ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

IMAGE STEGNOGRAPHY CONCEPTS AND TECHNIQUES: - A SURVEY

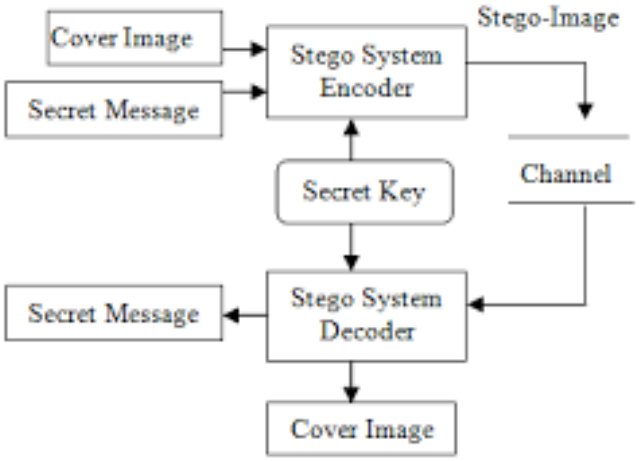
N.Thinaharan[1], B.Chitradevi[2], T.Suresh[3]
Research Scholar, Manonmaniam Sundaranar University, Tirunelveli [1]
Research Scholar, Periyar University, Salem [2]
Assistant Professor, Department of Computer Science, Bharathidasan University College, Kurumbalur[3]
citradevi.b@gmail.com

Abstract:- In recent arena of communications are done with the some secrete code words, it's are under some technologies, like the Steganography also of the communication techniques it uses the code words for communication purposes, it is also refer as the science of in visible communication. It is differ from the normal encryption and decryption techniques, the main aim is to secure the communication and prevent from an attacker or eaves-dropper, the Steganography Techniques challenge to cover the availability of the images itself from the observer. In some enterprises, organizations and government sectors are have the Copyrights of their sources of information like the text, image, voice or multimedia In the technology of Image Steganography, Secret Communication is accomplish to insert a text information ie message into the cover image after that generate a Stegoimage. Here we analyzed the various steganography techniques and covered the concepts of steganography and its major types, classifications and applications. Information hiding is based on digital watermarking. The DWM- is the short form of Digital Watermarking, it is a method of is the method of entrenching information into Digital Multimedia, it is a process to extract/detect for prevention and control. The information hiding and digital watermarking is the main goal of steganography is to be communicating in secure manner.

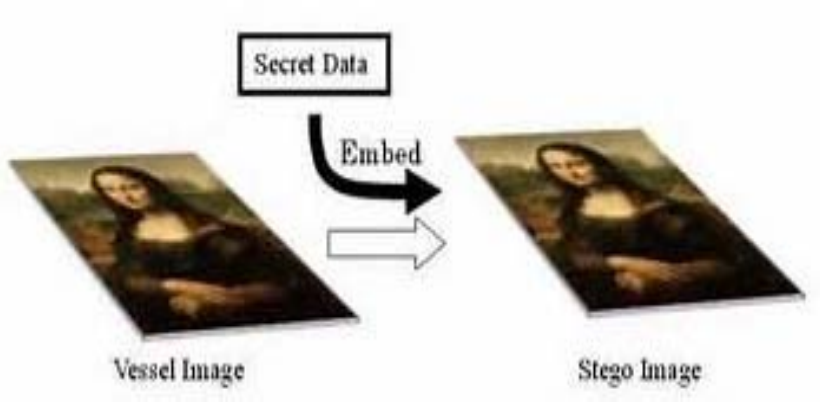
Key Words: Data hiding, Steganography, Cover Images, Steganalysis

I. INTRODUCTION

The method of steganography is the methods that have an attention recently. Goal of steganography is to hide information in the cover media so that other person will not perceive the occurrence of the information. This is the main difference between this process and the method of covert information. In Cryptography mechanism, the For example, in cryptography, the persons notice the info by seeing the coded info but they will not be able to realize the information.



In steganography, the survival of the information in the source will not be notice at all. Most of the steganography jobs have been carried out on images, video clips, texts, music and sounds. Using a combination of steganography, information security has improved significantly. And it is used for covert exchange of information. It is used in other establishment such as patent, averting e-document forge. The techniques to hide the multimedia data sounds, videos and images are called as data hiding techniques.



II. BASIC COMPONENTS

Steganography and cryptography are dissimilar and take apart from each other, still there are some similarities between them, and some researchers term steganography is a type of cryptography and as well as hidden communication is a type of Secret Writing. Steganography uses audio, text, images, and video media for hiding data.

The components of the Digital Steganography techniques are as follows;

a. The Embedding of data with secrete data.
b. The Secret Data can hold the Image also.
c. The outputs of above two steps are known as Stego files.

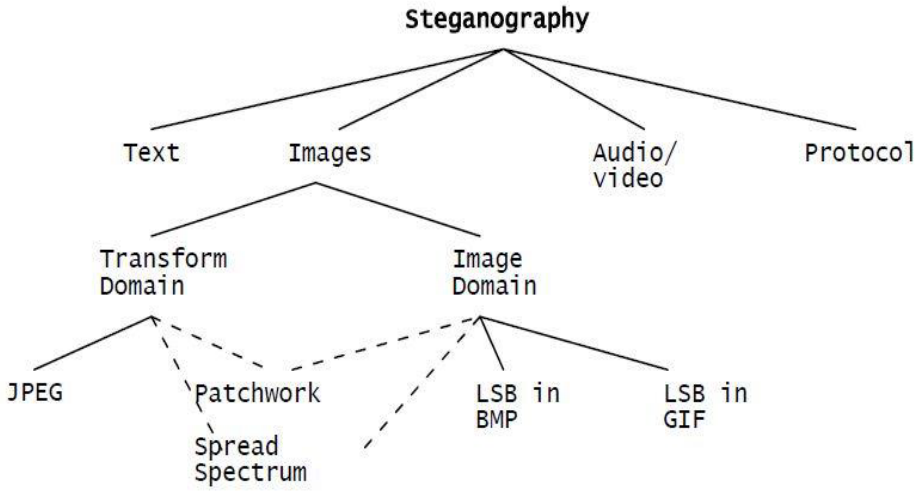
In the environment of steganography, Image steganography is broadly used the technique that compared to others because of its simplicity and a stress-free way to secrete the data in images. The main purpose is the amount of data is more than the sufficient existing in the images and can be altered easily to hide secret messages in them, and because it has a controlled power of the Human Visual System (HVS). In image steganography, the cover image is recognized as the unique image. The stego image is called the consequential which comes after embedding the secret bits into cover image that has no aptitude, and then the sender can transfers the stego image to the other side throughout a unrestricted channel.

III. REQUIREMENTS OF HIDING INFORMATION DIGITALLY

The number of rules are imposed the to enable the hidden image. The proprieties and techniques must satisfy a number of desires so that steganography can be functional correctly.

The consequent agenda of main desires that steganography techniques must satisfy:

- When the Integrity Emendations of the hidden information, the Stego object will be corrected.
- Stego object must remain affected.
- The updation of image steganography not affects the watermark.
- As a final point, it assumes that the aggressor knows that there is hidden info inside the stego object.



IV. ASSESSMENT OF DIFFERENT TECHNIQUES

The discussed above concepts are represents the strong and weak points of the image steganography, if we took the strong points our research. These are all important to make the suitable algorithms for image steganography analysis. The image steganography algorithms have to act in agreement with a few basic desires. The most important prerequisite is that a steganographic procedure has to be scarcely noticeable.

These requirements are as follows:

- **Invisibility** – The invisibility of a steganographic algorithm is the initial and primary requirement, since the force of steganography lies in its capacity to be ignored by the human eye.
- **Payload Capacity: -** It needs to embed only a tiny amount of patent information, steganography aims at concealed communication and therefore requires sufficient embedding capacity.
- **Robustness Against Statistical Attacks:-** The statistical Steganalysis is the observation and detection of the hidden information with the help of Statistical test on image data's.
- **Robustness Against Image Manipulation:-** A Stego Image communicated with the trusted systems the image may go through modifications by a dynamic supervisor in a challenge to take out hidden information.
- **Independent of file format:-** With many different image file formats used on the Internet, it might seem disbelieving that only one type of file format is continually communicated with the two parties.
- **Unsuspicious files:-** Requirements includes all characteristics of a Stenographic algorithm that may result in images that are not used normally and may cause notion. The table represents comparison of the Least Significant Bit.

The following table compares least significant bit (LSB) with BMP and GIF files, JPEG Compression Steganography, The Patchwork Approach and Spread Spectrums Techniques;

Table.1: Comparison of image steganography algorithms

	LSB in BMP	LSB in GIF	JPEG compression	Patchwork	Spread spectrum
Invisibility	High*	Medium*	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious files	Low	Low	High	High	High

* - Depends on cover image used

V. CONCLUSION

The demanding and significant task is data hiding in the field of information security. This article focused the and discussed about the digital images and the concept overview of Steganography Techniques. Numbers of ways are used to decrease the bits needed to Encoded a Hidden data. Robustness is a real constraint for a steganography and many steganography systems that are considered to be forceful towards a specific class of mapping. It is also logical to generate an untraceable steganography algorithm which is capable of resist image process manipulations which may occur by accident and not passing through an attack. This paper gives a few clues and recommendation for designing the steganographic system. Steganography techniques generally include great endeavor for achieving a high embedding rate. It is a noble supernumerary channel for images and video collection files that are large volume and good inaudibility.

REFERENCES

[1] Moreland T, Steganography and Steganalysis, Leiden Institute of Advanced Computing Sciences, 2003.
[2] M.H. Marghny, F.Al-Afari and M.A.Bamatra, Data Hiding by LSB Substitution Using Genetic Optimal Key – Permutation, International Arab Journal of e-Technology, Vol. 2, No.1, 2011.
[3] M. Al-Husainy, A New Image Steganography Based one Decimal Representation, Computer and Information Sciences, Vol. 4, No. 6, pp. 38-47, 2011.
[4] N.Johnson and S.Jajodia, Exploring Steganography: Seeing the Unseen, IEEE Computer, pp. 26-34, February 1998.
[5] M. Wu, E. Tang and B.Lin, Data hiding in Digital Binary Image, Proc. of 2000, IEEE International Conference on Multimedia and Expo. Vol. 1, pp. 393-396, 2000.
[6] R.J.Anderson and Fabien A.P.Petitcolas, On the limits of Steganography, IEEE Journal on Selected Areas in Communications, Vol. 16, no. 4. Pp. 474-481, 1998.
[7] Artz, D., Digital Steganography: Hiding Data with Data, IEEE Internet Computing Journal, June 2001.
[8] Bender, W., Grubl D, Morimoto N and Lu A, Techniques for Data Hiding, IBM Systems Journal, Vol. 35,1996.