ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.5

# A Review on Information Hiding Methods

Tanu Kumari[1], Kuldeep Singh[2]
M.Tech Student[1], Assistant Professor[2]
Department of Computer Science
Delhi College of Technology and Management, India

**Abstract:**
As the communication increases over the network, information security becomes an important issue. For secure data transmission, steganography is used. At about three decades, information hiding has been a good camouflage data transmission method. Now a days, there are several data hiding methods to hide the data from the attackers. Image Steganography is one of them. Steganography was introduced in 1980. Actually, these are the hiding tricks which are inspired by nature. For example, there are lots of bio species in this world which can change their color and can hide themselves from the attackers. Steganography can be defined as it is the method of hiding the data. Basically, the data is hide behind the images. It means that the text is send in the form of images. There are various algorithms which are used for image steganography such as LSB, DWT, DCT, DFT etc. In this paper, we review the various steganography methods in detail.

**Keywords:** Steganography, cover image

## I. INTRODUCTION

At this time, because technology is developing very fast so there is a need to protect our data from the attackers. That's why network security is our first precedence. Nowadays, a number of messages are channeling over the internet due to which sharing of data becomes more so we have to protect our data from the unauthorized users. So at the very first time, the concept of cryptography comes into the existence. In this method, the sender sends their data with the secret key i.e. encryption at the receiver end, the receiver receives that data by decode that data with hat secret key i.e. decryption. But the concept of cryptography was not so good. Other users can also decode that hidden data. So the concept of steganography comes. Steganography is the Greek word which means the "covered writing". At the first time, this was used by Greek. They write their message on the wooden slab and wax on it. This is much better than the cryptography. In this technique, the information is hidden in the cover image. And now the attacker doesn't know that is there any information or not? Now only the receiver can decode the message. Because he knows the procedure of decoding.

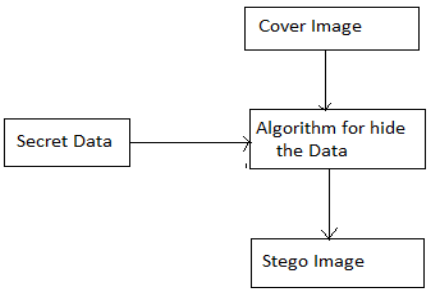


**Figure. 1. Data Hiding**

**Some applications of steganography are:**

- Data protection
- Media database system
- Secret communication
- Used by terrorist also

**Steganography is of two types-**

1.) Linguistic Steganography

2.) Technical Steganography

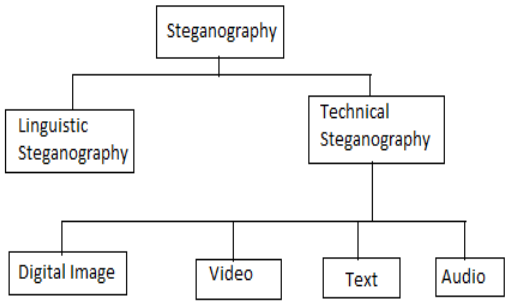


**Figure.2. Classification of steganography**

## II. TECHNIQUES OF STEGANOGRAPHY

There are various techniques for steganography. Here, we are talking about image steganography. Image Steganography is further divided into following categories:

A.) Spatial Steganography

B.) Frequency Steganography

C.) Masking and Filtering

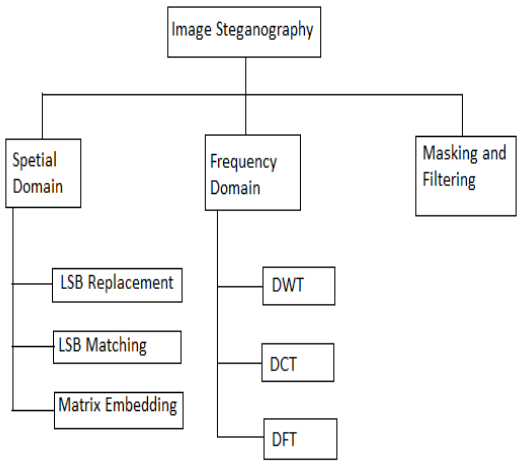


**Figure. 3. Classification of Image Steganography**

### A.) Special Domain Steganography

In this steganography technique, the secret message is hidden in the covert image by doing some changes in the pixels of the cover image by using LSB encoding. These changes in the cover image are undetectable. It means that the human eyes cannot detect these changes. In this technique, the secret message is embedded in the intensity of pixels of the cover image. And a large amount of data can be sent easily and safely by using this technique.

**There are various types of spatial domain steganography techniques such as**

- LSB Replacement
- LSB Matching
- Matrix Embedding

#### 1. LSB Replacement

In LSB Replacement technique of steganography, some of the bits embedded in to the message to encrypt the message. Due to embedding these bits the attacker cannot find the original message. But there is also some problems with this technique. This method of data hiding is not robust. Sometimes, even the receiver is not able to generate the correct image.

#### 2. LSB Matching

LSB Matching steganography is much better than the LSB Replacement steganography. In this steganography technique, 1 is adding or subtracting from the value of the cover image pixels. In this technique, it is not easy to detect or uncover the hidden message as compare to LSB Replacement steganography.

#### 3. Matrix Embedding

In this technique, the text message and cover image both are encoded by the error correction code. It changes the cover image due to the coding. In this steganography technique, the text bits are inserted alternatively as per the inserting change. So, due to it the efficiency of insertion increases.

### B.) Frequency Domain Steganography

Frequency Domain Technique hides the data into a particular area of the cover image. In this technique, the information is usually fixed into the different coefficient of the image. It gives more capacity for data hiding and robustness against attacks. The steganography technique uses JPEG file formats because of the small size. The use of JPEG is prevalent in digital photography. It is used for lossy compression technique. There are various steps in JPEG compression like RGB to YUV conversion. As per the review, there are various algorithms for frequency domain steganography. This technique hides the information in those areas of the image which are not exposed in the image processing. So, this technique is better than the LSB method of steganography.

Frequency Domain Steganography includes various techniques like:

- Discrete Wavelet Transformation
- Discrete Cosine Transformation
- Discrete Fourier Transformation

#### 1. Discrete Wavelet Transformation

Wavelets are those functions which obtained over a fixed interval and its average value is zero. For multi-resolution demonstration, this transformation is very important to be used for signal investigation and image processing. It may divide a signal into various factors in frequency domain. 1-D DWT segments a covert image is divided into two major components known as approximate component and detailed component. A 2-D DWT is used to segment a covert image into mainly four sub components: one approximate component (LL) and the other three components are (LH, HL, HH).

#### 2. Discrete Cosine Transformation

Discrete cosine transformation technique separates an image into various parts of differing significance and these differing significance is associated with the quality of the image. As it changes an image from its spatial domain into frequency domain, it harmonize the Fourier Transform Technique. In this method of steganography, for each color constituent, the JPEG format of image uses cosine transform to convert consecutive pixel blocks of size 8 x 8 into a count of 64 cosine coefficients each.

#### 3. Discrete Fourier Transformation

Discrete Fourier Transformation technique convert the time and space based message into frequency dependent message. This technique separates the images into the terms of sine and cosine, so it is important. All the frequencies of images does not includes in it. In applications like image compression, image filtering and construction, this technique is useful.

### C.) Masking and Filtering

In this technique, the data is hiding by marking the image. This technique used in greyscale images. In this method, the data is hiding by placing the watermark on the image. The information is hidden in the specific areas of the image, not only at the noise level of the image. Due to the lossy method of compression watermarking can be functional without the fear of image destruction. There are also some other techniques for hiding the data like information hiding in corners etc.

## III. RELATED WORK

**Provos[1]** In this paper the author noted that to the smaller portion of the images, by applying the same logic method could still be used for detection of randomly scattered information. However, for the generalized approach, the author does not give further details or estimates of false positives and negatives. **Provos[2]** In this paper the author carried out an vast discussion of JPEG images downloaded from eBay.

The author identify a number of suspicious images embedded with JP Hide&Seek and J-Steg, by using his steganalytic software. To recover the hidden information, a dictionary attack was then applied in an attempt. This test did not express the existence of hidden information **Pfitzmann and Westfeld[4]** In this paper, author introduced a method which is based on Pairs of Values (PoVs) of statistical analysis that are exchanged during message embedding. Pairs of Values are differ in the LSB only. When we know the information placement, this method provides very reliable results. **Mehdi Hussain [5]** In this paper the author defines steganography as a technique which is used to secure the information when it is transferred over the network. It is used in worldwide for hiding the confidential data which secures the confidential data from unauthorized user. There is a cover image used to embed the data and when we insert the data or information in it, it becomes stego image. There are various steganography techniques are used, in this paper and the author also defines uses various application or classifications our Conference Paper must follow these overall formatting specifications.

## IV. CONCLUSION

Steganography is the way of transfer the confidential data by hiding it. In this technique, the data encrypted by the sender and only receiver knows that how the data can be decrypted. Due to it the security of data increases when the data is transmitted over the channel and unauthorized person cannot access it. In this paper, there is a review on various types of steganography which are used for hiding the confidential data. In this paper, it studied that there are several different types of steganography technique such as image, audio, video and text etc. this paper, mainly focused on image steganography and its various technique which are discussed here.

## V. REFERENCES


[1]. N. Provos, "Defending Against Statistical Steganalysis", 10th USENIX Security Symposium, Washington, DC, 2001.

[2]. N. Provos and Peter Honeyman, "Detecting Steganog raphic Content on the Internet", CITI Technical Report 01-11, August 2001, submitted for publication.

[3]. M. T. Sandford II, J. N. Bradley, and T. G. Handel, "The data embedding method", In Proc. of the SPIE Photonics East Conference, Philadelphia, September 1995.

[4].A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," Lecture Notes in Computer Science, vol.1768, Springer-Verlag, Berlin, 2000, pp. 61−75.

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

[6]. 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

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

[8]. T. Morkel, "AN OVERVIEW OF IMAGE STEGANOG RAPHY", ISSA. 2005, pp 1-11

[9]. R.Poornima, "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY", (IJCSES) Vol.4, No.1,February2013, pp 23-31

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

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

[12]. Abbas Cheddad, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Volume: 20, Issue: 3, March 2010, pp 727-752 +

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

[14]. 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

[15]. Rashi Singh, "A Review on Image Steganography", IJARCSSE, Volume 4, Issue 5, May 2014, pp 686-689

[16]. Gunjan CHUGH, "IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW ARTICLE", 2013. Fascicule 3 [July-September], pp 97-104

[17]. Shikha Sharda, "Image Steganography: A Review", IJETAE, Volume 3, Issue 1, January 2013

[18]. F. A. P. Peticolas,, "Information hiding-a survey", Proceedings of the IEEE, Vol. 87, pp. 1062-1078, 1999

[19]. Sunny Dagar, "Highly randomized image steganography using secret keys", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE) , pp. 1-5, 2014.

[20]. Reena M. Patel & D J Shah, "Multiple LSB data hiding based on Pixel value and MSB value", IEEE Nirma University International Conference on Engineering, pp. 1-5, 2013.

[21]. 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