International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 2
ISSN: 2454-4248
96 – 99

Analysis of Various Techniques of Steganography for Embedding and Securing Data

Chetna Sharma
Research Scholar
(M.tech Pursuing ,CSE)
GGSCMT,Kharar,Punjab,India
Chetna97sharma@gmail.com

Inderdeep Kaur
(A.P CSE & M.Tech Coordinator)
GGSCMT,Kharar,Punjab,India
Chandigarh, India
kaur.inderdeep@gmail.com

***Abstract*—**Data has become vulnerable to attackers and viruses so that security of the data has become main purpose now days. The steganography is a proficient technique to secure the data and has a long history but now the steganography has changed a lot. In modern steganography the digital carrier, electronic text, disk space, network packets, digital images, digital videos, digital audio etc are used for hiding the data. This study is organized with an objective to have an overview to steganography and its various types. The techniques for image steganography are also discussed in this work.

***Index Terms*—** Data Security, Image Steganography, Stego Image.

*****

I. INTRODUCTION

Steganography is a course of action of stealthily insertion of data within a data source without affecting its intuitive features. The word steganography is dawned from the word 'Steganos' and 'graphia' which is related to the Greek language. It truly stands for 'covered' and 'writing' respectively. 'Covered Writing' is notoriously used for it. It is widely perceived as a process of wrapping a record within other documents. In most of the cases the originality of the data which is going to be hidden behind the cover photo is not maintained [1]. The variations in the uniqueness of the hidden data take place sometimes. The original information is converted to the alternate system file such as images, audio, video etc. Steganography relies upon the idea of camouflaging the secret information within an approved multimedia files [2].

Steganography is totally different from cryptography. Steganography is derived from cryptography but it is vaguer than cryptography. In cryptography, it is not possible for the intruder to decrypt the encrypted text without having the access to encryption key whereas in steganography the information is hidden behind the cover image without destroying the information and cover image [3]. The steganography the intruder did not have any idea regarding the stego message. The purpose of both the techniques is similar as both are developed to provide the high level security to the confidential information. The use of cryptography and steganography together is a good idea because it provides the enhanced level of security to the data [4-7]. The combination of steganography and cryptography persuades the various needs such as capacity, robustness, and security corresponding to achieve secure data sharing over an open communication channel. The following is the generalize block diagram corresponding to the process of steganography [8].

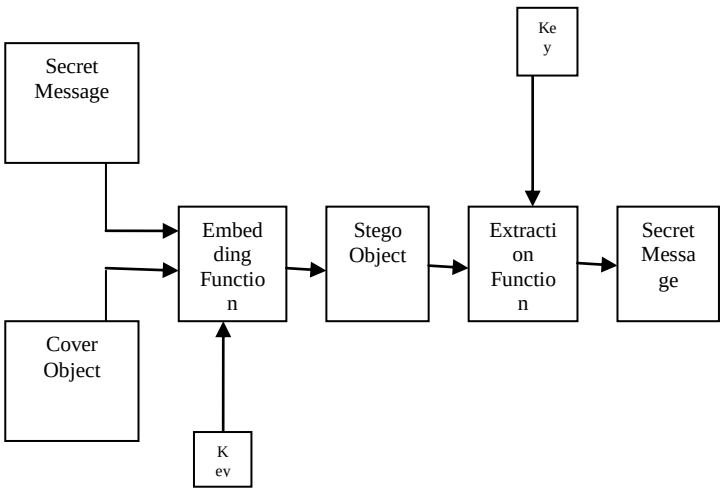

Figure 1. Basic Block Diagram of Steganography [9]

In figure 1 the process of steganography along with cryptography is shown. In this Firstly the message and cover image is selected and then the message is encrypted by using the private key by the sender and then the encrypted message is embedded on the cover image, after then the cover image is forwarded to the receiver. At receiver end the message is extracted from the cover image and then the decryption of the message is done by applying secret key shared by the sender [9].

 ISSN: 2454-4248
96 – 99

Basic impulse behind accomplishment of image Steganography is to communicate between the members without having fear of being attacked of messages. Due to its advantages, it has been used in several areas including military, intelligence operatives or bureaus. These fields of espionage required a method which can hide their critical data and no intermediate person can evaluate the meaning of the data. The main goal of using Steganography is to avoid the attention of the attacker from the hidden information in the transmitted as if attacker would come to know that there is a hidden data into the sent message then observer will try each possible idea so that he can read the hidden message.

A. Application of Steganography:

1. It is applied to make the communication process feasible over unsecure communication channel.
2. It bounds the third party to make alterations in confidential information.
3. It is also applicable to the domain of TV Broadcasting, audio and video etc.
4. For analyzing the network traffic.
5. For protecting copyrights.

II. CLASSIFICATION OF STEGANOGRAPHY

The classification of steganography is done as below:

1. Transform domain
2. Spread Spectrum Technique
3. Distortion Technique
4. Cover Generator Methods
5. Statistical Method

2.1 Substitution System Steganography

Substitution steganography method embeds the secret messages by replacing the insignificant bits of cover file with original message bits. The hidden message can be extracted by the receiver if and only if he has a knowledge regarding the location of the inserted bits of the hidden message. Temporal Spatial Domain techniques falls under the category of substitution based steganography method.

2.2 Transform domain Steganography

Transform domain us based on uses several frequencies regarding the insertion of the text in the image or cover file. It exploits domain methods for the purpose of steganography. Transform domain techniques are broadly classified such as below:

i) **Discrete Fourier transformation technique (DFT):** DFT is widely accepted efficient message embedding mechanism. In this, the brightness of the frame, magnitude corresponding to the coefficient is considered to evaluate the DFT.

ii) **Discrete cosine transformation technique (DCT):** The objective of using this technique is that it provides the good signal approximation by using certain coefficient values. This technique is used by many algorithms for the purpose of steganography.

iii) **Discrete Wavelet transformation technique (DWT):** DWT divides the cover image into four parts i.e. Horizontal section, Diagonal section, and Vertical section and Approximation section respectively. This process leads to an image with lower resolution. The DWT is more preferable technique due to less complexity and high accuracy. It is also efficient to manage the noise in the image.

2.3 Distortion Technique

Distortion of a signal is used to embed the secret message. Some modifications to the cover file are performed on the sender side. Then it is the responsibility of the receiver to recognize the original cover file and distorted cover file. In this a decoder is used for evaluating the modifications done by the sender so that the secret message can be recovered easily.

2.4 Cover Generator Methods

In variations to the above defined steganography techniques, when a confidential message is implanted to a unambiguous cover file by using a suitable message embedding techniques, few of the steganography based applications engender a digital entity with an objective of covering the information with an cover file.

2.5 Statistical Method

Statistical steganography method works on the basis of the "1-bits" scheme. Under this scheme one bit of information is embedded to the digital cover file. The message embedding is done by altering the cover file in such a manner that its statistical characteristics change itself if a "1" is transmitted. And if it is not "1", then its cover file remains unchanged. This is done so that the receiver can recognize the modified or unmodified ones.

III. LITERATURE SURVEY

In [1], the author recommended a steganography method by which is based on edge detection mechanism. This technique was capable to hide the large amount of text behind the edges of the colored images. In this, the boundaries of the objects in the images selected as a region of interest for hiding the data. The 3*3 window method and the first object alteration scheme were utilized for storing the hidden data. A high embedding capacity and high

 ISSN: 2454-4248
96 – 99

quality of the embedded image was appraised during the simulation of the purposed work.

In [2], An enhancing steganography digital method was developed by the author. The steganography was done by using the digital video files. The embedding location of the secret message was elected on the basis of the ROI (Region of Interest).first of all the frames from the video was extracted and then these frames were used for electing the region of interest for storing the hidden data. And thus, the steganography video was produced. The region of interest was selected from human faces and skin tones. The RGB image was converted to the YCbCr images. In YCbCr, the Cb was used corresponding to the center point of the skin tone and Cr was used for providing the security to the hidden data. The proposed work leads to the less distortion in the in the cover video because the parameter evaluation was before embedding the data.

In [3], the author developed a method to hide the secret data behind the three components of the image i.e. red, green and blue layer of the image. This was done by separating the layers of the image and then separated m*n matrix was assembled corresponding to individual color. Then pixel embedding method was implemented to each matrix. The message embedding was done by using sequential manners. The first bit of the secret message embedded behind the first pixel of the red layer, second bit is located behind the first block of the green layer and third bit behind the first pixel of the blue layer. Thus, the processing of the proposed work goes on. After getting the results, it was observed that the proposed work generated high quality images with high level security to the hidden data.

In [4] this paper author used the PVD technique as the basic of the image steganography. The purpose of this technique was to hide data behind the RGB pixels where the range of the pixels was limited to the 255. But in case of PVD technique the value of the pixel may reach out of the range of the pixel value which is disadvantageous. To overcome this problem the overflow of the pixel in the image is discarded. To achieve the security, data was hidden behind the number of bits of a pixel and it was quite tough to find out the number of bits used. After simulating the proposed technique it was observed that this technique was a lossless technique. Hence it was much better than the traditional techniques.

In [5], defined that **i**mage Steganography is a way to secure the data from the attackers. In this, author defined a new approach for data hiding with respect to colored image by using the combination of more than one technique. The methods used in this were LSB and adaptive LSB. Advanced Encryption Standards were used in order to embedding the pixels randomly and filtering for the purpose of removing the noise from the final image. The idea behind the proposed technique was that the pixels at the edges of the image are stronger to adapt the changes that are done in the image for hiding the data and also retains the originality of the image. The proposed technique was compared by the various techniques such as Chi square, histogram analysis and RS analysis etc. From the comparison results it was observed that the proposed technique posses much imperceptibility and the hiding capacity as compare to other techniques.

In [6] two techniques were utilized, one was wavelet transform and other was Genetic Algorithm. Frequency domain was used in order to increase the robustness of the technique. GA was used to embed the data by using DWT coefficient for achieving optimal mapping. It was done so that the amount of error between original and stego image can be reduced. Hence it leads to the increment in the hiding capacity due to lossless data compression. The results proved the working capacity of the proposed technique with respect to various dimensions such as efficiency, hiding capacity, robustness etc.

In [7], proposed a method for hiding the color grayscale image into a true image. Hiding of colored image behind the actual image is another technique for image steganography. A traditional cryptography technique named DES was used by the author. The comparison was done on the basis of image quality and data hiding capacity of the data. After results it was observed that the proposed technique leads to the better image quality in contrast to another technique. All in all it can be said that the proposed technique was better than the traditional technique with respect to the quality and data hiding capacity.

In [8], the author defined that in today's era users gets attracted towards the digital products because they offers high Quality of service. Digital products provide best services for wireless or wired products. Image steganography uses a digital image for hiding the data. Image steganography is one of the most prominent research areas for the research work because it provides high security to the confidential data. A new technique was proposed in which the data was hidden behind the intermediate significant bit of the image. In this technique the original data was alienated into number of blocks to reduce the length of the data. Then these blocks were used to embed data behind the image. The technique was compared with traditional techniques to find out the efficiency.

 ISSN: 2454-4248
96 – 99

IV. CONCLUSION AND FUTURE SCOPE

This study provides an overview of steganography and its various types on the basis of cover file that can be used for the purpose of steganography. The objective of this study is to analyze the techniques that can be used for embedding data behind a cover file.. The various authors developed many steganography techniques by using the advanced technologies. A literature study is also drawn in this work. his can be a guide to the researchers of this field.

V. REFERENCES

[1] Sneha Arora, Sanyam Anand, "A Proposed Method for Image Steganography Using Edge Detection," International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 2, February 2013, pp 296-297.

[2] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Enhancing Steganography In Digital Images," Canadian Conference on Computer and Robot Vision, IEEE 2008, pp: 326-322

[3] J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain," International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, pp 83-93.

[4] J. K. Mandal , "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain" International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, 2012, Pp 83-93

[5] Mamta Juneja, "Improved LSB based Steganography Techniques for Color Images in Spatial Domain", IJNS, vol 16(6), 2014, pp 452-462

[6] Sabyasachi Pramanik," Image Steganography Using Wavelet Transform And Genetic Algorithm", IJIRAE, vol 1(1),2014, Pp 17-20

[7] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., " A new Steganographic method for color and gray scale image hiding", Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, 2007, pp. 183-194

[8] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , 2012, pp.192-197.

[9] Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 201**3.** pp. 363-372.

[10] Vojtech Holub and Jessica Fridrich, "Low Complexity features for JPEG Steganalysis using undecimated DCT", IEEE transactions on information transactions and security, Vol. 10, No. 2, Pp. 219-228, February2015

[11] Vipul Sharma and Sunny Kumar, "A new approach to hide text in images using Steganography", International Journal of Advanced Research in computer science and software engineering, Vol. 3, No. 4, April 2013

[12] Krishna Nand Chaturvedi, Amit Doeger, "A Novel Approach for Data Hiding using LSB on Edges of a Gray Scale Cover Images", International Journal of Computer Applications (0975 – 8887) Vol. 86, No. 7, Pp 36-40, January 2014.

[13] Vijay Kumar Sharma, Vishal Shrivastava,"A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection", Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1 pp 1-8.

[14] S.Nanda Kishor, Dr. G. N. Kodanda Ramaiah and Dr.S.A.K.Jilani, "A Review On Steganography Through Multimedia", International Conference on Research Advances in Integrated Navigation Systems, April 2016

[15] Rina Mishra and Praveen Bhanodiya, "A Review on Steganography and Cryptography", 2015 International Conference on Advances in Computer Engineering and Applications, Pp. 119-122, 2015