International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.3., 2016
(May-June)

REVIEW ARTICLE

ISSN: 2321-7758

DIGITAL IMAGE STEGANOGRAPHY TECHNIQUE BASED ON LSB- A REVIEW

DHARAMBIR SINGH[1], PARDEEP KUMAR[2], BHAWNA RAO[3]
[1,3]M.Tech Research Scholar , SITM Rewari, Haryana, India
[2]M.Tech Research Scholar, CGC Landran, Punjab, India

DHARAMBIR SINGH

PARDEEP KUMAR

BHAWNA RAO

ABSTRACT

The art of steganography is derived from ancient Greek technology of writing hidden secret messages. The role of steganography is to hide the existence of the message from unauthorized person. It is a method of unobservable communication by hiding data. The confidential information get embedded into the carrier and then transported over medium. It uses different type of carriers like audio, video, text, digital images and multimedia components for message embedding. Here our concern is about digital images as they are more frequent over the internet. In spy/hacker world Steganography and Cryptography are cousins. Cryptography alters a message so it cannot be understood whereas Steganography hides the message so that it cannot be read. There are lots of steganography techniques based on digital images like LSB (Least Significant Bit), in this techniques some bits of digital cover image get inverted when some input or alteration in image element i.e. pixel are found.

KEYWORDS- Steganography, Communication, Carrier, Digital Image, Cryptography, LSB, Pixel

1. INTRODUCTION

The word Steganography is a combination of two Greek words Steganos, which means secret and covered and graphy means drawing and writing. The goal of steganography is to hide data and messages inside other harmless messages in a way that does not allow any unauthorized person to even detect that there is a second secret message present [2]. The process of Steganography required a proper media to hide data inside it so that it can keep data undetectable from hackers/ attackers. The size of media which contains secret data plays vital role as one can easily detect it because of unusual size, as the size of media increases the possibility of its detection directly get increased. That's why steganography techniques are usually used for hiding data in fixed sized media [13].

Now a day, there are several steganography techniques used by technicians for data hiding such as [1]:

- Permutation Steganography.
- Least Significant Bit (LSB).
- Bit Plane Complexity Segmentation (BPCS).
- Chaos Based Spread Spectrum Image Steganography (CBSSIS).

The basic model of steganography consists of Message, Password and Carrier. Carrier is also known as cover object in which message get embedded.

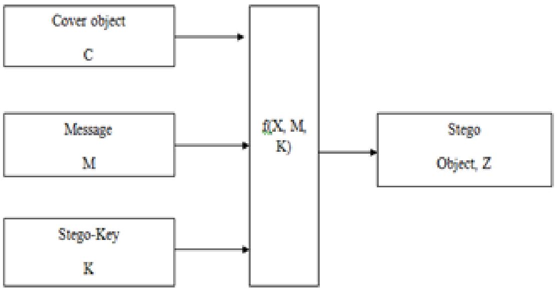


Figure 1 Basic Model of Steganography.

Message M, is the data which the sender wishes to remain in confidential form, it may be in simple text, cipher text, digital images or in any other multimedia form. The message can be anything that can the embedded in a stream of bit such as water mark and copy right mark or a serial number etc. Password is commonly known as stego-key K, is used to ensure that the only recipient to know the corresponding decoding key would be able to extract the message from the cover object C. The cover object in combination with message M is known as stego-object, Z. On the counter part, for recovering messages is from a Stego-Object Z requires the cover object C as well as the decoding key if a stego-key was used during the encoding process [15]. In some application there is no need of original image to extract the message there may be following cover object which can be used as suitable carriers:

- Networking Protocols such IP, UDP and TCP.
- Audio files in different formats like WAV, MIDI, MPI, AVI, VOC and MPEG.
- Disk such as FDD, Pen Drive and other Flash drives.
- Digital Image in both grey-scale and colour format such as bmp, .jpg and gif [3].

Steganography has void range of applications in different areas like [9]:

- Validation: The way of finding Uniqueness.
- Solitude: used to conform that the message has reached to required receiver.
- Integrity: it prevents message alteration.
- Non-repudiation: it certifies that the message is authentic.

1.1 APPLICATIONS OF STEGANOGRAPHY

There are lots of applications of Steganography in every field of hidden communication. At broad level we divide them in three major categories:

- Pay Load: Basically it denotes the capacity of information embedding. It plays vital role while embedding lots of information into a cover image such as embedding the personal data of any person with his finger print.
- Imperceptibility: It comes into existence when a secret communication occurs between two parties and the facts and data regarding the communication are kept secret like data exchanged at the time of online transaction or in credit cards.
- Robustness: finger printing , watermarking and all other copyright protected applications needs robust steganography methods so that information become reliable and integrated so that information can be retrieved easily without causing any serious damage to the cover image [7].

2. LITERATURE REVIEW

Majeed M. A. et al (2015) has proposed a technique to calculate highest value of PSNR (Peak Signal to Noise ratio) and compared it with previously calculated values which shows effective results of data hiding and maintains minimum changes in stego-image. The proposed technique has good quality of un-detectability and invisibility of hidden message. For securing message two levels of security has been added to LSB steganography. First level technique uses only two colours i.e. blue and green and avoids the red colour of RGB in steganography standard because red colour will result in noise data to any intended attacker. The second level of technique is the new bit inversion technique which reverses the bit of stego-image after applying LSB method [9].

Sadi G. A. et al (2015) has suggested LSB insertion method for hiding messages in stego-image with the help of JPEG image. JPEG image format shows higher ability to embed secret message inside an image without affecting the real appearance of the image. It requires the use of Discrete Cosine Transformer (DCT) to be applied on image for imager content transformation [6].

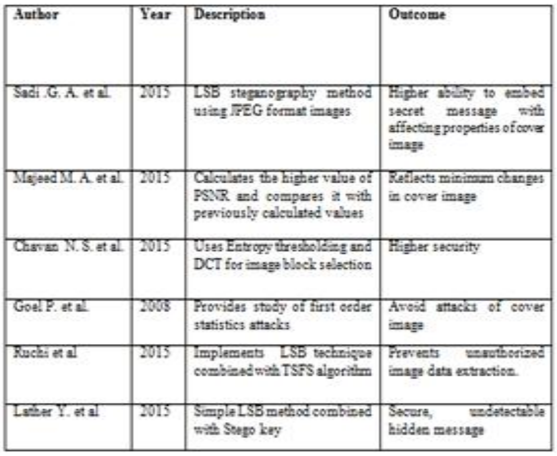
Ruchi et al. (2015) has proposed LSB steganography technique combined with TSFS (Transposition, substitution, folding and shifting) encryption technique. For preventing image data extraction, they have used two keys and encrypted the plain text with the help of TSFS Algorithm using key1 and the cipher text get embedded into the cover image using LSB technique plus key2. The proposed algorithm studies the behaviour of cover image while neglecting the message bit stream. This technique also has its application in "Active Warden Framework" Steganography [14].

Chavan N. S. et al. (2015) has suggested that the Entropy thresholding provides better quality of image and the system avoids the suspicious views of the attackers which results in higher security. Image adaptive selection of pixel blocks is more reliable than that of DCT (Discrete Cosine Transformer). The message decoder does not know about the exact location of the hidden message in the stego-image so they follow the same sequence and criteria as employed by the encoder. They also suggested that adding redundant bits in information bits provides error recovery of the hidden data at the receiver end and the quantization matrix helps in increasing the robustness and reducing the payload [10].

Lather Y. et al. (2015) has proposed a simple LSB steganography technique for providing a mean of secure communication. A stego key gets applied on the system while embedding the message into the cover image. They have embedded secret message bits into the cover image randomly instead of embedding them sequentially. Evaluation results show that a steganography technique with key provides higher security to that of non-key steganography technique because without the knowledge of the key, it is very difficult for the third party person to recover the embedded message [15].

Goel P. et al. (2008) presents study on first order statistic attacks on hidden messages in stego-images. Two algorithms are implemented which helps in preserving the first order statistics of a stego-image. Practical implementation result shows that preserving the image statistics using the proposed algorithm improves the security of the images against attacks. The second approach aims at resisting Blind Steganalytics Attacks especially Calibration based Blind attacks which try to estimate a model of the cover image from the stego image [12].

Table1. Brief description literature review



Author	Year	Description	Outcome
Sadi .G. A. et al	2015	LSB steganography method using JPEG format images	Higher ability to embed secret message with affecting properties of cover image
Majeed M. A. et al	2015	Calculates the higher value of PSNR and compares it with previously calculated values	Reflects minimum changes in cover image
Chavan N. S. et al	2015	Uses Entropy thresholding and DCT for image block selection	Higher security
Goel P. et al	2008	Provides study of first order statistics attacks	Avoid attacks of cover image
Ruchi et al	2015	Implements LSB technique combined with TSFS algorithm	Prevents unauthorized image data extraction.
Lather Y. et al	2015	Simple LSB method combined with Stego key	Secure, undetectable hidden message

3. LEAST SIGNIFICANT BIT TECHNIQUE

LSB steganography technique is the basic technique with simple implementations which is used to hide data in different type of digital medias like images, videos, audios and MIDI format etc. It basically operates on the pixel colours values by replacing the last significant bit (LSB) of any cover image by hidden message data. Least significant bit can be defined as the last bit at right hand side of any binary number. Changes at the last bit of any binary number reflect less effect on the original binary value of digital image [5]. LSB have its application of steganography in 8-bit and 24-bit images for hiding data, as these both type of images have their pros and cons.

- 8-bit Image: 8-bit images are small in size and have limited number of colours i.e. only 256. So that here each pixel can be represented by a single byte. Embedding data in RGB (Red, Green and Blue) type of images can easily be intercepted as changes in the images appear clearly. Whereas 8-bit Gray colour images are more frequently used for Steganography because they are less detectable.
- 24-bit Images: This type of images are more desirable for steganography purpose as they have large number of colours which results into hiding more data inside the cover image. Here 3 bytes are used to represent single pixel of the image, each byte of the pixel is corresponding to Red, Green and Blue colour. So that each pixel can have 256*256*256 values of different colours [4].

Algorithm for LSB Embedding:

```
Input: Cover_Image C
For  i=1 to Length (C), do
$Z_y$  <- $C_x$
For i=1 to Length (M), do
$Z_{yi}$ <- LSB ($C_{yi}$) $_=$ $M_i$
End for
Outcome: Stego image Z
```

Algorithm for LSB Extraction:

```
Input: Secret image Z
For i=1 to Length (M), do
$M_{yi}$ <- LSB ($C_{yi}$)
End for
```

In message extraction process, the fixed length message (M) can be extracted from the stego image (Z) by excluding cover image (C). The collection of hidden message takes place in the similar manner as in the embedding process. All the LSB collected and lined up for getting secret message [11].

4. CONCLUSION

Steganography is covering wide range of area of digital world by providing useful applications to all. It has its vital role in defence, terrorism and in other means of secret communications. We have discussed about various parameters related to steganography like its applicability on various types of mediums, its advantages and so on. LSB technique of steganography provides the basic services of steganography with higher quality result. In future LSB technique of steganography have wide scope. We suggest that in future if LSB together with Pseudo table get implemented then it will provide a more secure way to embed secret message into a cover image.

REFERENCES

[1]. A.K. Jain and U. Uludag, “Hiding Biometric data”, IEEE, 25:1494-1498, Nov. 2003.

[2]. Cachin, “An information-Theoretic Model for steganography”, in proceeding 2nd Information hiding Workshop, vol. 1525.

[3]. D.Artz, “Digital Steganography: hiding Data within Data”, IEEE Internet Computing, pp. 75-80, may-jun 2001.

[4]. Dagar, “highly randomized image steganography using secret key”, In Recent Advance and Innovations in Engineering (ICRAIE), 2014. IEEE.

[5]. Das P. and Kushwaha, “Multiple Embedded Secret Key Image Steganography using LSB Substitution and Arnold Transform”, 2015, (ICECS):845-9.

[6]. G. A. Sadi, “Image Steganography Approach”, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 8, August 2015, Pg. 166-169.

[7]. K. Solanki, N. Jacoben, U. Madhow, B. S. Manjunath and S. Kumar, “ Robust Image-Adaptive Data Hiding using Erasure and Error Correction”, IEEE Trans. Image Processing, Vol. 13, p. 1627-1639, Dec. 2004.

[8]. M. A. Majeed and R. Sulaiman, “An Improved LSB Image Steganography Technique using Bit- Inverse in 24- bit Colour Image”, Journal of Theoretical and Applied Information Technology, Vol. 08, Oct. 2015.

[9]. N. F. Johnson and S. Jajodia, “Steganography: Seeing the Unseen”, IEEE, 1998.

[10]. N. S. Chavan, “Research Article Image Steganography – An Overview”, International Journal of Recent Scientific

Research, Vol. 6, Issue 6, pp. 4800-4804, June 2015.

[11]. N. F. Johnson, S.C. Katzenbeisser, "A Survey of Steganography technique".

[12]. P. Goel, "Data Hiding in Digital Images: A Steganography Paradigm", 2008.

[13]. N. Provos, P. Honeyman, "Hide and Seek: An introduction to Steganography", IEEE Secur Priv, 2003, 1(3): 32-44.

[14]. Ruchi and V. Goyal, "Image Steganography Combined with TSFS using LSB", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 8, August 2015.

[15]. Y. Lather, M. Goyal and V. Lather, "Review Paper on Steganography Techniques", International Journal of Computer Science and Information Technology, Vol. 4, Issue 1, Jan 2015.

A BRIEF BIO OF AUTHORS

Mr. Singh pursuing his M.tech in Computer science And Engineering From SITM Rewari, he has his bachelor of technology from Dronacharya College Of Engineering Gurgaon, Haryana, India in Computer Science And Engineering. Currently he is pursuing Research in Steganography.

Mr. Pardeep Kumar pursuing his M.Tech from CGC Landran Mohali Punjab, India. In Computer Science and Engineering. His research area is Wireless Sensor Networks and Steganography. He has published a number of research papers in reputed International Journals.

Ms. BHAWNA RAO currently pursuing her M.Tech from SITM Rewari, Haryana, India. She has his bechelor of technology from Vaish college of engnieering, Rohtak, Haryana, India in Computer Scienec And Engineering currently she is pursuing Research in Sentiment Analysis.