A Review on Steganographic Techniques

Avni Singh Chauhan, Shreedhar Agarwal

Abstract: Steganography is the art of coveting data through which the sensitive information can be secured by covering it through a compatible media. Steganegraphy focuses on the existence of the cover media through which the data can't be accessed illegitimately. The paper provides a spectral view on the basic implementation and the various steganographic techniques. Here we profoundly deal with transmission techniques of tender data so as to make the system more reliable and robust.

Keywords: Steganograpgy, LSB, DCT, DWT, CNF, GNF, PSNR, Pseudorandom sequence.

I. INTRODUCTION

The word steganography has been derived from the Greek word 'stegano' which means covered and graphia means writing. Steganography is the process of coveting sensitive information through a cover object such that the triggered information cannot be discerned by the user. It focuses on hiding the sensitive information by embedding it into another media in such a manner that attacker cannot detect assailant cannot spot its presence. This technique has gathered recognition since there has been an aggression in the field of piracy, data sabotage and illegitimate communication between arsonist organization. The stego message (coveted information including text, audio, video, image and other types of medias represented by a bit stream) is embedded into the stego(cover media) passing through a communicational channel that is monitored by a stego key(secret). Being divided into two parts: ***Information embedding algorithm*** and ***Hidden information detection /retrieval method,*** the stego fields efficiently embeds the data**.** Information embedding is a type concealing dependent and for this digital images are regarded as a quite dependable cover. The covering media which embeds the sensitive data is a ***Stego image.*** Since we require a higher level of security for masking the sensitive data, the secret message is encrypted. The stego key is used by the sender in order to encode the code and so does the receiver require a decoding stego key. The basic considerations for the development of a steganograhic system are:

- ***Invisibility***: It difference between the stego image and the original cover image should not be perceived by human eyes.
- ***Capacity***: It is considered that greater is the storage capacity of a media, greater is the security and reliability that media provides.

Steganography is vividly used to prohibit the sabotage of sensitive information by unauthorized individuals. Even the famous terrorist group AL-Qaeda was found to use steganographic techniques in the year 2012 when one of their members was arrested with a memory stick in Russia, containing 100's of documents in concealed in two videos.

Revised Version Manuscript Received on May 20, 2015

Avni Singh Chauhan, IIIrd year, Department of Computer Science, Bachelor of Technology, JECRC University, Jaipur, India.

Shreedhar Agarwal, IIIrd year, Department of Electronics and Communication Engineering, Bachelor of Technology, LNM Institute of Information and Technology, Jaipur, India.

II. WORKING OF THE STEGANOGRAPHIC SYSTEM

Steganographic System basically stores secret information by converting it into an alternative compatible and equivalent media. This alternative media is then concealed within another object of the same media and then is transmitted to the recipient over a network. At the recipient's side, actual messages are then decrypted using a decrypt stego key.

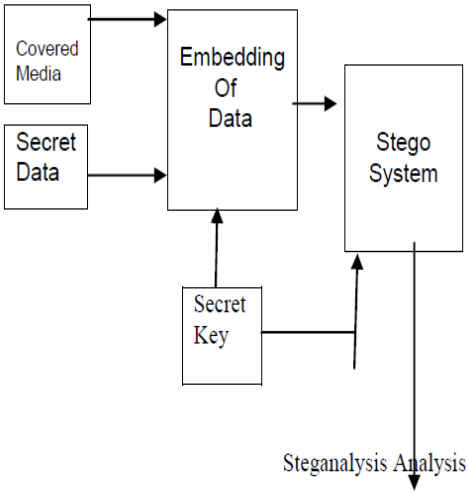

Figure.1: Basic Steganographic System

With a combination of cryptography and steganography, coveting of sensitive information can be implemented efficiently and dependably. In the former stage the secret message may be encoded with the help of cryptographic techniques and in the later stage the encoded stream can be steganographed in a compatible media. Now in such a case the sensitive message has a double layered protection, i.e., in case the steganographed pattern is identified, there still is an another secured layer of cryptographic encoding to be cracked. This makes the system more reliable.

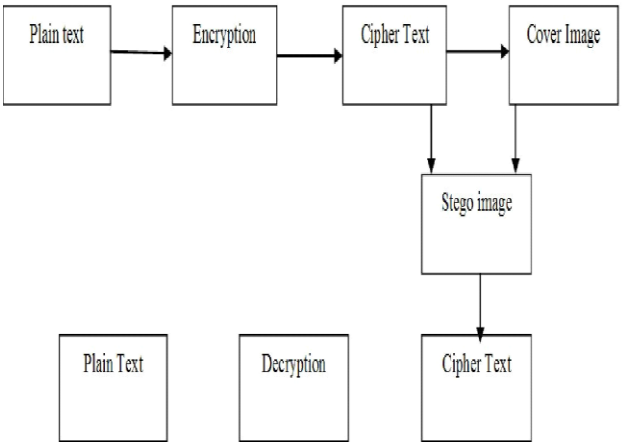

Figure.2: Combination of Steganography and Cryptography

Recently there has been a combination of LSB algorithm with the Discrete Wavelet Transform intending to determine security by the biometric measures. For example the identification of a person through his/her facial geometry, iris, ears or the uniquely defined finger prints.

III. STEGANOGRAPHIC TECHNIQUES

I. Image Steganograpgy:

In this technique the vulnerable data is concealed into an image through various steganographic techniques.

A. Spatial Domain:

This is generally implemented over gray scale in order to obtain an output through message bits. Here generally TIFF, JPEG and MPEG format of images is used since it uses DCT for its compression. One of the most widely used algorithm is LSB algorithm where the LSB of the given shade is replaced by the LSB of the given data by rendering and masking.[3] Basically the stegano image is fragmented into various bit planes and then the bit plane is replaced by the data to be coveted. This substitution implies the theory of substitution of the bit with minimal weight, so that there is no modification in the original image.[6] There is only one bit gap between the shades so that it cannot be perceived by human eyes. The disadvantage to this technique is that it is vulnerable and has a high noise ration that typically affects the PSNR (Peak Signal Noise ratio).[4]

The PSNR is obtained by the formula:

$$\mathbf{PSNR=10 \log 10 \ \frac{M \times N \times 255^2}{\sum ij \ (yij - xij)^2}}$$

here M and N are the image sizes and x and y are the image intensity values before and after embedding.[5] This type of embedding leads to a 0:5 bits/pixels on an average.[4].

B. Frequency Domain:

In this domain the hidden data covers significant area of the stego image but the usage of Compression, Cropping or Image Processing(may use Z- Transform technique) instead of the LSB algorithm.[6] The prime motive to use Frequency domain is to ensure the formation of a more reliable and secure algorithm. Here we basically alter the DCT coefficients of the stego cover.[7] It is well explained through the diagram:

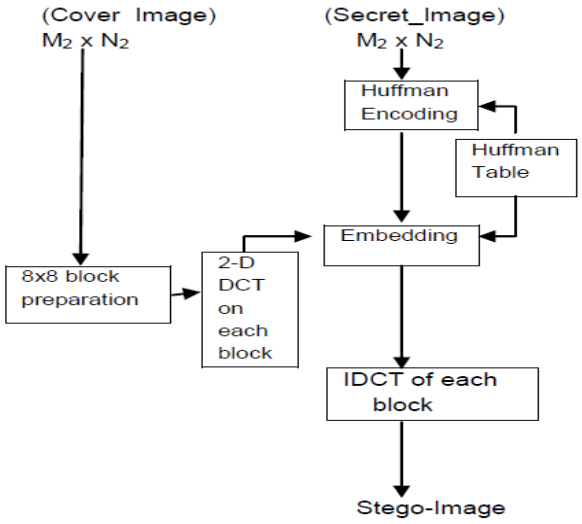

Figure3: Text Steganography (Insertion of stego image into cover.)

So, it is now clear how a JPEG image can be compressed and converted into DCT and now it can even use DWT, DFT and adaptive approach. [7] F5 implants data in DCT coefficient by taking a round off the quantized coefficient. Methods can be compressed and correlated steganography as proposed by Zheng and Cox.[8]

IV. TEXT STEGANOGRAPHY

Text Steganography is hiding up of sensitive data behind the text. It is quite easy to hide data in a video, audio or image but in case of text we have the structure of data to be conceived similar to that of the text so an ambiguity may arise in certain cases. So in such documents we require to bring about structural changes that are not noticeable as well as help in the implementation swiftly. Besides a text file takes a bare minimal memory as compared to the rest of the medias.[9] It can be classified into three major parts:

A. Format Based methods:

In this type of steganography we there occurs physical altering of text but this technique is not flawless since the word file may contain certain misspellings, change in font size or any other change may be detected by any human being.

B. Random and Statistical Method:

In this there occurs a random hiding of the sensitive sequence. In another method statistical properties like mean ,median, mod etc of word length is used in order to have similar statistical properties.[6][9].

C. Linguistic Method:

It determines the linguistic properties generated and determined.[9] It is a combination of syntax and semantics. It used the space structure like white space which are hidden and are not perceived by human eyes. The CFG creates a tree structure which is used for hiding the bits,here the left branch is 0 while the right one is 1. Here even GNF can be used. The text is syntactically flawless.

V. AUDIO STEGANOGRAPHY

In this there exists a technique in which the hidden text is covered by an audio media in such a manner that the coveted text cannot be perceived by human.

A. Least Significant Encoding:

This is used for the pitch period prediction conducted during low bit speed encoding. Watermark encoder usually selects the subset of the host of audio samples. It has a very high watermark channel's bit rate and a computational complexity that is really low. [1]

B. Phase Coding:

In this the audio file splits into blocks and the whole secret text is converted into first segment of the block.

C. Spread Spectrum:

In this technique two approaches are used: Direct Sequence Spread Spectrum and Frequency Hopping Spread Spectrum.[10] It spreads its functionality by multiplying it by pseudorandom sequence.

VI. IMPLEMENTATION

It is vividly is in the following ways:

- ***Usage in Modern printer***: Steganography is being used in modern printers, such as HP and Xerox brand colored laser printers. Tiny and little dots of yellow are added on top of each page. These dots are so tiny that they are barely visible to naked eyes. They contain encoded printer's serial number along with date and time stamps.
- ***Covered Communications***: Steganography enables us with potential capability to covert the existence of sensitive and confidential data. It is used for Strengthening of the secrecy of the encrypted data.
- ***Steganography for criminals***: It is also used in the non-commercial sector for hiding information. Terrorists can also use steganography to keep their communications secret and to coordinate attacks as seen on 26/11 in India.
- ***Alleged use by intelligence service***: It is used by the intelligence services to spy on the commencement of any illegal or felonious activity.

VII. CONCLUSION

Due to a sudden aggression in the field of data hiding Steganogaphy has emerged as an eminent factor. The paper provides a profound understanding of steganographic technique and its utility measures. The above techniques are efficient enough to bring about intrigue outcomes in the fore-coming developments in this field.

ACKNOWLEDGEMENT

The authors of this paper are highly endowed to the researcher's whose work has been referred to. It was a great source of inspiration without which we would not have reached to the level of writing this paper. This paper would be quite worthwhile in the research and development of Steganography in the near future.

REFERENCE

1. R.F. Olanrewaju, Othman Khalifa and Husna binti Abdul Rahman "Increasing the Hiding Capacity of Low-Bit Encoding Audio.Steganography Using a Novel Embedding Technique",World Applied Sciences Journal 21 (Mathematical Applications in Engineering. http://www.idosi.org/wasj/WASJ21(mae)13/14.pdf
2. J.R. Krenn January 2004,"Steganography and Steganalysis" http://www.krenn.nl/univ/cry/steg/article.pdf .
3. Anjali A. Shejul, Prof. U. L. Kulkarni, "A DWT based Approach for Steganography using Biometric", International Conference On Data Storage and Data Engineering, IEEE, pp. 39-43, 2010.
4. Ms. G. S. Sravanthi, Mrs. B. Sunitha Devi and S. M. Riyazoddin & M.Janga Reddy,"A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method",Global Journal of Computer Science and Technology Gaphics & Vision International Research Journal Publisher: Global Journals Inc. (USA) https://globaljournals.org/GJCST_Volume12/1-A-Spatial-Domain-Image-Steganography.pdf
5. A.Antony Judice,Dhivya Shamini.P,Divya Sree.D.J,"Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform",IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014 .
6. Rakhi1, Suresh Gawande"A REVIEW ON STEGANOGRAPHY METHODS",International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 10, October 2013.
7. A.Nag!, S. Biswas*, D. Sarkar*, P.P. Sarkar,"A novel technique for image steganography based on Block-DCT and Huffman Encoding",International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010 .http://www.airccse.org/journal/jcsit/0203csit8.pdf
8. Dr Mahesh Kumar and Mukesh Yadav and,"Image Steganography Using Frequency Domain",INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 9, EPTEMBER 2014. http://www.ijstr.org/final-print/sep2014/Image-Steganography-Using-Frequency-Domain.pdf
9. Monika Agarwal,Department of Computer Science and Engineering,"TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON ",International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013. http://www.airccse.org/journal/nsa/0113nsa07.pdf
10. Soumyendu Das ,Information Consultant,"Steganography and steganographic analysis:Different approach"

AUTHORS PROFILE

Avni Singh Chauhan, Qualification: III Year,Bachelor Of Technology Department, Computer Science Engineering, University/College: JECRC University, Jaipur, Rajasthan, India

Shreedhar Agarwal, Qualification: III Year, Bachelor of Technology Department, Electronics and Communication Engineering University/College : LNM Institute of Information and Technology, Jaipur, Rajasthan, India