Volume 6, Issue 6, June 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Review Paper on Image Steganography

[1] Ashadeep Kaur*, [2]Rakesh Kumar, [3]Kamaljeet Kainth

[1] Research Scholar, Sachdeva Engineering College, For Girls, Gharuan, Mohali, India

[2, 3] Department of Computer Science & Engineering, Sachdeva Engineering College, For Girls, Gharuan, Mohali, India

***Abstract****—Steganography refers to the data hiding. The main purpose of steganography is to hide the data behind images. It means that it encrypts the text in the form of image. The steganography is done when the communication takes place between sender and receiver [5]. Now a day's in data transfer over the network, the security is the main issue concerned with this. In order to secure the data while transmission steganography is used. Before the development of the steganography, Security of the data is the main concern of research for the researchers. The number of techniques was developed in order to secure transmission. Steganography use algorithms for hiding the data. In this the data is hiding behind the cover image. The data is hidden character wise behind the pixels of the image. The various algorithms or techniques used for steganography are LSB-Hash, RSA Encryption and Decryption [5].***

***Keywords— Data hiding; Audio; Video; Text; Security; LSB; Encryption***

## I. INTRODUCTION

In this modern era, where technology is developing at fast pace and each day new developments are made, security is of utmost priority. The data needs to be kept secure and safe so that it could be accessed only by the authorized personnel and any unauthorized user cannot have any access of that data. Data sharing is increasing as thousands of messages and data is being transmitted on internet everyday from one place to another. The protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that only the receiver should be able to understand the message. At first technique of cryptography was invented to send secret messages over places. In cryptography the message was encoded in another message in a covered way such that only the sender and receiver knew the way to decrypt it [5]. A cryptographic key was used to decode the message that was known only by the authorized persons. The limitation of cryptography was that other person came to know that the message had a hidden text in it and so the probability of message being decoded by other person increased. To overcome this limitation the technique of steganography was introduced.

The word steganography belongs to Greek language. In Greek the steganography stands for "covered writing". The first of all steganography was used in Greece. They use to enter the message on a wooden tablet and then apply wax on it to hide the written data. The technique of steganography was far better than cryptography as in it the data was hidden in image. The image was then sent over internet. It had advantage over cryptography as now the middle person does not come to know whether data is hidden in the image or not. The data could only be decrypted from image by the authorized person as he knows the phenomenon to decode it and had the authorized key with him that was required to decode the data. The security and the reliability of data transmission also improved with invention of steganography as now no other person could change the sent data. The main application fields of steganography are [4]:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by terrorists
- Digital Watermarking

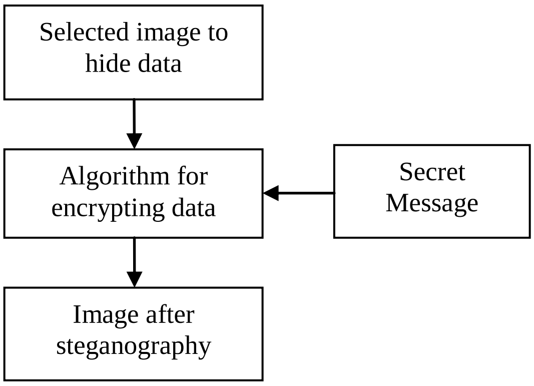
Selected image to hide data
Algorithm for encrypting data
Secret Message
Image after steganography

Figure 1 Diagram of Steganography

The steganography is done for the purpose of data security. The various techniques are used for steganography. The techniques are LSB, Data Compression, Masking and Filtering, Distortion Technique etc…

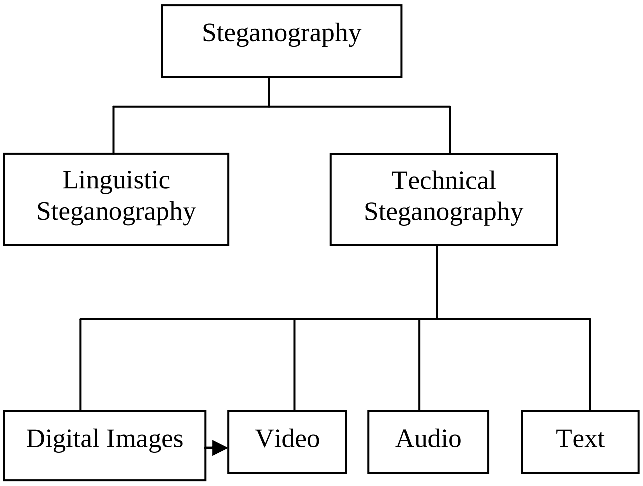

Figure 2 Types of steganography

## II. TECHNIQUES OF STEGANOGRAPHY

The various techniques for steganography is available. Some of them are as follows[4]:

- LSB
- Distortion Technique
- Masking and Filtering
- Transform Domain Technique

### *A. LSB*

LSB stands for Least Significant Bit. This is a technique for image steganography which works on the Least Significant Bit value of the pixels. This technique does not lead to any kind of distortion in the image while embedding data behind it. The value of least significant bit varies but this change is invisible to human eye. The LSB have many advantages such as the image does not depreciated or distorted and by using LSB one can encrypt large amount of data behind an image. It also poses some lacks also it is less robust in nature, sometimes changes in image can lead to the data lost, hidden data can be revealed easily i.e. less secure. LSB transfers the data to the receivers end with security without allowing the intruder to access the encrypted data [5].

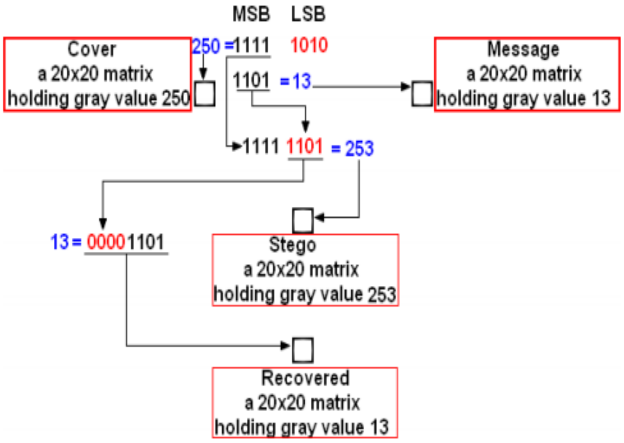

Figure 3 LSB technique for steganography

### *B. Distortion Technique*

Distortion technique encrypts the data by decoding it. In this original cover image is decoded into encrypted or distorted cover image. In this technique the receiver applies a function on encrypted or decoded image in order to decrypt it. In this steganography is applied by making distortions in image. This technique perform a sequence of alterations in cover image. Then this sequence is applied for the purpose of comparing the encrypted message with forwarded message. The data is encrypted behind randomly selected pixels. In case when the encrypted image vary from original image then bit "1" is used else bit "0" is used. In this cover image is send to the receiver which is a barrier in the security provided by this technique. It is a rule tat the cover image should always used for once while steganography if any cover image is used more than once in steganography then it will easy for the intruders to attack the image for accessing the encrypted data behind the image [5].

### *C. Masking and Filtering*

This technique works similarly to the technique of watermarking. In this case data is not hidden behind any image. Instead of hiding data is appended or inserted on such space which is secure from attackers. In this technique watermarking is used for securing the data. This method facilitate the user with the feature of robustness, compression is done because data is embedded on a secured surface and visible to everyone. The limitation of this system is that it is meant for only gray scale images [5].

### *D. Transform Domain Technique*

This technique posses much complexity as compare to other techniques. It performs steganography by hiding the data behind an image. It uses many algorithms to encrypt the data. Some transformations are also used for steganography. As it is clear from the name of the technique that number of transformation domains are used for embedding the data and then further algorithms are used for encryption. The data is embedded in frequency domain. It is much preferable technique of embedding the data in comparison of time domain. This technique hides the data in that images which are safe from attackers and there is no need of data compression in this technique [5].

## III. RELATED WORK

**Amritpal Singh, et al. (2015), [1]** In this paper the author states that steganography is a technique which hides the data in such a way that it is not visible to user. Steganography has divided into many types like Audio, Video, Text, Image. In case of image steganography data is hidden behind the image. In this cover image is used to hide the data. The image obtained after embedding the data is known as stego image. Various methods used for steganography are like LSB, Transform Domain, DFT and many more. All the techniques have some advantages and disadvantages. In this paper enhanced LSB technique is developed by the author which overcomes the limitations of other techniques. LSB technique for color images by embedding the information into three planes of RGB image in a way that enhances the quality of image and achieves high embedding capacity. The PSNR value of the proposed technique is better than previous steganography methods.

**Mehdi Hussain et al, (2013), [2]** In this paper the author defines steganography as a technique which secures the confidential data from unauthorized user. It is used world wide for the purpose of securing the data while transmission. With the increase in number of users for internet the use of the steganography is also increased to an extent. It is also known as invisible communication between sender and receiver. This technique deals with hiding the message existence for the purpose of security. Normally the data can be embedded in audio, video, image, sound, text etc. The application of steganography is military communication. Steganography is also used in content copyrighting. In this first of all a cover image is used to embed the data behind it and after inserting the data the image becomes stego image. In this paper author uses various steganography techniques and application or classifications are also defined.

**T. Morkel et al, [3]** The author in this paper states that steganography is a creativity to hide the data behind an image, an audio, video or text. In other words it is also known as the process of hiding the information within other information. Many file formats are used for steganography like .jpeg, .png. The digital image is more preferable for steganography due to its frequency over the internet. There are many techniques for steganography. The choice of the technique is based on the nature of the application for which it is being used like some application requires high level of confidentiality whereas some demands for medium level secrecy in their application. In this paper the main focus is on checking the compatibility of the technique of steganography for application and then the most suitable technique is applied to the application for steganography.

**R.Poornima et al, [4]** In this paper author described that the hiding capacity is an important concern of data hiding or steganography. Steganography is a technique which hides the data behind the image or audio, video etc. in such a way that the original data can't be visible to the user. Only receiver can decrypt the data. Various methods for steganography are like audio, video, text or image. The image steganography is most widely used technique for hiding data. The methods used for this technique is transformation domain. In this communication is done by encrypting the password. But only sender and receiver have the access of message.

**Anil Kumar et al, 2013, [5]** In this paper author says that security is the major concern for the researchers as mostly people use internet for data transmission. Steganography is a technique for encrypting the data in such a way that only sender and receiver can decrypt the information. No one else except receiver can access the data or information. But still researchers focus on securing this technique to a high level. In this paper author defines various techniques for steganography like Hash- LSB with RSA algo. This ensures that by using this technique data is much secure. In this technique the data is encrypted firstly and then embedded behind the image. In case if encrypted data is revealed even then only receiver can access the data.

**Shaveta Mahajan et al.2012, [6]** In this paper author organizes a survey and observed that various techniques are available for steganography. This technique is the process of converting the information in a pattern or format which is only visible to the sender and receiver. Along with encryption this also adds other changes in the image. The various methods of steganography are audio steganography, video steganography, image steganography, text steganography. The main parameters considered in image steganography is quality of the stego image and capacity of the cover.

**Jasleen Kour et al. 2014, [7]** In this paper author states that steganography deals with a way to achieve the secrecy of communication between sender and receiver. It is also known as invisible communication. It encrypts the data in such a way that the secrecy of the information remains. Various kinds of steganography techniques are image steganography, video steganography, audio steganography, text steganography. Each and every technique uses some algorithm for the purpose of encryption. Therefore all techniques poses some advantages and disadvantages also. The defined techniques of steganography are LSB, Transformation Domain etc. Some other are ISB, MLSB.

## IV. CONCLUSION

Steganography is a technique of covering the data in such a way that the message could be transmitted secretly and only the sender and receiver knows the way of decrypting that secret text or message. Steganography increases the security of data to be transmitted and also ensures that only authorized personnel can have access to that message. This paper presents a review of steganography and techniques that are used for steganography. Various papers have been reviewed on steganography. It is studied that there is various types of steganography like text, audio, video, image, network or protocol steganography [7]. This shows that text or data using steganography can be hidden in many ways. Techniques of steganography have been reviewed and studied in the paper.

## REFERENCES

[1] Amritpal Singh, “An Improved LSB based Image Steganography Technique for RGB Images”, Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015., pp 1-4

[2] Mehdi Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013, pp 113-124

[3] T. Morkel, “AN OVERVIEW OF IMAGE STEGANOGRAPHY”, *ISSA*. 2005, pp 1-11

[4] R.Poornima, “AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY”, (IJCSES) Vol.4, No.1,February 2013, pp 23-31

[5] Anil Kumar, “A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique”, IJARCSSE, Volume 3, Issue 7, July 2013, pp 363-372

[6] Shaveta Mahajan, “A Review of Methods and Approach for Secure Stegnography”, IJARCSSE, Volume 2, Issue 10, October 2012, pp 67-70

[7] Jasleen Kour, “Steganography Techniques –A Review Paper”, International Journal of Emerging Research in Management &Technology, Volume-3, Issue-5, May 2014, pp 132-135

[8] Atallah M. Al-Shatnawi, “A New Method in Image Steganography with Improved Image Quality”, Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915

[9] C.P.Sumathi, “A Study of Various Steganographic Techniques Used for Information Hiding”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013, pp 9-25

[10] Rashi Singh, “A Review on Image Steganography”, IJARCSSE, Volume 4, Issue 5, May 2014, pp 686-689

[11] Gunjan CHUGH, “IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW ARTICLE”, 2013. Fascicule 3 [July–September], pp 97-104

[12] Shikha Sharda, “Image Steganography: A Review”, IJETAE, Volume 3, Issue 1, January 2013

[13] Stuti Goel, “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, pp 8-14

[14] Rakhi, “A REVIEW ON STEGANOGRAPHY METHODS”, IJAREEIE, Vol. 2, Issue 10, October 2013, pp 4635-4638

[15] Anjali Tiwari, “A Review on Different Image Steganography Techniques”, IJEIT, Volume 3, Issue 7, January 2014, pp 121-124

[16] Prof.S.V.Kamble, “A Review on Novel Image Steganography Techniques”, IOSR-JCE, ISSN: 2278-0661, ISBN: 2278-8727, PP: 01-04

[17] Amandeep Kaur, “A Review on Image Steganography Techniques”, International Journal of Computer Applications (0975 – 8887) Volume 123 – No.4, August 2015, pp 20-24

[18] Abbas Cheddad, “Digital Image Steganography: Survey and Analysis of Current Methods”, Signal Processing, Volume: 20, Issue: 3, March 2010, pp 727-752

[19] Soumyendu Das, “Steganography and Steganalysis: Different Approaches”