemes like TIFF images. For lossy compression scheme like JPEG, some of message bits get lost during compression step.

Transform Domain

- These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in transform domain is widely used for robust watermarking.
- Similar techniques can also realize large capacity embedding for Steganography. Candidate transforms include discrete cosine Transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT).

- By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. Eg: we can perform a block DCT and, depending on pay-load and robustness requirements, choose one or more components in each block to form a new data group that, in turn, is pseudo randomly scrambled and undergoes a second-layer transformation.
- Modification is then carried out on double transform domain coefficients using various schemes.
- These techniques have high embedding and extraction complexity. Because of robustness properties of transform domain embedding, these techniques are more applicable to “Watermarking” aspect of data hiding.

Spread Spectrum

- Spread spectrum transmission in radio communication transmit message below level of noise frequency.
- In Steganography it deals either with cover image as noise or tries to add as pseudo-noise in the cover image.
- Cover Image As Noise: A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This means that the channel capacity of the image changes significantly. Thus, while this value can be a real number, in practice, the difficulty in recovering a real number decreases the value to a single bit.

- To permit the transmission of more than one bit, the cover image has to be broken into sub images. When these sub cover images are tiles, the technique is referred to as direct-sequence spread spectrum Steganography.
- When the sub cover images consist of separate points distributed over the cover image, the technique is referred to as frequency-hopping spread-spectrum Steganography. These techniques require searching the image for the carrier in order to then retrieve the data.
- These techniques are robust against gentle JPEG compression and can be made more robust through the pre-distortion of the carrier.

STATISTICAL METHODS

- Also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process.
- This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation.
- Statistical Steganography techniques exploit the existence of a “1-bit”, where nearly a bit of data is embedded in a digital carrier.

STATISTICAL METHODS

- This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if “1” is transmitted, otherwise it is left unchanged.
- To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message.

Distortion Technique

- It require original cover image during decoding process where decoder functions to check for differences between original cover image and distorted cover image in order to restore secret message.
- Encoder, adds a sequence of changes to cover image. So, information is described as being stored by signal distortion .
- Using this technique, a stego-object is created by applying sequence of modifications to cover image. This sequence of modifications is selected to match secret message required to transmit. Message is encoded at pseudo-randomly chosen pixels.
- If stego-image is different from cover image at given message pixel, then message bit is a “1.” Otherwise, message bit is a “0.”
- Encoder can modify “1” value pixels in such manner that statistical properties of image are not affected (which is different from many LSB methods).

Steganography Properties

- A few key properties that must be considered when creating a digital data hiding system are
  - Imperceptibility: Imperceptibility is the property in which a person should be unable to distinguish the original and the stego-image.
  - Embedding Capacity: Refers to the amount of secret information that can be embedded without degradation of the quality of the image.
  - Robustness: Refers to the degree of difficulty required to destroy embedded information without destroying the cover image.