IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Survey on Various Steganography Techniques

Priyanka Sharma[1], Astha Gautam[2], Ruchi Singh[3]

M.Tech. Student, Computer Science & Engineering, L.R.I.E.T, Solan (H.P), India[1]

Assistant Professor, Computer Science & Engineering, L.R.I.E.T, Solan (H.P), India[2,3]

Abstract: Steganography is progressive to gain its importance due to the aggressive growth and secret communication of potential computer users over the internet. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Normally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other objectives.

Keywords: Data hiding, Steganography, Cover writing.

I. INTRODUCTION

Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means "cover writing". Generally steganography is known as "invisible" communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today's steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information.

Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis.

II. STEGANOGRAPHY IN DIGITAL MEDIUMS

Depending on the type of the cover object there are many useful steganographic techniques which are followed in order to obtain security. It can be shown in Figure 1.

A. Image Steganography
Taking the cover object as image in steganography is known as image steganography. Mostly, in this technique pixel intensities are used to hide the information.

B. Network Steganography
When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields.

C. Video Steganography
Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

D. Audio Steganography
When taking audio as a carrier 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 WAVE, MIDI, AVI MPEG or etc for steganography.

E. Text Steganography
General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code and etc is used to achieve information hiding.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

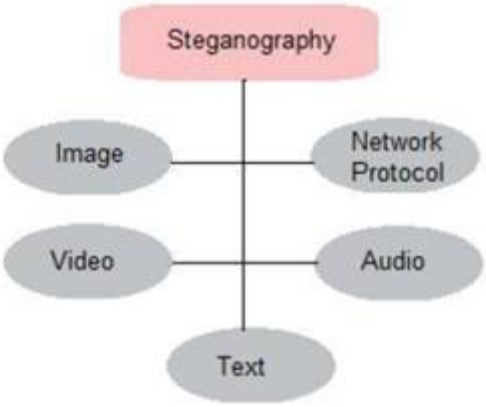

Fig. 1 Digital Medium to Achieve Steganography

III.NEED OF STEGANOGRAPHY

Currently, the use of internet increasing quickly. One of the most important areas which attracted by people is security is related to internet and also related to communication. At present, security for hiding data is most popular technique which receives more attention than cryptography. Various methods such as cryptography, coding Steganography, etc. are used for hidden communication. The major benefit of Steganography over other coding techniques is that it hiding the data inside other data in such a way that no other person recipient, even know the existence of it.

A. Terms used in Steganography are:
1) Cover Image
The medium in which information is to be hidden. It may be an audio, video, image or a text file.

2) Key
It's a secret value which help in encoding or extraction of data, without which data cannot be encode and extract.

3) Stego-image
A medium within which information is hidden.

B. Message
The data to be hidden or to be extracted.

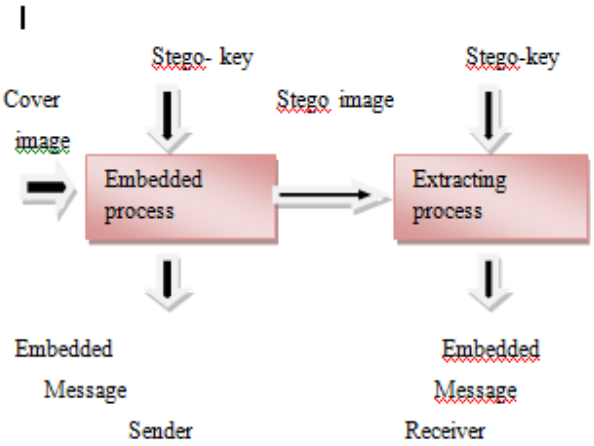

Fig. 2 General Block Diagram of Steganography

For Steganography, the size of cover image can be of any size -8 bit, 24 bit, 32 bit, 36 bit. The image can be in any format either jpeg, gif, bmp, etc. we have a key which is used to select the random pixels in which data is to hide. Therefore Stego image is generated which is send to another person. Now on the receiver side the Stego image is processed and extraction of message can be done with the help of secret key. The key is the one by which receiver knows the position of the pixel on which message is rooted.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

IV. STEGANOGRAPHY TECHNIQUES

There are some approaches in classifying the Steganography techniques are given below:

A. Substitution Technique

These techniques try to encode secret data by substituting insignificant parts of the cover image by secret data bits. It consists of many techniques such as least significant bit substitution, pseudorandom permutation etc.

B. Transform Domain Technique

These techniques conceal message in a significant area of the cover image which makes them stronger to attack. It consists of DCT, DWT methods**.**

C. Spread Spectrum Technique

In this technique, it tries to extend a secret message over a cover, in order to make it impossible to recognize. By this technique, it is hard to remove the embedded message. It includes two types of methods: -one is direct sequence method and second is frequency hopping.

D. Distortion Technique

This technique requires the knowledge of original cover in the decoding process. Most text based hiding methods are of distortion type.

V. FACTORS AFFECTING ON STEGANOGRAPHY

Some factors that determine how efficient and powerful a technique is are as follows:

A. Robustness

Robustness refers to the ability of embedded data to remain unbroken if the stego image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations.

B. Imperceptibility

The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

C. Payload Capacity

It refers to the amount of secret information that can be hidden in the cover source. Watermarking needs to embed only a small amount of copyright information, on the other side, Steganography aims at hidden communication and therefore requires sufficient embedding capacity.

D. PSNR (Peak Signal to Noise Ratio**)**

It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the reliability of its representation. This ratio is mainly used as a quality measurement between the original and compressed image. The higher the PSNR, the better the quality of the compressed image

E. MSE (Mean Square Error)

Mean Squared Error is the average squared difference between a reference image and a distorted image. An Image Steganography technique is able if it gives low MSE.

F. SNR (SIGNAL TO NOISE RATIO)

It compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power.

VI. RELATED WORK

In [1] Stuti Goel et al. presented comparison between three techniques that are LSB, DCT, and DWT. They evaluated the performance on the basis of MSE, PSNR, Normalized Coefficient, Processing time, capacity and robustness.

In [2] Himanshu Gupta et al. This paper presented the use of LSB algorithm for image domain. They have shown that as the number of bit substitution increases, PSNR increases and MSE decreases.

In [3] Vikas Tyagi et al. proposed the LSB and a new encryption algorithm. They have shown that by matching the data to an image, there is less chance to attacker being able to use Steganalysis to recover data. Before hiding the data in an image the application first encrypts it.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

In [4] Vijay Kumar Sharma et al. presented a new steganographic algorithm for gray scale and color image based on logical operation. They embedded the MSB of secret image into LSB of cover image.
In [5] Navdeep Kaur et al. presented embedding based on the quantized DCT coefficients using the concept of Hadamard matrix. The result shows very high capacity as compared to other existing DCT techniques.
In [6] Zaidoon Kh. et al. have given a general overview of Steganography types, general Steganography systems, characterization of Steganography systems and classification of Steganography techniques.
In [7] Khan Farhan Rafat et al. presented the survey report of steganographic techniques and mainly focused on digital ASCII text documents as cover.
In [8] Nadeem Akhtar et al. proposed the variation in plain LSB algorithm by using bit inversion technique. They have used RC4 algorithm to achieve the randomization of message bits before hiding the message bits into the cover image. The result shows enhancement in security as well as quality.
In [9] Babloo Saha et al. presented review of different existing digital image Steganography techniques of data hiding in spatial, transform and compression domains.
In [10] Mamta Juneja et al. presented an approach to embed the text into gray scale image using RC4 stream cipher method and stored the text in non sequential pixel in image by use of variable hop value power. In this approach they have shown that robustness increases due to multilevel security architecture along with faster embedding and extraction process.
In [11] Gopika Mane et al. proposed stream cipher cryptography using RC4 algorithm, steganography by F5 algorithm and watermarking using quantization index modulation algorithm to give access of the original data to the authorized party only.

VII. PROPOSED WORK

In Proposed work, Cryptography and Steganography differ to each other because cryptography is used to keep the contents of the message secret while steganography is used to hide the existence of secret message. Both techniques are used to protect information from the unauthorized use but sometime it is used in illegal means and neither cryptography is alone perfect nor steganography. Both approaches can be used with each other, to provide better security because cryptography makes the message secret and steganography make existence of message invisible. Steps used in proposed work:

- Implement text combined image based Steganography.
- Encode the text in the sentences in the form ASCII codes.
- Take a stego- image in order to hide the information data.
- Hide the message information using least significant bit algorithm.
- Calculate the Peak signal to noise ratio and mean square error.

In the proposed work we combine two techniques text steganography and image steganography. Proposed text based steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence construction.

VIII. FLOW CHART OF THE METHODOLOGY

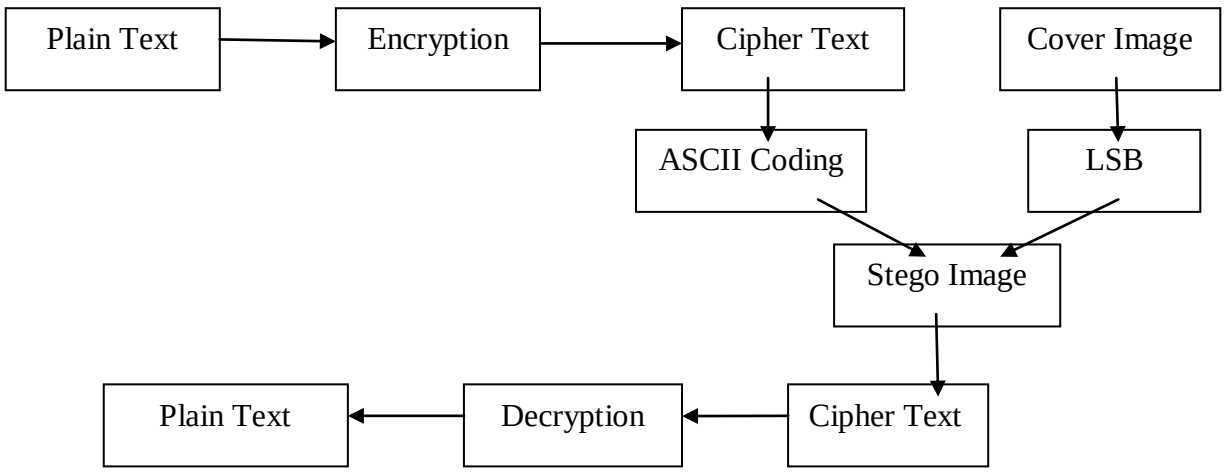

Fig. 3 Methodology flow chart

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

IX. CONCLUSION

In the era of fast information interchange using internet and World Wide Web, Steganography has become essential tool for information security. This paper presents a review work in different steganography methods and factors which affect the steganography.

REFERENCES

[1] Stuti Goel, Arun Rana and Manpreet kaur, "Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems, vol.3, May 2013, pp. 20-30.
[2] Himanshu Gupta, Ritesh Kumar and Soni Changlani, "Steganography Using LSB Bit Substitution for Data Hiding", International Journal Of Advanced Research in Computer Science and Electronics Engineering, vol.2, October 2013, pp. 676-680.
[3] Vikas Tyagi, Atul Kumar, Roshan patel, Sachin Tyagi and Saurabh Singh Gangwar," Image Steganography using Least Significant Bit With Cryptography", Journal of Global Research in Computer Science, vol.3, March 2012, pp. 53-55.
[4] Vijay Kumar Sharma and Vishal Shrivatav, "A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimizing Detection", Journal of Theoretical and Applied Information Technology, vol.36, February 2012, pp.1-8.
[5] Navdeep Kaur and Sukhjeet K.Ranade, "High Capacity Data Embedding System in DCT Domain for Colored Images", International Journal of Computing and Business Research, vol.3, September 2012.
[6] Zaidoon Kh.Al-Ani, A.A Zaidan, B.B Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography", Journal of Computing, vol.2, March 2010, pp.158-165.
[7] Khan Farhan Rafat and Muhammad Sher, "Survey Report: - State of the Art in Digital Steganography Focusing ASCII Text Documents", International Journal of Computer Science and Information Security, vol.7, 2010, pp.63-72.
[8] Nadeem Akhtar, Pragati Johri and Shahbaaz Khan, "Enhancing the Security and Quality of LSB Based Image Steganography", Proceedings of IEEE International Conference on Computational Intelligence and Communication Networks, September 2013, pp.385-390.
[9] Babloo Saha and Shuchi Sharma,"Steganographic Techniques of Data Hiding Using Digital Images", Defence Science Journal, vol.62, January 2012, pp.11-18.
[10] Mamta Juneja and Parvinder S. Sandhu, "An improved LSB based Steganography with Enhanced Security and Embedding/ Extraction", Proceedings of IEEE International Conference on Intelligent Computational Systems, January 2013, pp. 29-34.
[11] Gopika Mane, Priti Deshmukh, Sukul Fadnis, Sheetal Jadhav and Manoj S.wakchoure, "Imperceptible Stego- Marked Image Manipulation for Encrypted Data Hiding", International Journal of Application or Innovation in Engineering & Management, vol.2, October 2013, pp.72-77.

DOI10.17148/IJARCCE.2017.6574