The Method of Covering and Hiding Secret Data by using Various Methods: Steganography

Devendra Mhatre
Master of Computer Application

Rahul Yadav
Master of Computer Application

Shweta Jha
EXTC Department

Akansha Bhargava
EXTC Department

Abstract :- **Steganography is the art of hiding information within other information in such a way that it is hard or even impossible to identify the existence of any hidden information. There are many different carriers for steganography. Of which, most popular ones are digital images. Due to recent developments in steganalysis, providing security to personal contents, messages, or digital images using steganography has become difficult. We can understand the secret message by using stegnalysis. This project introduces a novel steganographic approach for covert communications between two private parties. The approach introduced in this project makes use of both steganographic as well as cryptographic techniques. The process involves converting a secret image into a text document, then encrypting the generated text into a ciphertext using a key (password) based encryption algorithm, and finally embedding the ciphertext on to a cover image. This embedding process is carried out using a threshold based scheme that inserts secret message bits into the cover image only in selected pixels. The security to maintain secrecy of message is achieved by making it infeasible for a third person to detect and retrieve the hidden message.**

Keywords – Secret message, covering message, cipher text ,threshold, retrieve

I. INTRODUCTION

Over the years the lack of information security has led to leakage of private information. A lot of recent developments has happened in the field of cryptography . Steganography is useful in situations where sending encrypted messages might raise suspicion, such as in countries where free speech is suppressed. Digital watermark is also used to detect whether the audio files and image is lost to find. And on a less practical note — it's just cool.it is the method to hide the data in form of any secret message with the use of the key. We can use any message as audio, image ,video etc.

II. CRYPTOGRAPHY

There are many possible definitions for cryptography. One of which is, “The computerized encoding and decoding of information” to define cryptography. This is a process of converting a message from a human readable or understandable form(plaintext) to non-understandable format (ciphertext) to enable secure sending and back to original format at other receiving end. The encrypted text in cryptography always shows static information of input text. Many methodologies were introduced that follow their own strategy, but all the methodologies use some patterns. The underlying idea in pattern based approach isto decode the encoded message, that is, using apattern of one’sown choice or a standard pattern, asender encodes the message and thus generates a ciphertext. The receiver usesthe same pattern and decodes the ciphertext to generate message (plaintext). Over a period,cryptographic approaches evolved overphases. It is suggested that a key should be used in the process of encoding and decoding a message. Based on this concept ofkeys, cryptography is further classified into two types, *symmetric-key cryptography* and *public-key cryptography*. In case of symmetric key cryptography, same key has to be used by both sender and the receiver while encoding and decoding respectively. In contrast, in the case of public key cryptography, the keys used by the sender and the receiver are different.

III. STEGANOGRAPHY

It can be defined as "The art and science of communicating in a way which hides the existence of the communication. A steganographic model facilitates hiding or embedding of sender’s secret message in a file (carrier) that does not give out a clue about the existence of secret message in it when viewed. For this, any media format or file format like .bmp, .doc, .gif, .jpeg, .mp3, .ppt, .txt and .wav is taken as a carrier that can act as cover for the sender’s message, that is, a message here is hidden in a carrier and that carrier is transmitted. The underlying operation of this methodology is both logical and technical. In general, a steganography algorithm takes a secret message and a carrier as input and gives a carrier message as output (in which the message is embedded). In the process of steganography, the carrier which hides the message in it will be sent to the receiver. The carrier gives the receiver no information about the message but reveals it only after using the tool or algorithm that is used by the sender. Cryptography and steganography, both the techniques have found usage in many applications. For example, attack transmission plans uses steganography technique to hide information about their strategies in military teams. Many other applications of data hiding techniques other than its original objective, have gained importance, which include authentication and identification, watermarking and transmitting passwords etc.

One way of steganography is hiding image behind video, suppose if we take example of hiding a image of 1 mb behind 200 mb video . it is not possible to understand the secret message whereas if we hide a video 200 mb behind a image of 1mb, then it would be understood that a secret

message is hiding behind the image .it is not possible to hide it that way.

Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in ordinary cover media so as not to arouse an eavesdropper's thought. In the past, people used hidden tattoos or indistinguishable ink to convey steganographic content. Today, computer and network technologies supply easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identify a cover medium's unnecessary bits (those that can be adapted without destroying that medium's integrity).The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence untraceable, but steganographic systems— because of their enveloping nature—leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resultant stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis.

You can hide the information in different ways in which information hiding system contend with each other: capacity, security, and robustness. Capacity defines information hidden in the cover medium, security to an attacker inability to detect hidden information which is covered by medium, and robustness defines the amount of modification the steganographic medium can withstand before an attacker,enemy can destroy hidden information.Information hiding generally defines to both watermarking and steganography. The primary goal of watermarking system is to achieve a high level of robustness—that is, it should be unable to remove a watermark without harming the data quality of object. Steganography, in other way, strives for high security and capacity, which often entails that the hidden information is easily broken or damaged. Even normal modifications to the stego medium can destroy it.

Fig 1: Data hiding in image

IV. TYPES STEGANOGRAPHY

Text Steganography: The methods used in text steganography are number of tabs, spaces, letters, as Morse code is used to assure secret message hiding.

Image Steganography: hiding ourdata as image in steganography is called image steganography. In this method image sharpness intensity is used to hide the message. The 8 bit and 24 bit size images are commonly used.if it hides the information then the image will be larger in size but the larger images need to undergo reduction and the methods are LSB insertion and Masking and filtering.Network Steganography: Hiding our message as network protocol i.e. TCP, UDP, IP etc, where they are used as carrier in method is called network protocol steganography. In the OSI model there are number of layers where some of the message could be sent in any of the layer .

Audio Steganography: Hiding our message in audio is called audio steganography.it is very popoular field in message hiding.it is used in digital form of audio. Many ways can be used in this method.

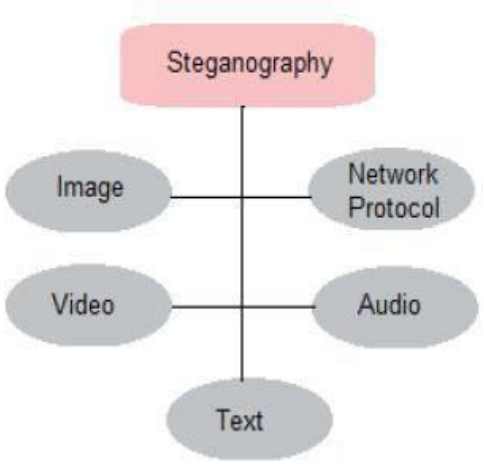

Fig 2 : Stenganography Types

A FEW KEY POINTS THAT MUST BE CONSIDERED TO HIDE DATA :

• 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.

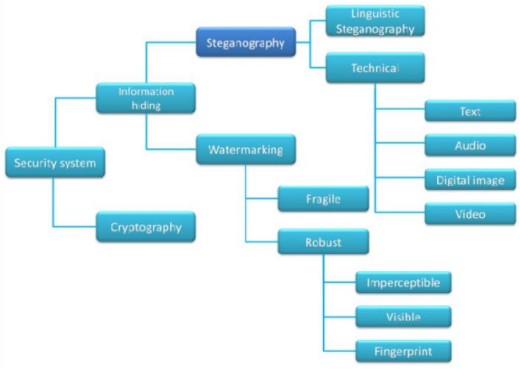

Fig 3 : Steganography

V. STEGANOGRAPHY TERMINOLOGY

Steganography consists of two terms that is message and cover image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it.

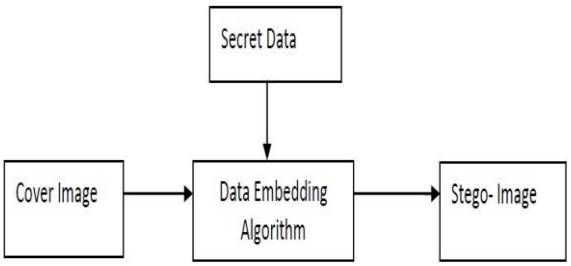

Fig 4 : Steganography

VI. STEGANOGRAPHY TECHNIQUES

1. Spatial Domain Methods: pixels embed the secret data in image intensities. In the process of hiding data some of the values of pixel may get changed .Spatial domain techniques are distinguished into following categories: i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labelling or connectivity method vii) Pixel intensity based

i) LSB: this method of steganography is most commonly used for hiding secret data. To hide the data the bits of secret data is replaced by least significant bits Resultant image obtained is similar to original image as the change in LSB doesn't bring much change in the image

ii) BPCP: complexity is used to measure the segmentation of the desired image. Complexity is used to detect the noisy embedded in the block. the blocks which contain noise of bit plan are replaced by 0 and 1 i.e binary pattern mapped from secret message .

iii) PVD: Here in this process 2 successive pixels of image are chosen for embedding the data. coPayload is determined by checking the dissimilarity between 2 successive pixels and then it decides whether 2 pixels fit in to same edge area or not.

2. Spread Spectrum Technique: The technique of spread spectrum is used in steganography. In this process the secret data is extended over a wide area of frequency bandwidth. Signal to noise ratio in any frequency band must be so small so that it becomes difficult to ensure the presence of data. Still if some part of data is removed from frequency band, there would be enough information is present there to recover the lost secret data.so it is difficult to eliminate the secret data fully without entirely destroying the cover part. Although it is used in many places but it finds its main application in military communication.

3. Statistical Technique: In the process data is embedded by altering quite a few properties of the cover image. It includes the separating of cover image into blocks and then embedding one data bit in each block of image. The cover block image is customized only when the size of data bit is one or no changes are necessary.

4. Transform Domain Technique: In this technique; the secret data is embedded in the transform or frequency domain of the cover part of image It is one of the complex method of hiding secret data message .dissimilar algorithms and transformations are used on the image part to hide secret data in it. Transform domain techniques are distinguished such as i) Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT) iv)Embedding in coefficient bits

5. Distortion Techniques: In this method the secret data message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder block actions the dissimilarity between the original image and the distorted image to notice the series of modifications and thus will get the secret data.

6. Masking and Filtering: These techniques hide information by marking an image. Steganography only hides the information where as watermarks becomes a potion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images.

VII.CONCLUSION

Steganography is used in many places as,to keep confidential message transmission and reception . one of the use of steganography is in defense for security that is to hide secret message under water mark which is undetectable by naked eyes. It prevents eve teasing from the outside world

PROCEEDINGS PAPERS:

[1] Some New Methodologies for Image Hiding using Steganographic Techniques Rajesh Kumar Tiwari and Gadadhar Sahoohttps://www.techopedia.com/definition/4131/steganography
[2] Steganography and classification of image steganography techniques rk bansal , savita bansal
[3] Steganography Techniques –A Review Paper Jasleen Kour Deepankar Verma
[4] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON- 2008, (2008) November, pp. 1-6.
[5] [15] M. Chaumont and W. Puech, "DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, (2006) September 4-8.
[6] [16] A. M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, (2009).
[7] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.
[8] A research Paper on Cryptography Encryption and Compression Techniques Sarita Kumar