COMPARISON OF VARIOUS STEGANOGRAPHY TECHNIQUES USING LSB AND 2LSB: A REVIEW

Aishwarya Pandey
Shri Shankaracharya Technical Campus
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
aishwaryapandey.smvit@gmail.com

Prof. Jharna Chopra
Shri Shankaracharya Technical Campus
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
Jharna.chopra@gmail.com

Abstract

With rapid growth in the digital market, Steganography is going to increase its importance by which the exponential development and secret communication of potential computer users are also increased over the internet. It can also be well defined as the study of secret invisible communication that generally deals with the different ways of concealing the existence of the communicated message. Usually, the data embedding is obtained in communication such as image, text, voice or multimedia content for copyright and also in military communication for authentication and many other different purposes. In image Steganography, the secret hidden communication is obtained through embed a message into a cover image which is used as the medium to embed message into the image and generate a stego image which is a generated image which is carrying a secret hidden message. In this paper we have analyzed various steganography techniques and also have covered steganography overview and its major types.

Keywords— *Data hiding, Steganography, Cover image, cover writing.*

I. INTRODUCTION

Steganography word is originally from two Greek words Steganos which means Covered and Graptos means writing and which literally means "cover writing". Usually steganography is also known as "invisible" communication. Steganography means to hide messages existence in a particular medium such as audio, video, image, text communication. In recent steganography systems uses multimedia objects like image, audio, video, etc., as their cover media because people often send digital images over email or may share them through other internet communication application. It is very different from protecting the actual content of a hidden message. Steganography simply means that is not to be alter the any structure of the secret message, but hides it inside a cover-object which is used as medium for transmitting message. After hiding the message, the process cover object and stego-object which helps to carrying hidden information object. So, steganography is used to hiding information and cryptography is used to protecting information are totally different from each another. Due to which the invisibility or hidden factor is so difficult to recover information without any known procedure in steganography. For Detecting information procedure of steganography is known as Steganalysis.

II. STEGANOGRAPHY IN DIGITAL MEDIUMS

There are many suitable steganography techniques which are depending on the type of the cover object which are illustrate below in order to obtain security. It can be shown in Figure 1.

- Image Steganography: by taking the cover object as image in steganography is known as image steganography. Usually, in this technique, the intensity of pixels are used to conceal the information.
- Network Steganography: in this, while taking cover object as network protocol, such as UDP, ICMP TCP, IP etc., where protocol is used as medium, is known as network protocol steganography. In OSI network layer model, there exist cover medium where steganography can be obtained in unused header bits of TCP/IP fields.
- Video Steganography: Video Steganography is a technique to hide any type of information files or information into digital video format. Video which is a combination of pictures is used as medium for hidden information. Usually discrete cosine transform (DCT) alter values which is used to hide the information in each of the images consisting in the video, which is not visible by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

- Audio Steganography: When taking audio as a medium for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as AVI MPEG, WAVE, MIDI or etc for steganography.
- Text Steganography: The general technique used in text steganography, such as number of white spaces, capital letters, tabs, just like Morse code and etc is used to obtain information hiding.

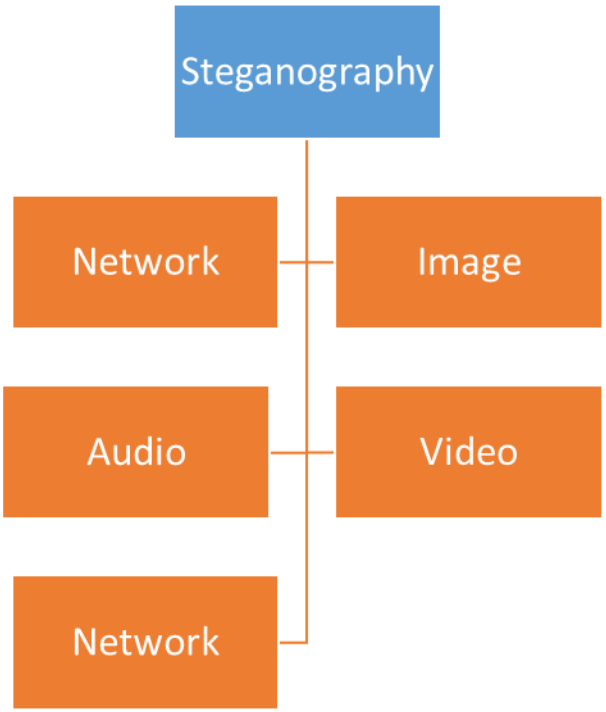

Fig.1. Digital Medium to Achieve Steganography

III. LITERATURE SURVEY

Xinyi Zhou [1], focused on the image hiding method in this paper combine the cryptography and information hiding. On the one hand, by using information hiding does not change the visual characteristic of cover image, we can embed secret information in another public image and transfer. On the other hand, by using digital signature and encryption technology of cryptography , we can make the unauthorized users can not know the location of the embedded secret information, so that the secret information cannot be extracted. The effective combination of the above two means further improves the security of information hiding.

Champakamala .B.S [2], focused on the enhanced LSB technique described in this project helps to successfully hide the secret data into the cover object without any distortion. Matlab function is an easy to use, user interface function that guides a user through the process of either encoding & decoding a message into or from the image respectively. Since LSB doesn't contain any information there is no loss of information and secret image recovering back become undistorted.

Shamim Ahmed Laskar [3], focused on the proposed method has been employed for applications that require high-volume embedding with robustness against certain statistical attacks. The present method is an attempt to identify the requirements of a good data hiding algorithm. And it is not intended to replace steganography or cryptography but rather to supplement it. Steganography is the data hiding technique which comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography is not a good solution to secrecy, but neither is encryption. But if these methods are combined, we will have two layers of protection. If a message is encrypted and hidden with a LSB steganographic method the embedding capacity increases and thus we can hide large volume of data.

V. Lokeswara Reddy [4], focused on BMP uses lossless compression, LSB makes use of BMP image. To be able to hide a secret message inside a BMP file, one would require a very large cover image. BMP images of 800×600 pixels found to have less web applications. Moreover such uses are not accepted as valid. For this reason, LSB Steganography has also been developed for use with other image file formats.

Mr . Vikas Tyagi [5], has proposed a paper which is a short introduction to the world of steganography. We have shown how the simplest methods work and how they can be explored. We have used symmetric encryption algo to provide more security. Research in this field has already begun. Next to steganography, one of the most active fields of research is mass detection tools for hidden contents.

***TABLE I**. Shows comparison between various existing approaches and its limitation*

Ref. No.	Method Used	Data Source	Approach	Strength	Limitation
1	Improved LSB algorithm	RGB Image	Author propose an improved LSB information hiding algorithm of color image using secret key is be proposed, combining information hiding and cryptography, increasing the human eye visual features, and the identity authentication based on digital signature	method demonstrates better security and higher PSNR	-Less security of data hiding -Required Improvement in Technique
2	LSB algorithm	Image	A new technique of LSB steganography has been proposed which is an improvised version of one bit LSB technique.	there is no loss of information	- does not support for different image format
3	High Capacity LSB algorithm and encryption algorithm	Image	Author propose a high capacity data embedding approach by the combination of Steganography and cryptography. In the process a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using LSB insertion method	Demonstrate the effectiveness of the proposed method by computing Mean square error (MSE)	-Need to maintain the level of resistance to visual and statistical attacks.
4	2LSB algorithm	Image different format tiff, jpeg, png etc.	Proposed paper explains the LSB Embedding technique and Presents the evaluation for various file formats.	It emphasizes for various file formats.	-does not effectively hide secret data over different format e.g. png or jpeg
5	Secure 2LSB Algorithm and encryption	Greyscale and RGB	paper discussed a technique based on the LSB(least significant bit) and a new encryption algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it.	It provide security to the data	PSNR of resultant embedded image is low

IV. CONCLUSION

With rapid growth in the digital market, Steganography is going to increase its importance by which the exponential development and secret communication of potential computer users are also increased over the internet. It can also be well defined as the study of secret invisible communication that generally deals with the different ways of concealing the existence of the communicated message. This paper gives an overview of various steganography techniques, its major types and classification of steganography which have been proposed in the literature during last few years.

REFERENCES

[1] Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, "An Improved Method for LSB Based Color Image steganography Combined with Cryptography", 2016 IEEE ICIS 2016, June 26-29, 2016, Okayama, Japan.

[2] Champakamala .B.S, Padmini.K, Radhika .D. K, "Least Significant Bit algorithm for image steganography", INTERNATIONAL JOURNAL OF ADVANCE COMPUTER TECHNOLOGY | VOLUME 3, NUMBER 4.

[3] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012

[4] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011).

[5] Mr . Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, "IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY", Journal of Global Research in Computer Science, 3 (3), March 2012, 53-55.