iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VIII **Month of publication:** August 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue VIII, August 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Various Steganographic Approaches: A Review

Shefali Narang[1], Ashish Shrivastava[2]
[1]M.Tech Scholar, [2] Assistant Prof.
CSE Department. PIET, Samalkha (Hr.)

Abstract-Steganography is basically the procedure of hiding top secret information within any medium. Today there is huge internet growth i.e. Demand of internet is increasing day by day and it becomes the mainly vital factor of information technology. But due to this the threat of information security increases. Now it is significant to protect the data so that no unofficial person can interfere with the secret message or information. The steganography is a security tool using that we can use to conceal a important secret message. In our paper we have been provided a review on various approaches of steganography.
Keywords: Steganography; Stego-Images; Audio Steganography; Video Steganography; Image Steganography etc.

I. INTRODUCTION

Nowadays increase in the demand of the internet becomes the most imperative factor of information technology & communication department but due to this the risk of information security increases. So it required that no unofficial person can use it. The steganography is a powerful safety tool. We can conceal a secret message in any media using this tool [4]. Steganography is basically the Greek word which has the meaning the covered or enclosed writing. As in the coming year's need of data hiding, official document protection, and privacy increases, steganography is to be used because of its some exclusive features [1]. It is basically the key area of research in current years involving a large number of applications. It is the process of embedding information into the cover image without causing statistically major alteration to the cover image. The modern image steganography represents a challenging task to transfer the embedded information to the receiver without being detected [5].

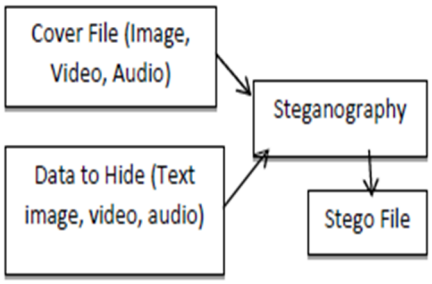


Figure 1: The method of hiding data [5]

A. Image Steganography Terminologies [6]

Basic image steganography terminologies are as follows:-

1) *Cover-Image*: Original image which is to be used as a carrier for secreted information.
2) *Message:* Real information which is to be used to hide into images is called a message. It can be a plain text or images.
3) *Stego-Image*: Embed message into the cover image is called as stego-image.
4) *Stego-Key:* It is used for embedding or extracting messages from the respective cover-images and the stego-images.

II. STEGANOGRAPHY OVERVIEW

Steganography word came from the Greek words Steganós means Covered and Graptos means Writing. The origin of steganography is the biological and physiological. The term "steganography" came into use in 1500's after the emergence of Trithemius' book on the subject "Steganographia". The overview of steganography field can be divided into three parts [7].

\

A. Past

It's very older origins can be traced back to 440 BC. In early times, messages were hidden on back of the wax writing tables, written on the stomachs of the rabbits, or the tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists [7]. Cryptography became very common place in the middle periods

B. Present

The majority of today's steganographic systems uses the multimedia objects like image; audio; video etc as cover media because people often broadcast digital pictures over email and other Internet communication [7]. So, in present world of steganography various steganographic techniques have been proposed. There are certain cases in which a combination of Cryptography and Steganography is used to achieve data privacy over secrecy [7].

C. Future

Nowadays, "Hacking" is very famous term. It is nothing but an unauthorized access of data which can be collected at the time of the data transmission. With respect to the steganography this problem is called as Steganalysis [7]. Steganalysis is a process in which a steganalyzers cracks the cover object to get the hidden data. It is hoped that Steganography along with Cryptography may improve the privacy as well as secrecy.

III. MODERN APPROACHES OF STEGANOGRAPHY

Common modern approaches of steganography are following [3]
Plaintext Steganography
Still imagery Steganography
Audio and Video Steganography
IP datagram Steganography

A. Plaintext Steganography

In this technique the message is hidden within a plain text file using various different types of schemes such as the use of selected characters, extra white spaces of the cover text etc.

B. Still Imagery Steganography

Nowadays the most extensively used technique is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot see the variation in luminance of color vectors at higher frequency side of the visual spectrum. A picture can be represented by a collection of color pixels. Each individual pixels can be represented by their optical characteristics such as 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s.

C. Audio And Video Steganography [3]

In this type, secret message is embedded into digitized audio signal which results in slight altering of binary sequence of the corresponding audio file.

D. IP Datagram Steganography [3]

This is another approach of steganography, which uses hiding data in the network datagram level in a TCP/IP based network like Internet. Network Covert Channel is the synonym of network steganography. Overall goal of this approach o make the stego datagram is undetectable by Network watchers like sniffer, Intrusion Detection System (IDS) etc. In this information to be hide is placed in the IP header of a TCP/IP datagram. Some of the fields of IP header and TCP header in an IPv4 network are chosen for data hiding.

IV. FACTORS AFFECTING A STEGANOGRAPHIC METHOD

The effectiveness of steganographic method may be calculated by comparing the concealed image with the cover Image. There are the factors that determine the efficiency of a technique. These factors are following:

A. Robustness

It refers to the ability of embedded data to remain undamaged if the stego- image undergoes through various transformations, such as linear and non-linear filtering and compression.

B. Imperceptibility

It means invisibility of a steganographic algorithm. It is the basic requirement, because the strong point of steganography lies in its capability to be unnoticed by the human eye [2].

C. Payload Capacity

It is defined as the amount of secret information which is hidden in the cover image.

D. PSNR (Peak Signal to Noise Ratio)

It may be defined as the ratio between the maximum power of a signal and the power of humiliating noise that affects the faithfulness of its representation. The higher value of PSNR represents the better will be quality of the image.

E. Mean Square Error (MSE)

It is defined as the average squared difference between a reference image and a distorted image. The lesser the MSE, the more efficient will be 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. SNR (Signal To Noise Ratio)

It is defined as the ratio between the signal power and the noise power. It compares the level of the desired signal to the level of background noise [2].

G. Various Steganography Attacks

There are several types of attacks based on the information available for study. Some of them are as following: -

1) Known Carrier Attack: The original cover media and stego media both are available for analyzing.

2) Steganography Only Attack: In this type of attacks, only stego media is available for analyzing.

3) Known Message Attack: The hidden message is known in this type of attack.

4) Known Steganography Attack: The cover media, stego media as well as the steganography tool or algorithm, are known.

V. STEGANOGRAPHY APPLICATIONS

Steganography can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. In the business world steganography can be used to hide a secret chemical equations or plans for a new development. It can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Steganography can also be used in the noncommercial sector to hide information that someone wants to keep private. Spies have used it since the time of the Greeks to pass messages undetected. Terrorists can also use steganography to keep their communications secret and to coordinate attacks [7].

A. Copyright Protection

A secret copyright notice can be embedded inside an image to identify it as intellectual property [8]. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to recognize potential pirates. A watermark can also serve to detect whether the image has been subsequently modified [4].

B. Feature Tagging

Captions, interpretation, time stamps, and other descriptive elements can be added within an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will only be able to extract and view the features.

C. Secret Communications

In various situations, transmitting a secret message draws unwanted attention. The use of cryptographic technology may be forbidden by law [8]. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers or eavesdroppers.

D. Digital Watermark

It is used to recognize ownership of the copyright of such signal. A digital watermark is a type of marker covertly embedded in a noise-tolerant signal such as audio or image data.

E. Used By Terrorists

Steganography on a large scale is used by terrorists, who hide their secret messages in innocent, cover sources to increase terrorism across the country [4].

F. Printers

It is also used in the printers. In printers, very small yellow dots are inserted into all pages. Information is hidden inside these yellow dots like serial number of the page or message, date and time stamp. This property is available in laser [8].

Other applications include the following:-

TV broadcasting,

Video-audio synchronization,

Protection of data alteration,

Companies' safe circulation of secret data, Access control system for digital content distribution,

TCP/IP packets

VI. CONCLUSION & FUTURE SCOPE

In the past decade, the steganography is attracted topic for image security. It plays an essential role for proficient covert communication. It is the ability and discipline of writing hidden secure messages such that that no one, apart from the sender and projected recipient, suspects the existence of the message. It is thus plays a role as book on magic. Its scope is growing day by day because it does not attract anybody by itself. Steganography usually deals with the methods of hiding the existence of the communicated data in such a way that it remains private.

REFERENCES

[1] Rakhi and Suresh Gawande A Review on Steganography Methods. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 10, October 2013.pp 4635-4638.

[2] Jasleen Kour and Deepankar Verma Steganography Techniques –A Review Paper International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5)May 2014. Pp.132-135.

[3] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal "Steganography and Steganalysis: Different Approaches" arXiv preprint arXiv:1111.3758. 2011/11/16.

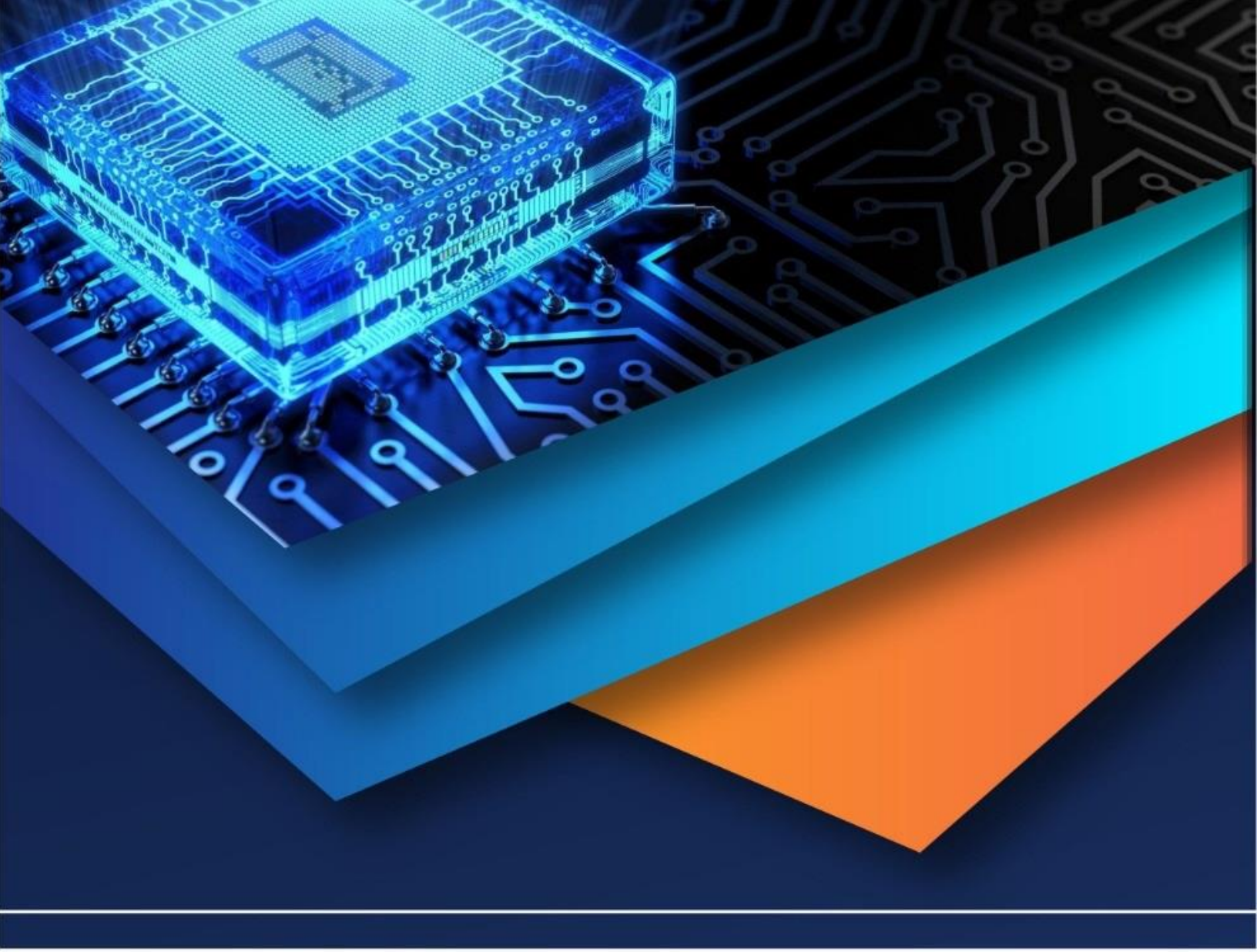
[4] Rashi Singh and Gaurav Chawla A Review on Image Steganography. International Journal of Advanced Research in Computer Science and Software Engineering.Volume 4, Issue 5, May 2014 ISSN: 2277 128X.pp 686-689.

[5] Stuti Goel, Arun Rana & Manpreet Kaur. A Review of Comparison Techniques of Image Steganography. Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0 Year 2013.

[6] Mehdi Hussain and Mureed Hussain " A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology Vol. 54, May, 2013. Pp. 112-125.

[7] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das "A Tutorial Review on Steganography" International conference on contemporary computing, volume 101, 2008/8/7.

[8] R.Poornima and R.J.Iswarya AN Overview Of Digital Image Steganography International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.pp 23-31.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY