Steganography-A Data Hiding Technique

Vinita Haridas
St.Joseph's college,
Irinjalakuda

***Abstract*--In this paper, steganography –a data hiding technique is presented. The techniques and methods used for implementing this steganography is discussed. Steganography word is from the greek word "steganos" the meaning is secret or covered & graphy means writing or drawing. The need of keeping up privacy in the communication between the two people in internet world is great concern in today's world. For this steganography technique has brought some concepts together which are cryptography, modern data compression, spread spectrum etc. This technique was being used long back from 2500 years in various forms. This paper tries to cover the various techniques by using various algorithms to secure the messages hidden in it.**

I. INTRODUCTION

In all areas of work the basic need is the communication. Each person want to keep some of their conversation or data safe and away from other people. Steganography is the concept in which we hide the confidential data into cover image, audio, video etc, and the intermediate observer will not be able to notice with naked eyes. This technique uses to replace the unused data bits in files by different bits of invisible information. As this information can be in any form a plain text, cipher text or an image. Cryptography is about protecting the content of messages (their meaning). Steganography is about concealing the existence of messages The goal of steganography is not to draw attention to the hidden information that is to be transmitted. And if the introducer is able to recognize that there is hidden message then our goal is defeated. Steganogrphy will not show up the presence of communication taking place in it. Johannes Trithemius was the first to use the term in his STEGANO-GRAPHIA a thesis on steganography and cryptography.

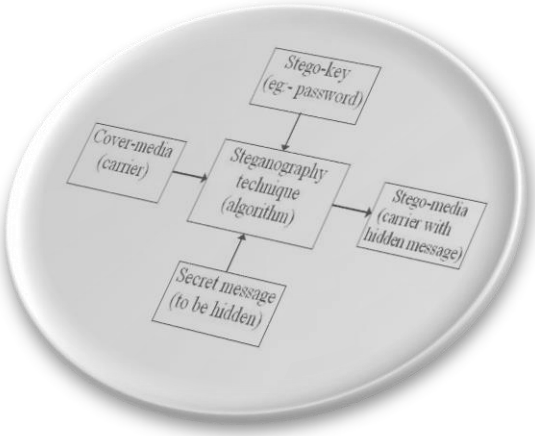
PAST:-Some of the examples of steganography used in past.

- Prisoners of Hanoi Hilton used the tap code for the communication between them. They created the code in matrix form.i.e 5x5.Each letter was assigned a tap sequence depended on the matrix.

	1	2	3	4	5
1	A . .	B . ..	C,K	D	E . .....
2	F .. .	G	H	I	J .. ..
3	L	M	N	O	P ... .
4	Q	R	S	T	U ....
5	V	W	X	Y	Z ....

- Ancient Romans used to write between lines using invisible ink based on various natural substances such as juices and milk. Their experience was not forgotten: even nowadays children play spies and write secret messages that appear only when heated.
- A message which is to be hidden was photographically reduced to the size of a period, and affixed as the dot for the letter 'i' or other punctuation on a paper containing a written message

A. Block Diagram of Steganography



B. TERMS

*1. Cover-Media(Carrier):*It is the carrier of hidden messages. A cover is generally selected as it will appear same as the ordinary and does not give doubt on it.

2. Stego-key:-It is key that embeds the data into a cover and also for extraction of data from the stego medium.

3. Secret Message:-The message that is to be hidden into the carrier.

4. Steganography technique:-The algorithm used to hide the messages.

5. Stego-media:-It consists of carrier with the hidden message in it.

B. Classificationof steganogrpahy:-

Steganogrpahy is mainly divided into 3

- *Pure steganography* where it does not contain any stego key. It assumes that no one is aware of this communication.
- *Secret Steganogrpahy*-Here the key (stego key) is exchanged previous to communication. This is most prone for the intruder to guess.
- *Public key* in which public key and a private key are used for the privacy and safe communication.

C. Types of steganography

1. Steganogrphy in Text :-Hiding of information into the text files.It has 3 types of coding (a)Line-shift coding(b)Word shift coding(c)Feature coding.

2. Steganogrphy in Image:- Image compression gives a solution to large sized image files. 2 types of image compression are lossless and lossy compression. Both have differing effects on any uncompressed secret data in the image. "Lossy" JPEG(Joint Photographic Experts Group) format files, offers high compression, but may not contain the original image's integrity.So it is called "lossy"."Lossless" compression maintains the original image data exactly, So it is more favored by steganographic techniques. Eg: (BMP),(GIF) Formats.

3. Steganography in Audio:-It s concept in which data files are hidden into the audio file. Different methods of audio steganography are a.)Phase coding,b.)Low-bit encoding c.)Echo Data hiding

4. Protocol or Network Steganogrphy:-Its cover object is the network protocols such as UDP,TCP,IP etc. for hiding the information.

D. Steganography Techniques:-

1.Spatial domain:-

Spatial domain technique is divided into

i. LSB:- This is the most commonly used method.Least significant bit(LSB) here replacing of the least significant bit of image pixels with the bit of confidential data.

ii. PVD:-Pixel value differentiating(PVD) in this the insertion of bits depends on whether the bit is edge or smooth area bit.Changes made to smooth areas is not noticeable by human visual system.

2.Masking and filtering:- This Techniques is done by marking on an image. Steganography is used to hide only the secret message whereas watermarks does on apportion of the carrier image. These techniques insert the message in the more considerable areas than hiding the message into the noise level. Watermarking techniques can be functioned without the image destruction due to compression done in lossy technique. This method is widely used in 24-bit & grey scale images.

3.Transform Domain Technique: In this technique; the message which is to be hidden is implanted in the transform or frequency domain of the cover. Its more complex way of hiding message into an image. There are different algorithms are used onto the image for hiding message in it. This technique are broadly classified into i)DFT ii) DWT iii)DCT iv)Embedding in coefficient bits v) DCT.

4. Spread Spectrum Technique: The concept used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The signal ratio to noise in each frequency band should be so minute that it become hard to spot the existence of data. Even though if piece of data are detached from a number of bands, there may be still sufficient information present in another bands to improve the data. Thus it is hard to eliminate the whole data without completely destroying the cover .It is a very strong technique mostly used in communication taken place in military.

*5.Distortion Techniques:*he message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

E. Factors affecting a steganography:-

1.Capacity:-This defines the amount of data that can be hidden into the cover medium by the algorithm.The rate is given in absolute measurement(the size of the hidden message) or in the data embedding rate(mostly in bits per non zero).

2.Robustness:- Robustness is the capability of embedded data to stay intacted if the stego- image undertake transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression.

3. Payload Capacity: It refers to the amount of hidden information that is to be hidden into the cover source. Watermarking usually insert only a little amount of information, whereas, steganography aims at secretcommunication taken place and therefore have enough embedding capacity.

4. MSE (Mean Square Error): It is defined as the average squared difference between a reference image and a distorted image. The smaller the MSE, the more efficient

the image steganography technique . MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

F. Applicatons:-

1.It is used to protect from data alteration.

2.Used for Confidential communication and secret data storing.

3.It is used for the access control system for the digital content distribution.

4.To maintain the media database systems.

5. E-Commerce

G. Algorithm:-

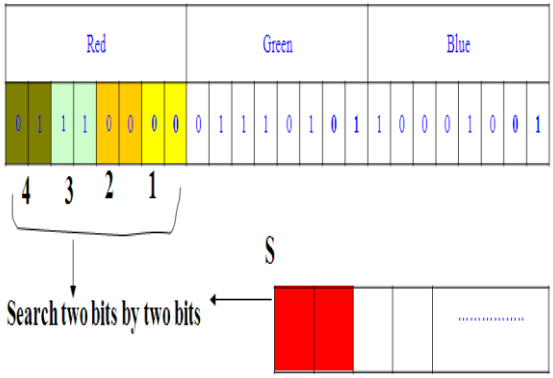
1. LSB

One of the most frequently used technique in steganography is least significant bit (LSB) insertion. It is also called LSB (Least Significant Bit) substitution and its process is of adjusting the LSB pixels of the carrier image. Its simple approach for implanting a message into the image. Here in this method, some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it take advantage of some limitations of the human visual system. The insertion of LSB varies according to number of bits in an image .In 8-bit image, the least significant bit i.e. the 8th bit of each byte of the image will be altered by the 1-bit of hidden message. And in 24 bit image, the colors of each component like RGB (red, green and blue) will be changed. Least significant bit steganography involves the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a series of binary number . In LSB substitution the least significant bits of the pixels are relocated by the bits of the secret message which gives rise to an image with a hidden message attached in it. The process of embedding is different according to the number of bits in an image (different in 8 bit and 24 bit images).

2.Proposed method

LSB hiding technique hide the secret message directly in the least two significant bits in the image pixels, hence that affect the image resolution, which reduce the image quality and make the image easy to attack. As well as this method is already has been attacked and broken. Therefore a new technique that able to make the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels.

New method in image steganography



Least Significant Bit Hiding Technique

Algorithm :-

The Proposed Hiding Algorithm.

*Inputs:*The message which to be hidden and the password for encryption and decrpytion,image.

Output: Stego image(carrier with the secret message)

Begin

First scan the image each row and then encode it into binary.

Encode the hidden message in binary.

Firlstly will verify the size of the image and the size of the secret message.

start sub-iteration 1:

Choose 1 pixel of the image randomly

Divide the image into three parts (Red, Green and Blue parts)

Hide 2 by 2 bits of the message in each part of the pixel by checking of about the identical.

If it is identical and is satisfied then set the image with the new values.

Otherwise hide in the two LSB and set the image with the new values

Save the position of the hiding bits in binary table.

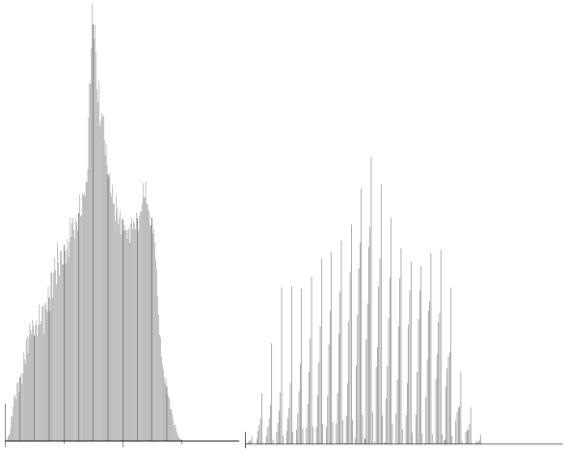
Endof sub-iteration 1.

Now setting the new values on to the image and save it.

End

a)Original image

b)3 bit are hidden



a)Histogram of original image. b)Histogram of 3 bits hidden image.

III. LITERATURE SURVEY

The paper named an overview of image steganography contains information on image steganography.The different kinds of steganography,different methods used for hiding the message.It discusses about the Spaitial domain,Transfer domain etc.image definition,image compression all these topic are discussed in brief.In transfer domain,what is jpeg and compression of jpeg is described.

The paper named Introduction to More Advanced Steganography contains overview of steganography with image examples.The paper describes deely in LSB technique and Bit Plane Complexity Segmentation.Using histogram it shows the viriation of original and stegoimage which is showed in the examples.

In the paper named A Practical Three Layered Approach of Data Hiding Using Audio Steganography ,there are various layers discussed to secure the messages.In the layers it uses different algorithms.the layers are i) First layer will convert the data using Hashing algorithm (ii) The output of the first step will be encrypted using cryptography technique (iii) The outcome of these two layers will be embedded to Sound files(iv)These three layers will work fine from the sender side and sound file will be transmitted over the network.

In the paper named Modern Steganography, what steganography is and what kind of applications can be implemented ,what is the embedding process ,what are the new scopes of steganography is discussed.

In the paper named A New Method in Image Steganography with Improved Image Quality, a new Steganography technique was presented, implemented and analyzed.This method hides the message which is depended on finding on the identical bits between the hidden messages and image pixels values.

IV.CONCLUSION

This paper was an introduction to the world. Steganography, in its large number of forms, has been in use factually for thousands of years. It have been mostly used efficiently in time of war. Based on the variety of forms implemented to hide the message will determine whether there is steganogrphy content or not. Thus for an agent to take decision on which steganographic algorithm to use, he would have to take decision on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.

REFERENCES

[1] Steganography Techniques –A Review Paper ,Jasleen Kour Deepankar Verma *M-tech Student,Computer Science Assistant Professor, Computer Science R.B.I.E.B.T, India R.B.I.E.B.T, India.*
[2] Social Steganography:Privacy in Networked Publics, danah boyd and Alice Marwick, Microsoft Research, Paper presented at ICA on May 28, 2011 in Boston.
[3] Evaluating Image Steganography Techniques: Future Research Challenges Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, Narayan C Debnath Department of Computer Applications, National Institute of Technology, Durgapur, India, Department of Computer Science, Winona State University, MN, USA.
[4] A New Method in Image Steganography with Improved Image Quality Atallah M. Al-Shatnawi,Department of Information Systems Al-albayt University , Mafraq, Jordan. Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915.
[5] Modern Steganography,Miroslav Dobscek Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Karlovo n´am_est´_ 13, 121 35 Prague 2, Czech Republic.
[6] A Practical Three Layered Approach of Data Hiding Using Audio Steganography,Nishu Gupta1, Mrs.Shailja2 Student (M.Tech), CSE, CDLU, Sirsa, India Assistant Professor, CSE, CDLU, Sirsa, India
[7] AN OVERVIEW OF IMAGE STEGANOGRAPHY T. Morkel , J.H.P. Eloff , M.S. Olivier Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa
[8] An Introduction to More Advanced Steganography.
[9] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing and Unseen", 0018-9162/98/$10.00 © 1998 IEEE.
[10] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi (2010)," Overview: Main Fundamentals for Steganography".