Image Partition Method for Hiding Secret Messages Steganography Technique using LSB

V.Raja[1], Dr. G.Kalpana[2]
Assistant professor, S.R.M Institute of Science and Technology, Chennai, India.
Assistant professor, S.R.M Institute of Science and Technology, Chennai, India.

Abstract: Steganography or stego means 'covered writing'. Steganography is the science of hiding information. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem. The goal of Steganography is to hide messages in digital images, audios, videos and text. It does not allow any enemy to even detect that there is a second message present. This paper proposes a new Block based method for encoding the secret messages in digital images using Least Significant Bit(LSB) encoding technique. And also the paper illustrates the efficacy of the secret key generation for encoding and hiding the message in digital images.

Keywords: Steganography, Cryptography, LSB, Secret Key

I. INTRODUCTION

As a result of increasing the usage of network to sending and receiving the secret data is more reliable than ever over the internet[1]. Hacking the data is a great problem in internet. To help the sender and receiver to send their information in a highly secured way with the help of Steganography methods. Steganography is a most vital technology to conceal and secure the data in an efficient way. In recent years, Steganography has become an interesting research area to enhance the security of network communication [2], online data sharing and copyright protection. Commonly, Steganography is used to generate an algorithm for hiding data, the existence of a secret messages into cover media such as audio ,video, image and text. In this paper, we prosed the cover media is an image which is called cover image also the image with secret data embedded within is named as embedded image or Stego Image.

Data-hiding techniques can be performed in three domains: namely frequency domain, vector quantization (VQ)-based domain and spatial domain. In the frequency domain of data-hiding techniques, discrete cosine transform is applied to transform [3] the pixels in the spatial domain to the Frequency domain ant the secret data are embedded into Transformed coefficients of cover images. The methods that are used in the frequency domain are secure against more attacks. In VQ-based data-hiding approach, an image is compressed by using VQ technique and the secret data are concealed in the VQ indices. VQ-based data-hiding techniques is suitable for low bandwidth transmission

Channels because of serious reduction in the amount of transmitted data. In the spatial domain, the secret data are directly embedded into two pixels of cover images [11]. The methods introduced in the spatial domain have low time complexity and low robustness against some attacks. These methods are popular because of their simplicity and low time complexity. In this paper, we proposed an adaptive data-hiding approach in the spatial domain. Therefore we mostly review the spatial domain methods, in detail [8]. The spatial domain methods can be categorized into three Types: 1) high embedding capacity approaches with acceptable image quality, 2) high image quality approaches with reasonable hiding capacity and 3) restricted embedding capacity approaches with a slight distortion in the quality of image [10].

In the first type of spatial domain approaches a well-known Steganography method is a least-significant-bit (LSB) Substitution which is vastly applied in the literatures In this method, the secret data bits are embedded Into k LBSs of the cover-image pixels. In the last decade [7],[9], Many approaches have been proposed to improve the Quality of Stego-images obtained by the LSB substitution approach, while keeping acceptable the visual quality. So more than the other data-hiding techniques [12]. The second type of spatial domain approaches is the Adaptive Steganography methods where the embedding Capacity of a pixel is determined based on differences between the neighbor pixels values in the cover image. According to human vision properties, eyes can tolerate more changes in the edge areas than in the Smooth areas [4]. Therefore more secret data can be embedded in the edge areas than the smooth areas. Several articles utilized this concept to obtain the Stego-Image with higher quality and larger embedding capacity Where of them are explained in the next section.

The third type of spatial domain approaches in the restricted Embedding capacity approach with a slight distortion in the Quality of image. In 2001, sharp proposed the LSB matching approach to upgrade the visual quality of the Stego-image by randomly adding or subtracting 1 from the pixels value of the cover image when the secret bit does not match with the LSB of corresponding pixels[5].

The method causes a very small distortion in the Stego-image quality, while the embedding capacity is only I bit per pixel (bpp). In 2006, meilikainen introduced LSB matching revisited method both improve the LSB matching approach that can less modify the cover image while holding the same embedding capacity[6]. In recent years, many papers developed the LSB matching approach.

II. PROPOSED METHOD

The main goal of the proposed method is to embed the secret message into LSB of each red, green and blue value of the pixels in the block of size 2×2 of the color image. We can use n maximum number of bits that can be embedded into a block of size 2×2. The proposed work contains four

Phases as describes as

I. Division Phases
II. Stego Key generation phase
III. Embedding Phase
IV. Extraction Phase.

Division Phase:

We choose a color image of any size which could be divided into 2×2 blocks. In the first block of the chosen image, we hide the length of the secret message in the LSB of first pixel in the first block. The process of embedding the secret message will be started from the second block of the image, next it goes to third and fourth block of the image.

Block-I Stego-Key	Block-II R LSB of Red value
Block-III G LSB of Green value	Block-IV B LSB of Blue Value

Stego Key Generation Phase:

We divide the bits into image into four blocks as B1, B2, B3 and B4. The proposed method is hiding the secret bits pos and pos+2 of from the second block onwards by using the following procedure. The original message is transformed to binary value based on the indexed table.

Number of required bit is 6 to store the single character of the original message.

Read the input secret data.

Do:

Read the first pixel value from the B2, B3, and B4 and retrieve the pixel value of red color. Green color and Blue color.

Pixel value = Red + Green +Blue

Hide First bit of the secret data into the least significant bit of the Red value in the Block2.

Hide Second bit of the secret data into the least significant bit of the Green value in the Block3.

Hide third bit of the secret data into the Least Significant Bit of Blue value in Block4.

Repeat the above step until length of secret data

Extraction Phase:

The embedded image is divided into 2x2 blocks. Each block contains the amount of pixels according to their image size. Select the first block of the image to read the Stego key to find out the length of the original message. The next three consecutive block can be taken to extract the secret data. And the following procedure used to extract the secret data completely from the Stego image.

```
Step1: Extract the secret bits from the LSB of pixel        Read
Block1 to extract the Stego key.
For rp = 1: End of stego key.
For Block = 2:4
        Switch (Block)
        Case1:
                PB =Block( PB + value of Rp(LSB (Red
                pixel)))
        Break;
        Case2:
                PB =Block( PB + value of Rp(LSB (Green
                pixel)))
        Break;
        Case3:
                PB =Block( PB + value of Rp(LSB (Blue
                pixel)))
        Break;
Next
Next
Step 2: Concatenate all the secrete data to obtain the original bit
stream of the secret data.
Step 3: End.
```

Finally the secret data bits will be extracted exactly without any alteration.

Example for the proposed method:

Original message: ABCD

Binary : 111010 011011 010100 111101

Number of Bits required to store each letter of the original message: c = 6

Length of original message: No. of. Input character = 4 X 6 = 24 bits

Therefore, the stego key = 0010 0100

Fig 1 : Block Representation of the proposed Image

Let us take the first pixel value and extract the red value from first pixel from Block II in the image.

Red value of first pixel = 001001

Plain Bit = 0

After Embed Red value = 00100**0**

Extract Green value of first pixel from BlockIII.

That is 111100

Plain Bit = 1

After Embed Green value = 11110**1**

Extract Blue vale of first pixel from BlockIV 11011101

Plain Bit = 1

After Embed Blue value = 1101110**1**

III. CONCLUSION

We have presented the better way of hiding information in an image. Steganography methods could take on a very new meaning of hiding information in a secured way. Anyone could simply hide the messages and send through the internet out of any kind of threats.

IV. FUTURE ENHANCEMENT

We could enhance the proposed method to store the user information in the RGB cubic arrays diagonal elements. We do improve the efficiency and capacity of the users' data to hide in an image. In this proposed method we developed an encryption algorithm to encrypt the user data and hide in an image and it provides high security.

V. REFERENCES

[1] Ali Bani, "A new Steganography approach image encryption exchange by using the least significant bit insertion.", IJCSN June 2008, Vol 8.

[2] Andrew, "Steganalysis of embedding in two Least significant bits", IEEE transaction on information forensics and security, vol 2 Mar –07.

[3] WaiChi, "Techniques and application of intelligent multimedia data hiding Springer,Jan 2010 .

[4] T.S.Das, "Multimedia data hiding in spatial and transformed domion", Springer, Mar 2007.

[5] L.F. Turner, "Digital data security system", Patent IPN WO 89/08915, 1989.

[6] R.Z. Wang, C.F. Lin and J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern recognition 34 (3) (2001) 671–683

[7] Lee, I.S.[IShi], Tsai, W.H.[WenHsiang], "Data Hiding in Binary Images with DistortionMinimizing Capabilities by Optimal Block Pattern Coding and Dynamic Programming Techniques", IEICE (E90D), No. 8, August 2007, pp. 11421150.

[8] Ingemax cox, matthewmiller and tonkalker "Digital watermarking and Steganography",Morgan Kanfman series in multimedia information system ,USA ,2008.

[9] Stefan katzen beisser and fabien a.p petitcoals "Information hiding techniques for Steganography and digital Watermarking" Artech house books , dec 1999.

[10] Frank y.Shih "digital Watermarking and steganography fundamentals and techniques" CRC Press ,dec 2007.

[11] Greory Kipper , “investigator’s guide to steganography”auerbach publication , 2004
[12] peter wayner disappearing cryptography Morgan Kanfman series in multimedia information system ,USA ,2009.