# A review on hiding of data using LSB technique

Atul Rana[1], Gaurav Dutt[2], Kamal Jindal[3], Sazid Malik[4]

[1,2,3,4]*Student, IMS Engineering College, Ghaziabad, Uttar Pradesh*

## ABSTRACT

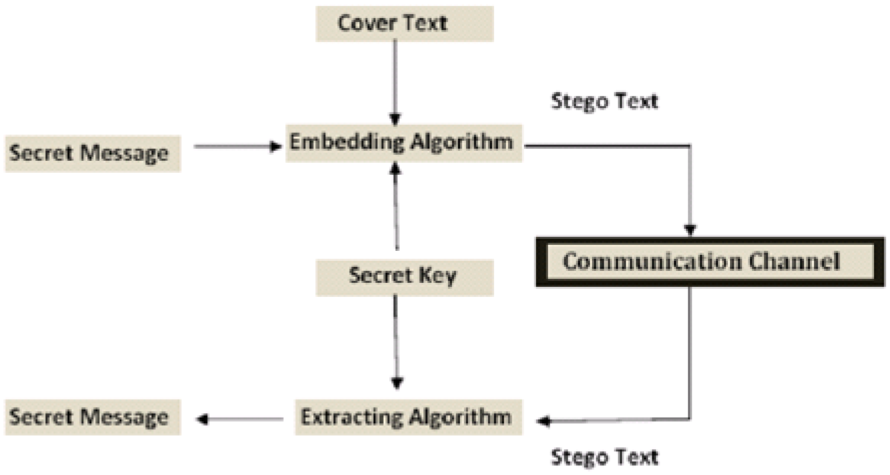
*The security is the main issue concerned with the sharing of data these days . For the secure transmission of the data from the sender's to the receiver's end , steganography is used .Steganography refers to the process of data hiding. The main role of steganography process is to hide the data behind images.Before the development of the steganography, Security of the data is the main concern of research for the researchers. Steganography use algorithms for hiding the data. 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 . In this technique the data hiding is done behind the cover image. The data is hidden character wise behind the pixels of the image. The number of techniques was developed in order to secure transmission. The various algorithms or techniques used for steganography are LSB-Hash, RSA Encryption and Decryption .*

**Keywords:** *Discrete Wavelet Transform (DWT) Steganography, Cryptography, Least Significant Bit (LSB), Discrete Cosine Transform (DCT).*

## 1. INTRODUCTION

The secured data can be copied for purpose of copyright violation, tampered with or illegally accessed without the knowledge of owner. So, for that there is a need of hiding secret identification inside different types of digital media so that owner can prove copyright ownership; identify the attempts to tamper with sensitive data and also to embed annotations. The main task of the field of steganography is the storing, hiding, and embedding of secret data in all types of digital media. The main goal of steganography is to communicate securely in a completely undetectable manner such that no one can suspect that their exist some secret information. In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. To share the information in a concealed manner two techniques could be used. These mechanisms are cryptography and steganography. Steganography makes data invisible by hiding (or embedding) them in another piece of data [2].Unlike cryptography, which secures data by transforming it into another unreadable format, Thus cryptography is science of changing secret writing while steganography as hiding secret writing.

In steganography the process of hiding information content inside any multimedia content like image , audio, video is referred as a "Embedding". To increase the confidentiality of communicating data both the techniques may be combined.Thus cryptography is science of overt secret writing while steganography as covert secret writing. The cover, host or the carrier is the target media in which information is hidden so that other person will not notice the presence of the information. The modified cover, including the hidden data, is referred to as a stego object which can be stored or transmitted as a message [3]. The secret information can be embedded in various types of covers. Ifinformation is embedded in a cover text (text file), the result is a stego-text object. Similarly, it is possible to have cover audio, video andimage for embedding whichresult in stego-audio, stego-video and stego- image respectively.Nowadays, the combinations of steganography and cryptography methods are used to ensure data confidentiality [4] and to improve information security.
*Cover medium + message + secret key = stego-medium*



**Overview of steganography**

## 2. LITERATURESURVEY

Most of the published articles are concerned with the description of some software tools designed and built to perform Steganography on some text, image, and audio cover media. The publication about the scheme of the stego system is more primitive, and mostly does not offer a key solution for some weak aspects which may face the discussed system. Among the large number of published articles, this section shows the current researches being done, in comparison with this research: LIU Tong and QIU Zheng-ding [18] and Vladimir Banociet al. proposed a DWT based color image steganography method. In the former method the secret information is hidden into a publicly accessed color image by a quantization-based strategy. Whereas, the latter case method processes grey scale images as cover object for creating subliminal channel and it utilizes transform coefficients of 2-Dimensional Discrete transform for embedding process. Johri and Asthana [14] proposed steganography and its implementation techniques. Deshpande Neeta,[20] et. al. proposed the Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. Ali AlAtaby, [12] proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. T. Narasimmalou[15] Proposed a new image data hiding technique based on discrete wavelet transform . The stegoimage is looking perfectly intact and has high peak signal to noise ratio value. Hence, an unintended observer will not be aware of the very existence of the secret-image. The extracted secret image is perceptually similar to the original secret image. In this paper two different techniques namely 1. using three level discrete wavelet transform and 2. using single level discrete wavelet transform for hiding images has been proposed and implemented.. The relative analysis between the proposed technique and the other existing techniques has shown the pre-eminence of the proposed technique. H.J .Patel and Dave [19] have proposed a new variant of LSB based image steganography. In this, both the parties will have to agree upon a set of carrier images and certain required parameters. Then the sender will select an image, from the set of carrier images which requires least number of bit manipulations on LSB substitution of secret data, and produce stegoimage. Then the receiver on receiving stegoimage will extract LSBs along with the help of the received parameters. The probability of guessing parameters is very less. So extraction without those parameters is very difficult. Here since both the parties agree upon a set of carrier images the visual difference between stegoimage and original image can be reduced. T. Narasimmalou[13], .Proposed an optimal discrete wavelet transform (DWT) based steganography. Experiments represent that the peak signal noise ratio (PSNR) generated by the proposed method is better. Ashok Kumar [17] proposed biometric steganography that uses skin region of images in DWT domain for embedding secret data. By embedding data in only specific region (here skin region) and not in whole image security is enhanced. Also image cropping concept introduced which maintains security at respectable level since no one can extract message without having value of cropped region. Featuresobtained from DWT coefficients are utilized for secret data embedding. This also increases the quality of stego because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive to. Swati and Mahajan [16] proposed a secure image steganographic model using RSA algorithm and LSB insertion. In this method, the secret data is first encrypted using recipient‟s RSA public key. Then each bit of the encrypted message is inserted to the LSBs of image in different images so as to find the best cover image. Best cover image is the one which requires minimum number of LSB extract the message in the encrypted form and will decrypt it using private key. Stuti Goel[21] proposed the performance and comparison of three techniques DCT,LSB &DWT is evaluated on the basis of the parameters MSE, PSNR, Capacity & Robustness. From the results, it is clearthat PSNR of DCT is high as compared to the other two techniques. This implies that DCT provides best quality of the image. DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security.

### Least Significant bit Technique Of Steganography

This is the most common and also a simple approach for embedding the data into an image. The (LSB) least significant bit (8th bit) of eachof the bytes inside an image is changed by the bit of the secret message. When we use 24-bit image, the three color bits components(R ,G ,B) are used which are red, green, blue, each byte store 3 bits in every pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of secret or embedded data. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When our data (the number 200), which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)

(11010010 10101100 01100011)

The number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On an average, only the half of bits in an image will be modified to hide a secret message using the maximum cover size. Since there are total 256 possible intensities of each primary color, and changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be detected by the human eye due to the negligible change. In these consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. And easy to detect, more secure system for the sender and receiver to share a secret key that specifies only some pixels to be changed In the simplest form, LSB makes use of BMP images, since they use lossless compression. It hides a secret message inside a BMP file, one would require a very large cover image. In BMP images of 800 × 600
Pixels are not generally used on the Internet and might arouse suspicion. For this reason, LSB steganography has also been developed for use with other image file formats [3]. It is a very simple method for embedding data in a cover image. This is the simplest algorithm in which information can be inserted into every bit of image information. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (least significant bit) of selected pixels of the image proposed a simple data hiding technique by simple LSB substitution. In this technique last bit of host data is randomly changed and produce the watermarked data at output. The cover LSB media data are used to hide the message

## 3. CONCLUSION ANDFUTURE SCOPE

### Conclusion

Steganography increases the security of data to be transmitted and also ensures that only authorized personnel can have access to that message . In this research work we did review on many papers on steganography techniques. These papers are good and have wide future scope .By reviewing these papers we observed that most of the steganography work is done in the year 2011 & 2014. In these years, LSB is the most widely used technique for steganography. Some researchers have also used the techniques likespatial technique, water marking, distortion technique, ISB, MSB in their work and provided a strong means of secure information transmission. Most of the papers that are discussed here are taken from IEEE Explore, AICCSA, IJET, IJCSE, IJCA etc. These papers provide a lot of help to the initiator for starting their work in this field. This review paper is enough for them to start their work in this field. The different security and data hiding techniques are used to implement steganography using LSB .The data can also be converted to other forms (such as Gray Code, Excess-3 Code ) , also it can be encrypted before using for hiding. In further research we are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data security.

### Future Scope

In this work it explores only a small part of the science of steganography. As a new displine, there is a great deal more research and development to do, The following section describe areas for research which were offshoots of, or tangential to,our main objectives. 1. Detecting Steganography in Image Files Can steganography be detected in images files? This is difficult question. It may be possible to detect a simple Steganographic technique by simple analyzing the low order bits of the image bytes. If the Steganographic algorithm is more complex, however, and spreads the embedded data over the image is random way or encrypts the data before embedding, it may be nearly impossible to detect. 2. How widespread is the Use of Steganography? If a technique or set of techniques could be devised to detect steganography, it would be interesting to conduct a survey of images available on the internet to determine if steganography is used, by whom and for what purposes. Steganographic applications are available on the Internet, but it is not known if they are being used. 3. Steganography on the World Wide Web The world wide web(www) makes extensive use of inline images.There are literally millions of images on various web pages worldwide. It may be possible to develop an application to serve as a web browser to retrieve data embedded in web page images.

## 4.REFERENCES

[1] Amin, Muhalim Mohamed, et al. "Information hiding using steganography." Telecommunication Technology ,2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE,2003

[2] Shashikala Channalli, Ajay Jadhav, "Steganography An Art Of Hiding Data" International Journal on Computer Science and Engineering Vol.1(3),2009,137-141.

[3] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An Overview of image steganography." ISSA. 2005.

[4] Yuk Ying Chung, fang Fei Xu,"Development of video watermarking for MPEG2 video " City university of Hong kong, IEEE 2006.

[5] Sohag,Saeed Ahmed ,Md Kabirul Islam , and Md Baharul Islam."A Novel Approach for Image Steganography Using Dynamic Substitution and Secret key "

[6] Bhattacharyya, Souvik, and Gautam Sanyal. "A Robust Image Steganography using DWT Difference Modulation (DWTDM)."International Journal of Computer Network & Information Security 4.7 (2012).

[7] Stuti Goel, Arun Rana , and Manpreet Kaur."A Review of Comparison Techniques of Image Steganography." Global Journal of Computer Science and Technology 13.4(2013).

[8] AL-Shatnawi, Atallah M.,and Bader M. AlFawwaz. "An Integrated Image Steganography System with Improved Image Quality." Applied Mathematical Sciences 7.71(2013):3545-3553.

[9] Bhattacharyya, Souvik, and Gautam Sanyal. "A Robust Image Steganography using DWT Difference Modulation (DWTDM)."International Journal of Computer Network & Information Security 4.7 (2012).

[10] Saddaf rubab and M Younus article: Improved Image Steganography Technique for Coloured Images using Wavelet Transform. International Journal of Computer Applications 39(14):29-32, February 2012. Published by Foundation of Computer Science, New York, USA.

[11] Banik Bamali Gupta and Samir K Bandvopadhvay " A DWT Method for Image Steganography "International Journal 3.6(2013)

[12] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform". The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010

[13] T. Narasimmalou, Allen Joseph .R " Discrete Wavelet Transform Based Steganography for Transmitting Images". IEEEInternational Conference On Advances In Engineering, Science And Management (lCAESM -2012) March 30, 31, 2012 370.

[14] J.R. Krenn, "Steganography and Steganalysis", January 2004

[15] T. Narasimmalou, Allen Joseph .R, "Optimized Discrete Wavelet Transform based Steganography" , IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),2012.

[16] S. Tiwari, R. P. Mahajan, and N. Shrivastava, "Steganography-an Approach for Data Hiding Based on Encryption and Lsb Insertion," IJECCE, vol. 3, pp. 76-83, 2012

[17] Ashok Kumar Balijepalli & L.Srinivas, NIET,Kantepudi. "steganography based secrete communication using dwt " International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012 ISSN: 2278-0181.

[18] T. Liu and Z. Qiu, "A DWT-Based Color Image Steganography Scheme," in Proc. IEEE, 6th International Conference on Signal Processing, 2002, vol. 2, pp. 1568-1571.

[19] H. J. Patel and P. K. Dave, "Least Significant Bits Based Steganography Technique," in Proc. IJECCE 2012, vol. 3, pp. 97- 103.

[20] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 2004.

[21] Stuti Goel,Arun Rana,Manpreet Kaur," A Review of Comparison Techniques of Image Steganography". IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48.