www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-7, Issue-1 March 2019
Review Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Data Security by Steganography: A Review

S. Bansal

Department of Computer Science & Application, Prestige Institute of Management, Gwalior, India

e-mail: satish_bansal@rediffmail.com

Received: 30/Jan/2019, Accepted: 26/Feb/2019, Published: 10/Mar/2019

Abstract- There is huge amount of data can be transmitted or store on internet in today life. This is not simple data, which is use or share by public or group of society, while personal, financial or secret data storing or transmitting for any personal or financial transaction. This is secret data, which we want to hide. Steganography is very latest or important field like cryptography. Cryptography use for privacy while Steganography use for secrecy. Steganography is a process of hiding the message in any kind of transfer file like image, audio, video. E-commerce is an application of internet, which is using rapidly day by day. The main concern of e-commerce to provide security in such way user can use without afraid. Steganography can be play very important role to provide security in e-commerce transaction. These data transactions include sensitive document transfer, digital signature authentication and digital data storage. This research paper show use of digital or image Steganography for information security through the Internet.

Keywords- Security, Steganography, Image Steganography

I. INTRODUCTION

The word Steganography is deriving from Greek origin and means, "covered or hidden writing". It is the art or science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third person or other party, the goal of Steganography is to hide or cover the data from a third party. In Steganography, information can be hidden in carriers such as images, audio files, text files, and video and data transmissions [1].

Now a day's one of major problem for internet user lack of security with on line transaction. Since some existing technique like cryptography and contemporary machine are able to brake them, but whole process is not confidential at all. Steganography is a branch of information hiding. It allows the people to communicate secretly.

Steganography is study of hiding secret message in some other media. The information to be hide is called the hidden message and the medium in which the information to be hidden is called the cover image. The cover document containing hidden message is called stego-image. This process is called steganography and reverse process is called steganalysis. Figure 1 depict hiding the data or message in the cover medium at the sender or source end and extracting the hidden data from the stego-document at the receiver end is called stego-system.

There are four ways to implement steganography:
1. Using text.
2. Using images.
3. Using audio files.
4. Using video files.

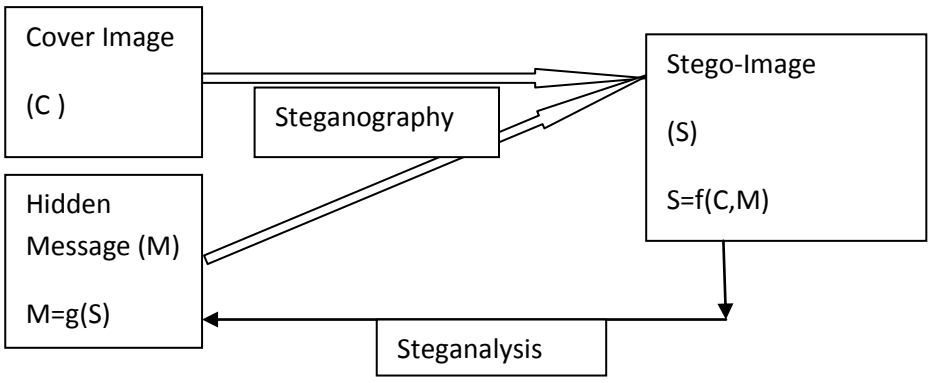

Figure 1 : Creating an Image with encoded message and converting back

II. LITERATURE REVIEW

Steganography is the discipline that involves communicating or transferring secret data in an appropriate multimedia carrier, e.g., image, audio, animation and video files.

It is the time for focus some technique, which used in protect the information over the network or internet. There has been some work already done and find some gap to improve in existing technique.

One article [2] proposed a novel technique for image Steganography based on Huffman Encoding. Two 8-bit gray level image of size M X N and P X Q are use as cover image and secret image respectively. This technique can be improving by converting 8-bit gray level image into color image.

One more article [3] proposed technique in a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improving by using bit-inversion technique.

Some researcher mainly focuses on image for data security. They [4] gone through the LSB insertion & RSA encryption technique using the robust image Steganography technique.

III. OBJECTIVES

Steganography has a broad diversity of uses, especially in the network or Internet, where there is so much sensitive data. Steganography starting with watermarking files that are copyrighted, when perform transaction or communication over the internet, which show the user authentication, through transport of personal information can be easy and there are many more operation can also be perform.

There are following objectives for using this approach:

- Security measures that can reduce or eliminate intellectual property theft.
- Available protection mechanisms to secure information sent between a client and a server.
- To secure the confidential data on e-commerce web site.
- Message integrity, security, preventing from altering information as it travels across the Internet.
- Safeguards those are available so commerce servers can authenticate users.
- Hiding information also gives a new effective method of protecting of copyright and licenses.

IV. IMPLEMENTATION OF STEGANOGRAPHY

Image Steganography: Image Steganography is an important category of Steganography, which most widely used. A Steganography technique that uses images or graphics as the cover media is call an image Steganography. The process of hiding secret messages in digital images is the most widely used technique as it can take advantage of the limited power of the human visual system (HVS) and also because images have a large amount of superfluous information that can be used to hide a secret message.

Secrets message is hide inside all sorts of cover information. The following formula provides a very generic description of the Steganography process:

cover_medium + hidden_data + stego_key = stego_medium

Where cover_medium is the file, in which we will hide the hidden_data, which may also be encrypt using the stego_key. The resultant file is the stego_medium (which will of course be the same type of file as the cover_medium).

Cover-Image: In which the secret information is going to hidden.

Stego-Image: the medium in which the information or message is hide. The "stego" data is the data containing both the cover image and the fixed information. Embedding is the process of hiding the secret information in the cover image.

Secret Key: this is the key used as a password to encrypt and decrypt the cover and stego respectively in order to extract the hidden message. Secret key is optional.

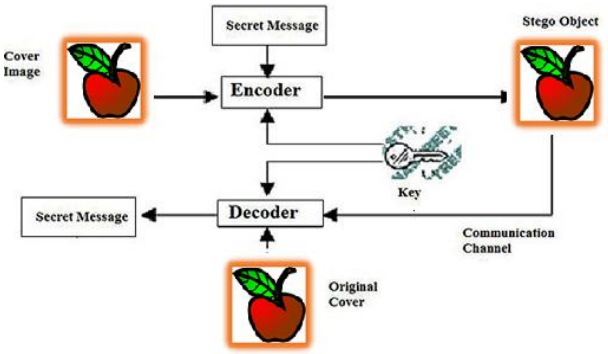

Figure 2: Implement Of Steganography

V. APPLICATION AND FUTURE SCOPE

There are many systems used for hiding facts by secret messages within image. Steganography is useful to any number of processes that will hide a message within an object particularly an image, where the hidden message will not be apparent to an observer.

Steganography hide the message not crypt the message but more security purpose it can be combine. This is one important area of image processing application where we can protect the image. The one having the true key can detect the data hidden in the image-by-image Steganography.

Today it is the time when we use internet so much for financial transaction or E-transaction, we want to secure in such a way that unauthorized person cannot access it. In today life, Hacker or unauthorized person try to access the data in data communication system, then steganalysis discover the message from Steganography.

VI. CONCLUSION

Steganography has a significant application in e-commerce. It allows the security of data, which may be generally available over the internet. Using Steganography, one can secure data without affecting thought that something important is in the file while in contrast to cryptography, where if something is encrypted, it must be important. Steganography or Hiding information also gives a new effective method of protecting and enforcement of copyrights and licenses. Steganography through Secret information can used to confirm important business transactions and user authentication.

REFERENCES

[1] R. Doshi, P. Jain, L. Gupta, "Steganography and its application in security, "International Journal of Modern Engineering Research(IJMER), vol. 2, no. 6, pp. 4634-4638, 2012.
[2] G. Prabakaran, R. Bhavani, P.S. Rajeswari, "Multi secure and robustness for medical image based steganography scheme, "Circuits, Power and Computing Technologies(ICCPCT), 2013 International Conference, pp. 1188-1193, 20-21 March 2013.
[3] N. Akhtar, P. Johri, S. Khan, "Enhancing the security and quality of LSB based image Steganography, "Computational Intelligence and Communication Networks(CICN), 2013 5th International Conference, pp. 385-390, 27-29 Sept. 2013.
[4] M. Junej, P. S. Sandhu, "Designing of Robust Image Steganography Technique based on LSB Insertion and Encryption", ICARTCC, 2009.

Author Profile

Mr. Satish Bansal completed his Bachelor of Science from Autonomous Science College, Gwalior(M.P.) and He obtained Master of Computer Application degree from Madhav Institute of Technology & Science (MITS), Gwalior in July 2000. He completed Master of Engineering from RGPV. He is currently pursuing P.HD. in Computer Science from Jiwaji University, Gwalior. He also cleared GATE and UGC NET Exam. He has a total of Sixteen years' experience out of which two years have been in Software development and Fourteen years have been in academics. He has Eighteen publications in his credit out of which Seven are international.

