A Review on Image Steganography Techniques

Amandeep Kaur
Department of CSE
Chandigarh University,
Gharuan, Punjab

Rupinder Kaur
Assistant Professor
Department of CSE
Chandigarh University
Gharuan, Punjab

Navdeep Kumar
Assistant Professor
Department of CSE
Chandigarh University
Gharuan, Punjab

ABSTRACT
The emerging Internet Technology has led to the need of high level of security of data during its transmission. For this purpose steganography plays a major role in society. Steganography is basically the art of secretly hiding data or message in any cover medium such as an image, audio or video. Hence it allows secret communication to take place without the knowledge of any unintended user. This article gives a brief overview of image steganography and the techniques used for hiding data in the cover image to obtain stego image. The evaluation of performance is based on the value of PSNR.

Keywords
Cover image; PSNR; Steganography; Stego image.

1. INTRODUCTION
Throughout time, security has emerged to be a prominent issue. Whether the data is printed on a piece of paper or transmitted over network it may get exposed to eavesdropping. Cryptography is one method that helps in encrypting the data to be transferred. Then the encrypted text generally known as cipher text can be sent over the network to the receiver who can decrypt the data using the private key [1]. But the cipher text may lead to suspicion no matter how strong the algorithm is. So data may become prone to interception as the intruder may alter it to give a fake thought of any individual. Here, the need of steganography arises where the secret data can be camouflaged in some other medium that may be text, image, audio or video and then transmitted to the receiver [2]. The combination of cryptography and steganography help in increasing the security level of the data being transmitted. Steganography has originated from the Greek words "steganos" that refers to cover and "graphein" that refers to writing. Thus together it means covered or concealed writing [3]. It mainly aims to embed data in a cover medium so that no one can suspect the existence of information in it and thus helps in secret communication. The cover medium is known as the carrier and the image that contains the secret message is known as stego-image. The secret message may also be referred to as payload.

There should be minimum error difference between the stego-image and the original image in order to retain the quality of the image that is obtained after the data hiding process using various steganography techniques i.e. LSB technique, pixel value difference etc.

Cover medium + message + secret key = stego-medium

The paper is divided in to various sections as follows: Section 2 provides an overview of image steganography process. Section 3 discusses the various techniques related to steganography. Section 4 describes the steganalysis process. Section 5 provides an overview of the previous work related to steganography and its methods. Section 6 constitutes the comparison of results in terms of PSNR obtained by using different techniques. Section 7 concludes the paper.

2. IMAGE STEGANOGRAPHY
The most popular files for hiding data are the images. Image Steganography refers to the process of passing secret or confidential data in an image. In this process, an image is taken and secret message (payload) is set in that image and is passed to the sender. The sender can then extract the information from the image using the key provided by the sender.

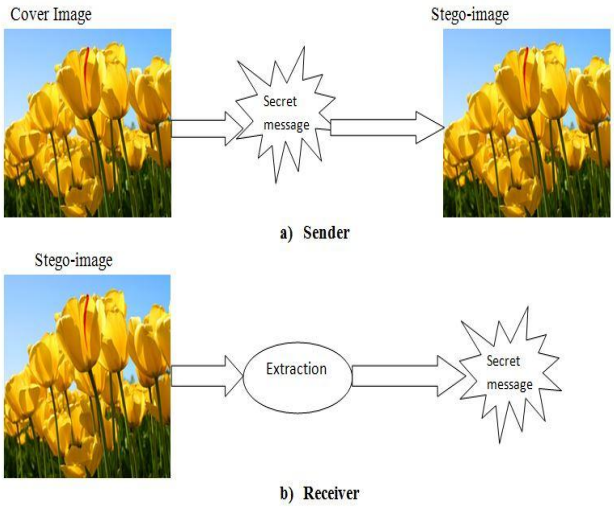

Fig 1: Steganography Process

3. CLASSIFICATION OF IMAGE STEGANOGRAPHY TECHNIQUES
There are numerous steganographic algorithms that can be used to embed secret information in a carrier medium. The algorithms can be categorized in following groups: spatial domain and frequency domain techniques which can further be divided as given below. Masking and filtering is also a common steganography technique.

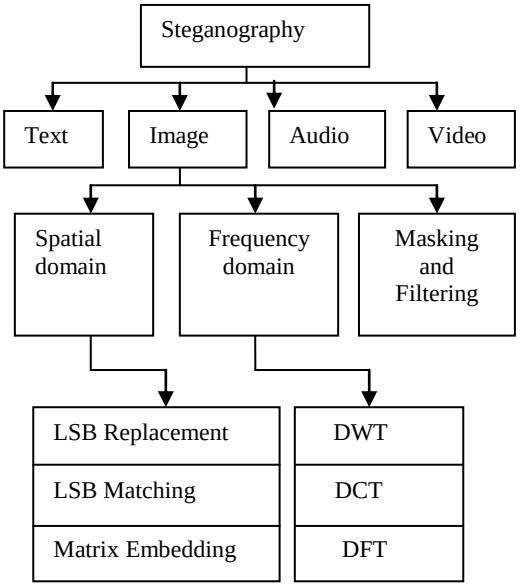

Fig.2: Classification of Image Steganography Methods

3.1 Spatial Domain Steganography

This method uses encoding in Least Significant Bits. LSB insertion method is an easy approach for embedding data into the actual image. There are numerous versions of this method; all these techniques reliably alter some of the bits in the values of image pixels for hiding data. LSB dependent steganography is one of the major techniques that hide confidential messages in the LSBs of some pixel values without any noticeable alterations [4]. For our human eye, variations in the LSB are unnoticeable. Embedding of bits of data can be carried out either simply or randomly. LSB techniques as well as Matrix embedding are some spatial domain techniques.

3.1.1 LSB Replacement

In this steganography, the cover pixel LSBs is substituted with a bit of the message that has to be embedded. Prior to embedding, the message is transformed into a sequence of bits which are then inserted sequentially where the LSBs are located [5]. This steganography is detectable even if there is low embedding rate.

Advantages of the LSB method are:

- Degradation of the original image is not easy
- Higher hiding capacity i.e. more amount of information can be embedded in an image

Disadvantages of LSB method are:

- Robustness is low
- Simple attacks may destroy the embedded data

1.2 LSB Matching

This type is much improved over LSB replacement method. In this process 1 is either randomly summed up or subtracted from the value of the cover pixel in case the bit of the confidential message is not equivalent to the LSB that come from the cover pixel [6]. As compared to LSB Replacement method it is hard to detect LSB matching.

1.3 Matrix Embedding

This technique encodes the original image as well as the message by an error correction code. It also alters the original image with respect to the result of coding. In this process the possible message bits are embedded randomly per an embedding change thus it helps in increasing embedding efficiency.

3.2 Frequency Domain Steganography

This method of steganography uses JPEG file format. This file format is quite common due to its small size. JPEG is a commonly used technique of lossy compression mainly for digital photography. JPEG compression involves various steps like conversion of RGB to YUV where Y refers to brightness, while U and V are used for chrominance and color [7]. Then is the transformation of image using techniques like Discrete Cosine Transformation etc. Then quantization and Huffman encoding is applied. It is recommendable to insert data before applying Huffman encoding as this stage is lossless. Transform domain techniques conceal data in the specific areas of the original image. Here the data is generally set into altered coefficients of an image giving much more capacity for information hiding and robustness against attacks. A number of algorithms are available for this. These techniques are better than LSB methods due to the fact that they embed information in particularly those areas of actual image which are not much exposed to processing of images. These techniques include:

3.2.1 Discrete Wavelet transformation

Wavelets are described as the functions obtained over a fixed interval and have zero as an average value. This transformation is an extremely necessary way to be used for signal investigation as well as image processing, mainly for multi-resolution demonstration. It may crumble a signal into a number of constituents in frequency domain. 1-D DWT segments a cover image further into two major components known as approximate component and detailed component [8]. A 2-D DWT is used to segment a cover image into mainly four sub components: one approximate component (LL) and the other three include detailed components represented as (LH, HL, HH).

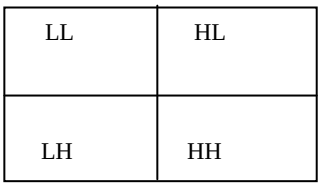

Fig 3: DWT Component

3.2.2 Discrete cosine transformation

This transformation technique is useful for separating an image into different parts of differing significance (which is associated with the image's quality). It resembles the Fourier Transform Technique as it converts an image from its spatial domain into frequency domain. In this technique, for every color constituent, the JPEG format of image makes use of cosine transform to convert consecutive pixel blocks of size 8 x 8 into a count of 64 cosine coefficients each. For each 8x8 block having pixel value f(x,y), the coefficients f(u,v) are given as [9]

$$F(u,v) = \frac{1}{4} C(u)\, C(v) \left[\sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2x+1)v\pi}{16} \right] \quad (1)$$

where

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, if\ u \leq 0 \\ 1, if\ u > 0 \end{cases}$$

3.2.3 Discrete Fourier transformation

This technique is important as it separates an image into the sine and cosine values. It converts space and time dependent information into the frequency based information. It is useful for a number of applications including image filtering and reconstruction as well as image compression. It does not include all frequencies that result to form an image but constitutes of only the set of those samples which are sufficient to describe the original image. The DFT for the vector *x* having length *n* is some other vector *y* having length *n* [10]:

$$y_{p+1} = \sum_{j=0}^{n-1} \omega^{jp} x_{j+1} \qquad (2)$$

Where ω signifies root nth for unity

$$\omega = e^{-2\pi i/n}$$

3.3 Masking and Filtering

Masking and Filtering is a steganography technique which can be used on gray- scale images. Hiding is similar to placing watermarks on a printed image. This method embeds the secret information particularly in more significant areas rather than hiding it only into the noisy section [7]. Watermarking methods can be functional without the fright of image demolition due to the lossy method of compression because it is more included into an image.

Some other techniques are based on hiding data in corners, hiding data based on texture similarity etc.

4. STEGANALYSIS

Cryptography and steganography together provide a higher security level to the secret data. Steganalysis is the process of detecting the secret information from the embedded image [8]. Because of the increasing popularity of the image steganography, there are a number of image steganalysis techniques. A commonly used technique is based on statistical interpretation.

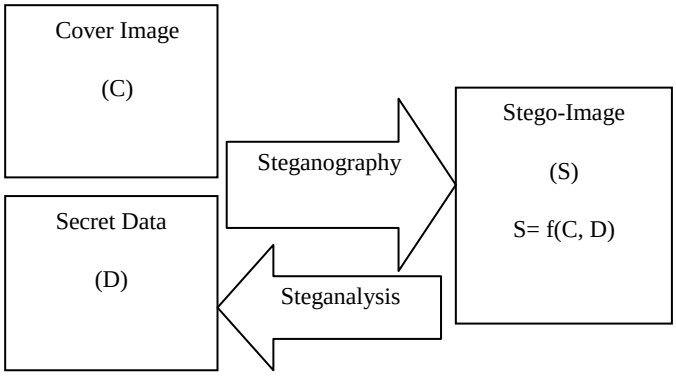

Fig.4: Steganalysis

The major challenges in steganalysis include:

- The suspected file may not contain hidden data in its contents
- The data might have been encrypted before it is embedded
- The file might be composed of noise of unnecessary data hidden in image

5. RELATED WORK

Reena M. Patel et al. [11] described various embedding techniques such as LSB insertion technique. The authors have also implemented some new methods of Multiple LSB methods. Various 8 bit gray scale images of 512x512 size were taken and Multiple LBS insertion technique was performed on them. Before the embedding the message it is converted in to ASCII bits. The length of data to be embedded has been taken as 15 KB or approximately 17143 characters. The parameters used are PSNR as well as MSE for the evaluation of results.

Amitava Nag et al. [12] presented a novel scheme for image steganography that involved LSB insertion using X-box mapping consisting several X-boxes having unique data. Embedding has been done by using this algorithm where four distinct X-boxes have been used with sixteen unique values where each value obtained was mapped with the four LSBs of original image. This was generally done to increase security and quality of the image. The mapping enhanced security level as without having sufficient knowledge about the rules of mapping it was not possible to extract the data.

Weiqi Luo et al. [13] reviewed the LSB Matching Technique for embedding data in an image. An edge adaptive scheme for data hiding using LSB Matching Revisited was provided. It helped to choose areas for embedding with respect to size of the confidential data as well as difference between any two successive pixels of original image. Regions having sharp edges were used for low embedding rate. The results were evaluated on 6000 different images that concluded that their proposed work enhanced the security level as compared to the other LSB based techniques.

Miao Ma et al. [14] proposed a rapid SAR segmentation method for images that relied on ABC algorithm. The image was firstly segmented using DWT. The low and high frequency coefficients were generated. An effective fitness function was produced for ABC after defining the grey number in the Grey Theory. The filtered image and the gradient image were then reconstructed and the grey entropy was defined to act as fitness function for ABC algorithm. By using this algorithm and the concept of onlookers, employed bees as well as scouts, the optimal threshold value was calculated. The results of the proposed technique concluded that this method was much better than Genetic Algorithm as well as Artificial Fish Swarm related segmentation methods.

El-Sayed [15] explored a method for detecting any misuse of steganographic techniques. The technique used neural network along with Levenberg-Marquardt propagation algorithm. It was used to eliminate the flaws of slow convergence that was common in back propagation as well as the problem of instability of the steepest optimization techniques. The proposed technique for automatically detecting stego images included embedding of messages by using the recently introduced Pixel Value Differencing Method. For this purpose Levenberg-Marquardt Neural Network had been used after analyzing the images prior to embedding as well as after embedding to get distinct features of image and then recognition model was built. The proposed

method was evaluated in comparison to some other machine learning techniques. The results showed that 99% detection rate had been obtained with few fake alarms

Manoj Kumar Ramaiya et al. [16] described an exclusive method of Image Steganography using the Data Encryption Standard that included S-Box Mapping as well as secret key for encryption. Encryption has been done in order to maintain security and authenticity of the data that has been embedded. The secret image's preprocessing has been done using an embedding function that included 2 distinct S-Boxes. This method resulted in enhancing security as well as the quality of image.

Zahra Zahedi Kermani et al. [17] presented a robust steganography technique with the help of gabor filter. Firstly the secret and cover image was divided in to 4x4 blocks. Then for each block of the secret image a similar block in the host image had been found. Gabor filter had been used to find out the resemblance with the texture patterns. Embedding was done by replacing the blocks of the image to be hidden with the blocks in cover image such that minimum distortion occurs. The results of this technique showed high capacity level and robustness.

Mohit Garg [18] proposed a new technique of text steganography that made use of html tags to embed secret data. The main idea behind this method was to embed data by altering the sequence of attributes as it would not affect the look that an html document has. HTML documents are generally used over the internet and hence do not attract the attention of intruders that there is any hidden data in the image. Therefore the data hiding capacity was more in the proposed technique.

Sunny Dagar [19] described a methodology which used two private keys to randomize the embedding process. This improved the security level of the hidden information. This technique used a pixel's R, G, B values and performed a few mathematical calculations. Depending upon the calculation, data to be hidden is inserted randomly at these positions. This helped to attain improved security that was not guaranteed in LSB substitution method. The parameter used for evaluation was PSNR which helped to evaluate the quality of the stego image. The results concluded that the proposed algorithm was more efficient when compared with other method.

N. Vinothkumar et al. [20] provided a method for steganography that used Integer Wavelet Transform along with Optimal Pixel Adjustment. Firstly they segmented an image in to 8x8 blocks using IWT. Optimal Pixel Adjustment had been applied after the message embedding in the transform coefficients had been completed. The proposed method enhanced the robustness of data hiding using frequency domain. IWT prevents the problems of floating point precision in the wavelet filters. The proposed method minimized the error difference of modified image as compared with the original image thus increasing the value of PSNR by providing a mapping function. It also improved the hiding capacity of image.

6. RESULTS

Table 1 provides a comparison of results obtained using various techniques for data hiding. The results are compared on the basis of PSNR. The greater the PSNR value the better will be the quality of embedded image. It is necessary that there should be minimum error difference in between the actual and embedded image order to maintain the quality of the image.

Table 1. Comparison of results of different Steganographic techniques

Techniques		PSNR (dB)
LSB Based [13]	Least Significant Bit Matching	61.1
	Least Significant Bit Replacement	62.2
Edge Based [13]	Pixel Value Difference	51.5
	Hiding Behind Corners	61.1
Edge Adaptive LSBM [13]		61.9
Multiple LSB Technique [11]	Pixel Value	49.84
	MSB Value	51.31
DWT Technique[8]		46.83
Texture Similarity [17]		47.9
Adaptive Steganographic based IWT Technique [20]		31.8

7. CONCLUSION

Steganography is the science of data hiding. In this paper a detailed study of image steganography is provided. Various image steganography techniques have also been discussed. The study concludes that many approaches have been available for embedding data in images. Least Significant Bit method is the most common technique but it is less robust as it can be destroyed by simple attacks. A more efficient method is Pixel Value Differencing Technique that allows data to be embedded in the LSBs of each pixel. This method helps to enhance the security level of data being embedded. The combination of encryption with steganography further enhances the security level. The edge Based methods called hiding behind corners and the LSB Replacement method provide greater PSNR value thus increasing the embedding capacity

8. REFERENCES

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

[2] Provos, N. & P. Honeyman, *"Hide and seek: An introductionto steganography",* IEEE Security Privacy, 1(3), pp.32-44, 2003.

[3] T Morkel, J.H.P Eloff, M.S Olivier, "*An Overview of Image Steganography",* Proceedings of the Fifth Annual Information Security South Africa Conference, 2005.

[4] Dr. Diwedi Samidha & Dipesh Agrawal, "*Random Image Steganography in Spatial Domain*", IEEE International Conference in Emerging Trends, VLSI, Embedded System, Nano Electronics and Telecommunication System, pp1-3, 2013.

[5] K.A. Darabkh, I.F. Jafar, R.T. Al-Zubi, & M. Hawa, "*An improved image least significant bit replacement method"*, IEEE 37th International Convention in Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp 1182-1186, 2014.

[6] Lalit Kumar Vashishtha Tanima Dutta Arijit Sur, "*Least significant bit matching steganalysis based on feature analysis*", IEEE National Conference in Communications (NCC), pp. 1-5, 2013.

[7] Monica Adriana Dagadita, Emil-Ioan Slusanschi, & Razvan Dobre, "*Data Hiding Using Steganography* ", IEEE 12th International Symposium in Parallel and Distributed Computing, pp. 159-166, 2013.

[8] G.Prabakaran & R.Bhavani, "*A modified secure digital image steganography based on Discrete Wavelet Transform*", IEEE International Conference In Computing, Electronics and Electrical Technologies (ICCEET), pp. 1096-1100, 2012.

[9] D.R. Denslin Brabin, Dr.V.Sadasivam, "*QET Based Steganography Technique for JPEG Images",* IEEE International Conference on Control, Automation, Communication and Energy Conservation, ISBN 978-1-4244-4789-3, 2009.

[10] Discrete Fourier Transform (DFT). Available at: http://in.mathworks.com/help/matlab/math/discrete-fourier-transform-dft.html

[11] 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.

[12] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, "*An Image Steganography Technique using X-Box Mapping*" IEEE International Conference On Advances in Engineering, Science and Management (ICAESM), pp. 709-713, 2012.

[13] Weiji Luo, Fangjun Huang & Jiwu Huang, "*Edge Adaptive Image Steganography Based on LSB Matching Revisited*" IEEE, Vol.5, No. 2, pp.201-208, 2010.

[14] Miao Maa, Jianhui Lianga, "*SAR image segmentation based on Artificial Bee Colony algorithm",* Applied Soft Computing 5205–5214, Elsevier, 2011.

[15] El-Sayed M. El-Alfy, "*Detecting pixel-value differencing steganography using Levenberg-Marquardt neural network"*, IEEE Symposium in Computational Intelligence and Data Mining (CIDM), pp. 160-165, 2013.

[16] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, "*Security improvisation in image steganography using DES*", IEEE 3rd International Conference in Advance Computing *(IACC),* pp. 1094-1099, 2013.

[17] Zahra Zahedi Kermani and Mansour Jamzad*, "A robust steganography algorithm based on texture similarity using gabor filter*", IEEE International Symposium on Signal Processing and Information Technology, pp. 578-582, 2005.

[18] Mohit Garg, "*A novel text steganography technique based on html documents"*, International Journal of Advanced Science and Technology, Vol *35*, pp 129-138, 2012.

[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] N. Vinothkumar, & T. Vigneswaran, "*Steganographic Method Image Security Based on Optimal Pixel Adjustment Process and Integer Wavelet Transform*", International Journal of Advanced Research in Electronics and Communication Engineering, Vol. 2, No. 3, pp-261, 2013