A Comparative Study and Literature Review of Image Steganography Techniques

Latika
M. Tech Research Scholar
Department of Computer Science & Engineering
PIET, Panipat, India

Yogita Gulati
Research Guide
Department of Computer Science & Engineering
PIET, Panipat, India

Abstract

In the era of modern technology, there is a need of safe and secure communication. The art of impregnable communication through a safe medium like images is known as steganography. The process that detects the embedded data in the medium is called as Steganalysis. In this review paper, we have studied various methodologies proposed by the researchers in the field of steganography. The main objective of image steganography is to hide the existence of data from unauthorized action. Image steganography is a technique that provides a safe way to the secret embedded data to the target user. To hide the secret data in the images various techniques are proposed by the researchers, some are complex and other produce good results. Each methodology has good and bad points, so techniques are compared as well.

Keywords: Image steganography, steganography, stego image, cover image, Embedding, PSNR

I. INTRODUCTION

In the field of Information technology, Steganography referred to "cover writing "which is derived from Greek language. Steganography is defined by Markus Khan [1] as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". The main goal of steganography is to provide secure and robust communication. There are two more concepts which are often mixed with steganography: Cryptography and watermarking. 'Cryptography" is the technique through which plain text is converted in to cipher text, but the data cannot be hidden from malicious intention even if the cipher text is in unreadable form. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, [2] but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

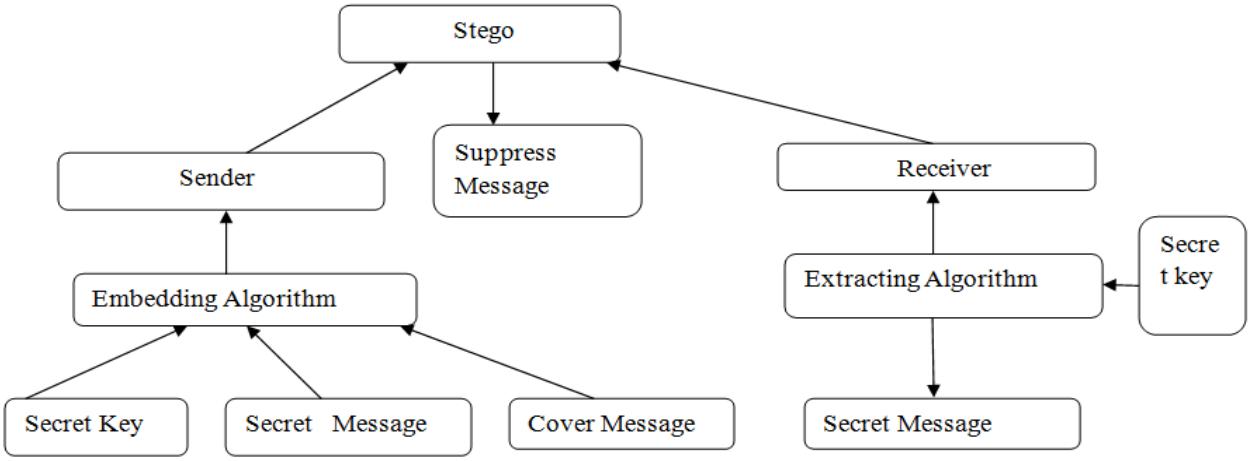

Fig. 1: Steganography system Scenarios [3]

The steganography can be done through different carriers i.e. we can classify steganography in to four types:

A. Text Steganography:

In this technique of steganography, the secret data is embedded in text form by altering certain properties of the text document. This technique is not widely used.

B. Image Steganography:

In this technique of steganography, the secret data is embedded in the image. This is achieved by adjusting the pixels values.

C. Audio Steganography:

In this technique of steganography, the secret data is embedded in the audio form.
Various audio formats which can be used to create a stego image are MPEG, AVI, etc

D. Protocol Steganography:

In this technique of steganography, communication protocol control elements are used to hide the secret data. This domain is referred to as the network steganography.

II. IMAGE STEGANOGRAPHY

Image Steganography is a technique through which we can embed the secret message in the image by adjusting the pixels intensities. Various terms that are used in Image Steganography are:

1) Cover Image: An image which is a carrier of secret information.
2) Stego Image: When the secret message is embedded in to the cover image, the resulting image is called as the stego image.
3) Message: The original data which is to be hidden
4) Stego key: To embed and retrieve the original data through embedding and retrieving algorithm respectively, the stego key is required.

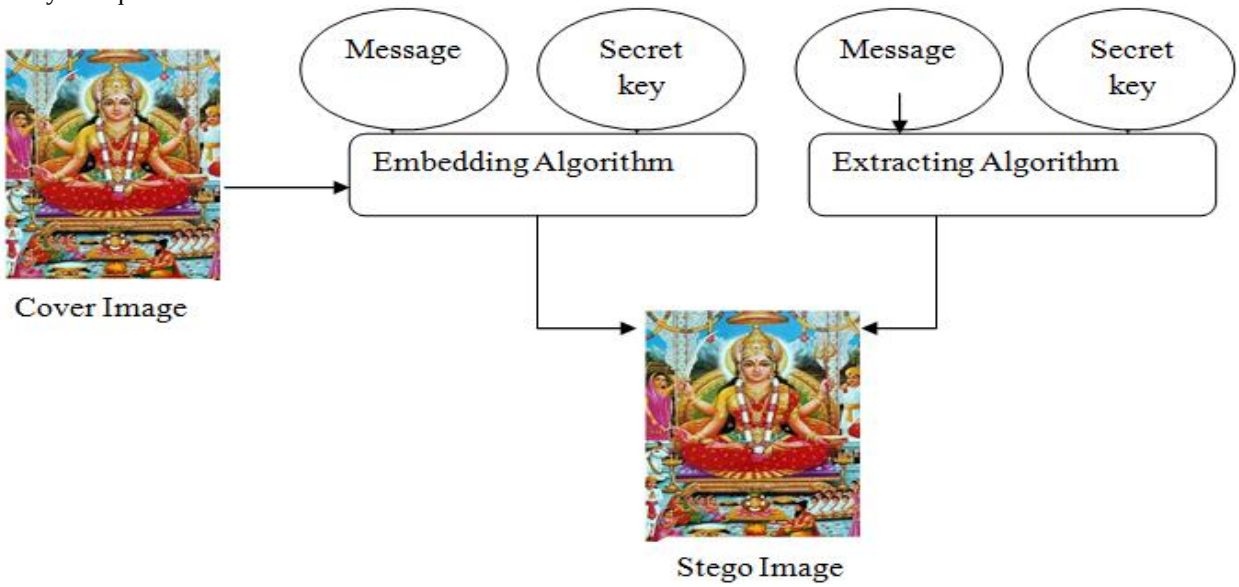

Fig. 2: Image Steganography Technique

A. Image Steganography Concepts:

1) *Image Definition:*

An image is a collection of numbers that constitute different light intensities in different areas of the image. [10] This numeric representation forms a grid and the individual points are referred to as pixels. The pixels in an image are displayed horizontally row by row. The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel.

2) *Image Compression:*

In images, there are two types of compression: lossless and lossy compression.
In lossless compression, every single bit of data is recovered when the image is decompressed; GIF (Graphic Interchange File) is one of the formats that provide lossless compression. In lossy compression, the extra information related to the original image especially the redundant information is removed permanently from the original file. JPEG image file provides lossy compression.

B. Evaluation Criteria for Steganography Techniques:

1) *Invisibility:*

The invisibility of steganography algorithm is the first requirement, since the strength of steganography lies in its ability to unnoticed by the human eye [4].

2) *Payload Capacity:*

Steganography aims at hiding information so, it requires large payload capacity.

3) *Robustness:*

When the steganography algorithms are applied then sometimes, they add a signature when embedding information; this can be easily detected through various statistical methods. There may be some cases where the image is cropped or its pixel values are altered before it reaches to the target destination, so the steganography algorithms should be robust against such malicious changes.

4) *Independent of the File Format:*

Only one format is used for secure communication even though there are different formats available on the internet, hence the steganography algorithms should be robust even that it should be able to embed the message in any kind of formats available on the internet.

5) *Unsuspicious Files:*

This requirement includes all characteristics of a steganography algorithm that may result in images that are not used normally and may cause suspicion.[4] Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

6) *PSNR:*

High is the PSNR , High is the secure communication because high PSNR refers to the fact that the difference between the stego image and cover image is less.

III. LITERATURE SURVEY

In [5], author has proposed an image steganography technique that is based on Integer Wavelet Transform (IWT). In the proposed technique the cover is 256x256 color image, two grey scale image of size 128x128 as secret message. Single level IWT of secret message is obtained; the resultant matrix consists of LL, LH, HL, HH bands. The LL sub bands hide the secret message. The authors showed through the experiments that two secret images can be hidden in one color image. The average PSNR values obtained are much better than other methods.

In [6], author has proposed a block complexity analysis for transform domain image steganography. Author has proposed an algorithm that is based on wavelet transform and bit plane complexity segmentation. The wavelet transform presentation of the cover is used to hide the secret message whereas the bit plane complexity segmentation is used as a measure of noisiness. The wavelet representation of an image is segmented in to 8x8 blocks and the capacity of each block is determined using BPCS. Author has also described various parameters which are associated with embedded image like PSNR, SSIM (Structural Similarity). The bit plane complexity images are obtained in embedding and extraction methods, which shows the improvement in the image quality.

In [7], author has proposed a data hiding scheme using image steganography and compression. Author has proposed a technique which processes the secret data first, and then this processed data is embedded in the LSBs of the cover image. 8 bit secret data is encoded as fixed length 12- bit code, in the compression process input characters are gathered in sequence along with it the dictionary is created that has single character strings corresponding to all possible input characters. So the capacity of all the cover images to embed the secret data increases by applying the proposed technique.

In [8], author has proposed a robust steganography algorithm which is based on DCT, Arnold Transform and chaotic system. In embedding process , the cover image is transformed using DCT , to further increase the security data is scrambled using Arnold transform , then the spreading is performed using chaotic sequences. The author has provided the concept of three keys, one for scrambling and two for generating chaotic sequences. In extraction process, inverse Arnold transform and inverse DCT is used. The experiment takes a host image which is first divided in to 4096 blocks of size 8x8, the cover image are 512x512 gray scale Lena, girl and Tank image . The logo is scrambled using Arnold transform. So the use of Arnold sequence increases the security level and algorithm is robust against the JPEG compression, addition of noise, low pass filtering and cropping operation as compared to other techniques. Thus the security is enhanced.

In [9], author has used various techniques like LSB, layout management schemes, only 0's and 1's are replaced from lower nibble from the byte and are considered for hiding secret message in an image. Author has also proposed various methods of data hiding based on the random bits of random pixels like replacing Intermediate bit, raster scan principle, random Scan principle, Color based data hiding, shape based data hiding. So, the techniques are analysed and it showed that the parameters responsible for noise in a cover image due to the hidden data depends on amount of data to hide , size of cover image, frequency of pixels available in an image, physical location of pixels.

IV. CRITICAL ANALYSIS

Table -1:
Comparison of Image Steganography Techniques

Lit. ref	*Image Steganography technique*	*Description*	*Advantage*
[5]	*Integer wavelength transform*	*Conceal Multiple Secret Images And Keys In A Color Cover Image*	*Best Of PSNR Value Are Obtained And The Technique Is Simple To Implement*
[6]	*Wavelet transform coefficients*	*By Retaining The Integrity Of Wavelength Coefficients At High Capacity Embedding , Best Secret –Embedded Image Is Produced That Is Indistinguishable From A Human Eye*	*Bit Plain Complexity Produces The Best Quality Images*
[7]	*LSB , LZW(Limpel-Ziv-Welch , modified Kekre Algorithm(MKA)*	*LZW Pre-Processes The Data (Lossless Data Technique), Compression Technique Is Also Used To Increases The Efficiency . The Data Hiding Capacity Is Calculated In Bytes.*	*High PSNR Value And Low MSE (Mean Square Error) Value Results In To Good Quality Image*
[8]	*DCT, Arnold transform and chaotic sequences*	*Concept Of Three Keys, One For Scrambling Through Arnold Transform And Two Keys For Generating Chaotic Sequences, Along With The Concept Of DCT And IDCT For Extraction Process. Testing Is Done In The Presence Of JPEG Compression , Low Pass Filtering ,Gaussian Noise Attack And Cropping Operation*	*Technique Is Very Secure, Provides Multilayer Security And Is Robust. Low Distortion Is Induced In The Cover Image*
[9]	*Spatial domain*	*Analysis Of Image Steganography Tools Is Performed And Parameters Of Image Are Considered Like Physical Location Of The Pixel, Intensity Value.*	*Noise Related Parameters Are Obtained Like Size Of Cover Image, Physical Location Of Pixel, Etc. These Parameters Can Produce More Robust And Secure Systems.*

V. CONCLUSION

In this paper, different image steganography techniques and their comparison were discussed, so that one can find the best technique for hiding the data. In literature review section, various proposed techniques are discussed. By analysing all the techniques , we have found that the combination of DCT, Arnold transform and chaotic sequence can produce a secure system and is more robust technique, hence can enhance the performance .

REFERENCES

[1] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html
[2] Ingemar J. Cox: Digital watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008
[3] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, vol., no., pp.385,390, 27-29 Sept. 2013.
[4] T. Morkel J.H.P Eloff, M.S. Olivier, "An overview of Image Steganography", information and computer Security architecture research group department of computer science, 2005.
[5] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, "a secure and high capacity image Steganography technique" Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, February 2013
[6] gowtham dhanarasi and Dr .A. Mallikarjuna Prasad, image steganography using block complexity analysis , International Journal of Engineering Science and Technology (IJEST) Vol. 4 No.07 July 2012
[7] Rahul Jain and Naresh kumar, "Efficient data hiding scheme using lossless data compression and image steganography ", International Journal of Engineering Science and Technology (IJEST) , Vol. 4 No.08 August 2012
[8] Siddharth Singh and Tanveer J. Siddiqui, "A Security Enhanced Robust Steganography Algorithm for Data Hiding" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012
[9] Dipesh Agrawal, Samidha Diwedi Sharma, "Analysis of Random Bit Image Steganography Techniques" International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013).
[10] http://prateekvjoshi.com/2013/03/20/image-steganography/