Scientific Journal of Impact Factor (SJIF) : 3.134

ISSN (Print) : 2348-6406
ISSN (Online): 2348-4470

International Journal of Advance Engineering and Research Development

# IMAGE BASED STEGANOGRAPHY
## REVIEW OF LSB AND HASH-LSB TECHNIQUES

Vikshit Rabara[1], Vatsal Shah[2]

[1]*Information Technology, BVM engineering College,vikshit_rabara@yahoo.in*
[2]*Information TechnologyBVM engineering College, vatsal.shah@bvmengineering.ac.in*

***Abstract*** *- Steganography means study of invisible communication that usually deals with the ways of finding the existence of communicated message. It has many applications in computer science and other related fields. Different steganography techniques are used to protect the information accessed by unauthorized person. Some methods of steganography are image, video, text and audio respectively. Image based steganography techniques are most useful techniques nowadays. In this paper I reviewed how the images can be used as the covering medium for text messages.*

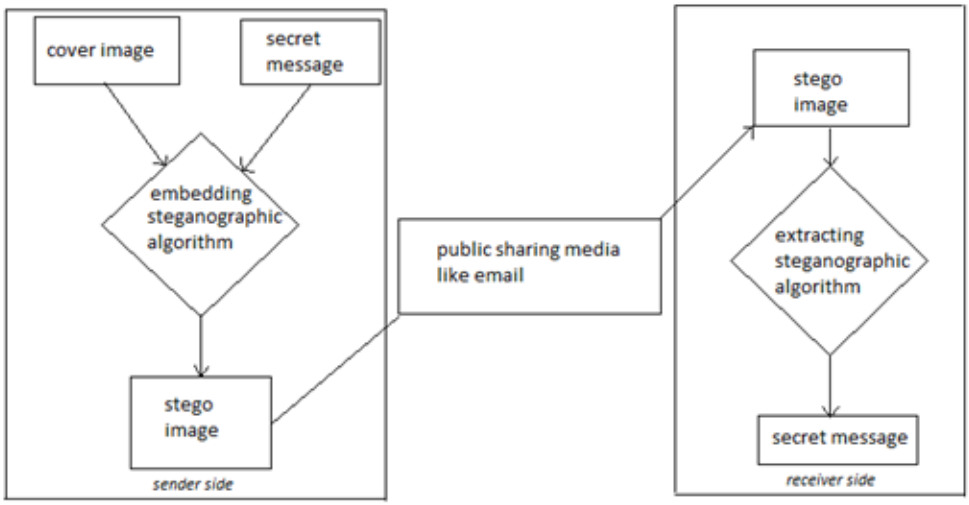
***Keywords:*** *Steganography, stego, LSB, Steganalysis.*

### I. INTRODUCTION

Security has become a critical feature for thriving networks and in military alike. In the present world of communication, one of the necessary requirements to prevent data theft is securing the information. There are many techniques to prevent data theft, 'STEGANOGRAPHY' is one of them. Text steganography, image steganography, video steganography are some steganographic techniques. The majority of today's steganographic systems uses images as cover media because people often transmit digital pictures over email and other Internet communication. This paper's focus is on a field of information technology known as image steganography. This paper will take a review of this technology by introducing the various concepts of image based steganography.

### II. IMAGE BASED STEGANOGRAPHY

In image based steganography, we use image as the cover of secret message. Following fig. 1 shows the sender side and receiver side flow chart for image steganography. At sender side first we take an image and hide our secret message using embedding steganographic algorithm, now we get 'stego image'. This stego image is then sent to thereceiver and receiverget the secret message by using extracting stenographic algorithm, called steganalysis [8].




*figer 1. Image steganography[1]*

### III. IMAGE BASED STEGANOGRAPHIC TECHNIQUES

a) Spatial domain method:

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data [1]. Some of the spatial domain techniques are as follow:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labelling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

b) Transform Domain Technique:
This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it [2]. Some transform domain techniques are:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

c) Distortion Techniques:
Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion [2].

d) Masking and Filtering:
These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image.

**Least Significant Bit Embedding**

Least significant bit embedding is define as the mapping secret message to pixel's steganography is the most classic steganographic techniques, which embeds secret message in a subset of the LSB plane of the image [4]. A large number of popular steganographic tools, such as S-Tools 4, Steganos and StegoDos, are based on LSB replacement in the spatial domain. LSB steganography can be describe as follows: if the LSB of the pixel value I(i, j) is equal to the message bit m to be embedded, I(I, j) remain unchanged; if not, set the LSB of I(i, j) to m. the message embedding procedure can be described using an Equation as follow;

$$Is(i,j) = \begin{cases} I(i,j) - 1 & LSB(I(i,j)) = 1 \text{ and } m = 0 \\ I(i,j) & LSB(I(i,j)) = m \\ I(i,j) + 1 & LSB(I(i,j)) \neq 0 \text{ and } m = 1 \end{cases}$$

In general, a p-by-q image is simply a p-by-q matrix, where each entry in the matrix is a positive integer called the pixel value, which determine the color of the pixel. For an n-bit image, these pixel values range from 0 to 2n – 1. In other words, the possible color values for each pixel in an n-bit image are the colors corresponding to the bit string of length n. unless there is a specific need to use the bit strings representations of pixel values, we will typically use the decimal representations.8 bit grayscale images are thus p-by-q matrices of integers ranging from 0 to 255, where 0 corresponds to black, 255 to white, and the values in between from a spectrum of varying shades of gray. The LSB is the bi correspondingto 20, that is, the bit that makes a value even or odd. Since these grayscale values varies little from the values on either side
of it [4].

```
If pixel value = odd
        Then increment by 1
        Else if the pixel value = 255
                then decrement by 1
If pixel value = odd
        if bit = 0
                then add 1
        else if pixel value = 255
        if bit value = 0
                then decrement by 1
        else if pixel value = even
        if bit = 1
                then increment by 1
```

Select the pixels of image using the key. Increment the grey level value of the pixel by 1 if the pixel value is odd and if the value is 255 subtract it by 1. Convert the data into bit stream and compare this bit stream with the pixel values. Increment pixel values by one if bit is 0 and pixel values is odd, and increase by one if bit is 1 and pixel value is even. Decrement pixel value by 1 if bit is 0 and pixel value is 255[3].

**Least Significant Bit Extracting**

Extracting is defined as the mapping pixels to image. In the image steganography the extracting process can be done on message which is the stego image. The recipient inputs the stego image, and when applicable, the steganographic key, into an extraction algorithm, which outputs the secret message [5]. This extraction algorithm is considered the inverse of the embedding algorithm, although the embedding and extraction algorithms may be created such that the extraction algorithm is not actually the mathematical inverse of the embedding algorithm. For steganalysis of LSB steganography some steps are as follow [5]:

```
1) stego image and key and the massage
   which is converted in the form of ASCII form. The hided
   massage is stored in Low level least significant bit.
2) search where message is being stored, for that
   set the threshold value which depends upon the cover
   image.
3) check the stego image is even or odd then set the
   message bit either 0 or 1.
4) Inverse of embedding process
        If pixel value = odd
                Then the bit value is 1
        Else if pixel value = even
                Then the bit value is 0
```

**Problem with Conventional LSB**

In traditional LSB technique we use gray scale images which is less useful in compare to RGB scale images, because gray scale images provides only 0-255 shades while RGB images provide a huge range(16 million) of colors to hide the information. To overcome these problem Hash-LSB technique is developed.

**Hash-LSB (Least Significant Bit) Process**

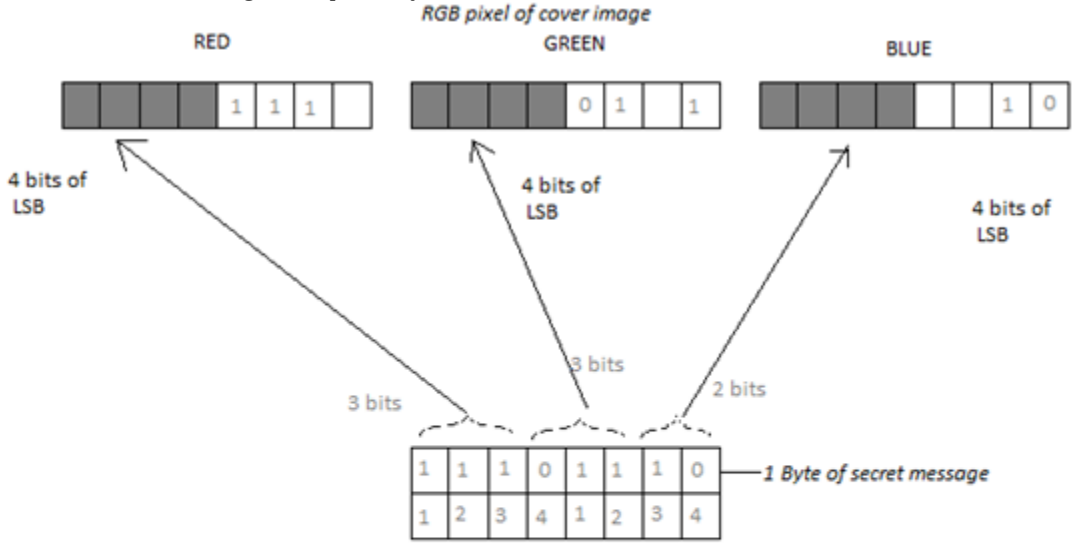
The Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the secret data is determined using hash function. Hash function finds the positions of least significant bit of each RGB pixel's and then message bits are embedded into these RGB pixel's independently. Then hash function returns hash values according to the least significant bits present in RGB pixel values. The cover image will be broken down or fragmented into RGB format. Then the Hash LSB technique will uses the values given by hash function to embed or

conceal the data. In this technique the secret message is converted into binary form as binary bits; each 8 bits at a time are embedded in least significant bits of RGB pixel values of cover image in the order of 3, 3, and 2 respectively [6]. According to this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB as illustrated in Fig. 2. These 8 bits are inserted in this order because the chromaticinfluence of blue color to the human eye is more than red and green colors [6]. Therefore the distribution pattern chooses the2 bits to be hidden in blue pixel. Thus the quality of the image will be not sacrificed. Following formula is used to detect positions to hide data in LSB of each RGB pixels of the cover image [6].

$$k = p \% n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Where, k is the LSB bit position within the pixel; p represents the position of each hidden image pixel and n is the number of bits of LSB which is 4 for the present case. After embedding the data in cover image, a stego image will be produced. The recipient of this image has to use the hash function again to extract the positions where the data has been stored. The extracted information will be in cipher text. After decryption of it, combining of bits into information will produce the secret message as required by the receiver.




*figer2. Hash process to find LSB of RGB pixel value*

This approach of image steganography is using RSA encryption technique to encrypt the secret data. Encryption includes a message or a file encryption for converting it into the cipher text. Encryption process will use recipient public key to encrypt secret data. It provides security by converting secret data into a cipher text, which will be difficult for any intruder to decrypt it without the recipient private key [7].

**Embedding Algorithm at Sender Side**:

Step 1: Choose the cover image & secret message.

Step 2: Encrypt the message using RSA algorithm.

Step 3: Find 4 least significant bits of each RGB pixels from cover image.

Step 4: Apply a hash function on LSB of cover image to get the position.

Step 5: Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function given in equation 1

Step 6: Send stego image to receiver.

**Hash-LSB Decoding and RSA Decryption**

In the decoding process we have again used the hash function to detect the positions of the LSB's where the data bits had been embedded. When the position of the bits had been specified, the bits are then extracted from the position in the same order as they were embedded. At the end of this process we will get the message in binary form which again converted into decimal form, and with same process we got the cipher text message. After retrieving the positions of LSB's that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use

his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable form [7].

Step 1: Receive a stego image.
Step 2: Find 4 LSB bits of each RGB pixels from stego image.
Step 3: Apply hash function to get the position of LSB's with hidden data.
Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.
Step 5: Apply RSA algorithm to decrypt the retrieved data.
Step 6: Finally read the secret message.

## IV. CONCLUSION

It is seen that from this paper work there are two techniques named LSB and Hash-LSB technique, I reviewed about, their advantages and disadvantages. The LSB insertion was used to embed the message in to the cover image. The selection of pixel to embed was crucial, since the LSB insertion modifies the pixels. Modified pixels in areas of the image where there are pixels that are most like their neighbors were much more noticeable to the normal eye. To solve this problem Hash-LSB technique is used, because it uses RGB color scheme. RGB color scheme has 16 million different shades, so Hash-LSB technique is more preferable than LSB.

## REFERENCES

[1] N. F. Johnson and S. Katzenbeisser, "A Survey of steganographic techniques. In Information Hiding Techniques for Steganography and Digital Watermarking, S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, (2000), pp. 43-78.

[2] H. S. Majunatha Reddy and K. B. Raja, (2009) High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security. pp. 462-472.

[3] R. Alwan, F. Kadhim, A. Al-Taani, "Data Embedding based on better use of bits in image pixels" International Journal of Signal processing, 2005.

[4] MamtaJuneja, Parvinder Singh Sadhu "Performance evalution of edge detection technique for image and spatial domain", International journal of computer theory and Engineering, 2009.

[5] Ching-Nung Yang, Tse-Shih Chan, Kun Hsuan, "Improvements of image sharing with steganography and authentication", the Journal of system and software 2004.

[6] KousikDasgupta, J. K. Mandal, Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.

[7] Mohammad A. Ahmad, Dr. ImadAlshaikhli, Sondos O. Alhussainan, "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No. 127-139, Sept., 2012.

[8] Westfeld, A., "F5-a steganographic algorithm: High capacity despite better steganalysis." in Proc. 4th Int'l Workshop Information Hiding, pages 289–302, (2001).