Optimal Implementation of Digital Steganography in an Image for the Secret Communication

Mr. Ranjit V.Bobate
M.Tech , IV Semester , Electronics Engg
Yashwantrao Chavan College of Engineering, Nagpur,
Maharashtra ,India
e-mail:ranjit.vb@gmail.com

Prof. A.S.Khobragade
Astt. Professor, Electronics and Telecomm. Engg
Yashwantrao Chavan College of Engineering, Nagpur
Maharashtra ,India
e-mail:atish_khobragade@rediffmail.com

***Abstract*—A real-life requirement motivated this case study of secure covert communication. Steganography is a technique used to transfer hidden information in an imperceptible manner. We proposed a novel approach of substitution technique of image steganography. The proposed method is completely flexible on size of secret message bits and allows us to embed a large amount of secret messages as well as maintaining good visual quality of stego-image. Using this method, message bits are embedded into uncertain and higher LSB layers, resulting in increased imperceptible and robustness of stego-image.**

Keywords-Data Hiding; Image Steganography; Substitution Techniques

I Introduction

Popularity of the Internet provides a great opportunity to transfer large amounts of data in networks. However, it also increases the risk of illegal and unauthorized access to deal with the content, while the data is transferred. Mechanisms should be prepared to provide protection against attacks and make a secure transfer. In the last ten years, several methods have been proposed by researchers to develop an environment for transferring important information.

Steganography is a way for secret communication by using digital media to convey essential messages. The word “Steganography” derives from Greek and it means "cover writing". Steganography is all about creating a form of secret communication between two parties and it is a complement of cryptography that whose goal is to conceal the content of a message. Steganography uses a media like an image, video, audio or text file to hide some information inside it in such a way that it does not attract any attention and looks like an innocent medium[1] .

There are lots of algorithms used in image Steganography area. However, they have their own weaknesses and strengths. Since Least Significant Bit (LSB) insertion method is one of the simplest data hiding techniques. In this study most of the effort is done to get a better imperceptibility and decreasing image’s distortion and increasing capacity without losing stego-image quality. The rest of this paper is organized as follows. In First section Introduction of Image Steganography ,In Second Section the Introduction to related work of the LSB method, Optimal pixel adjustment method, InThird sectionnew proposed method for images which is called “Optimal EmbeddingMethod ”. The Fourth section gives the experimental results and discussions. Finally, the conclusion and references are given

II. RELATED WORK

A. The Simple LSB Substitution

The word LSB stands for Least Significant Bit. This method is one of the most simple and easy to implement methods in Steganography area. This method actually substitutes the LSBs of cover image with secret bits sequentially. In order to hide messages by this approach at least one bit is stored in each pixel of cover image. For example by using 8-bit gray scale image format with the size of 512 * 512can embed 262144 bits (32768 bytes or pixels). By embedding this amount of data both stego-image and its respective cover image look the same since human eye cannot distinguish this little changed value of pixels, but embedding more than one bit in each pixel by using the edge area pixels will make more change in high frequency areas so it can be still undetectable by human eye as well [2,3]. By considering the size of cover image pixels there is no limitation on embedding rate in this method, but the more secret bits we can embed, the less imperceptibility of stegoimage is obtained which is shown in Fig1bit by bit embedding [ ]. So researchers proposed several methods to improve the weakness of this method.

B. The Optimal LSB method

The simple LSB method can be modified so the quality of stego-image gets improved. The algorithms of such improved schemes are still based on simple LSB method. In this section we introduce one of the improved methods, called Optimal LSB which applies Optimal Pixel Adjustment Process (OPA) to improve the stego-image quality. Three candidates are picked out for the pixel’s value and compared to see which one has the closest value to the original pixelvalue withthe secret data embedded in. The best candidate is then called the optimal pixel and used to conceal the secret data

The embedding process is described as follows

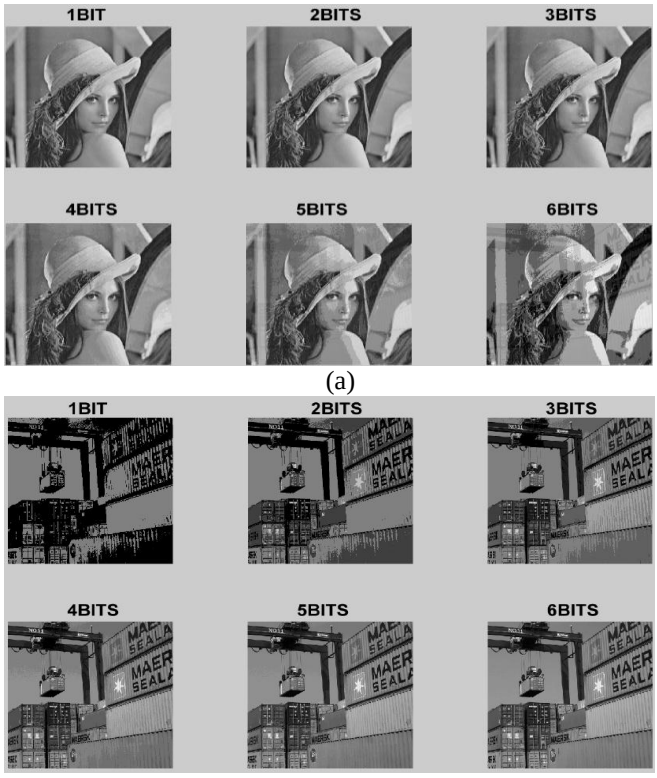

Fig 1:Satus of Image after Bit by bit embedding a:Cover Image b: Secret Image

1) Let Pi be the original pixel value and k bit(s) of secret data is to be embedded.
2) Embed k bit(s) of secret data into Pi' by using the LSBs method. The stego-image Pi' can then be obtained
3) Generate another two pixel values by adjusting the (K +1) th bit of Pi'. Therefore, P+' and P-' can be calculated as follows obviously, the hidden data in P-' and P+' are identical to Pi' because the

$$(p'_+, p'_-) = \begin{cases} p'_+ = p'_i + 2^k \\ p'_- = p'_i - 2^k \end{cases}$$

last k bits of them are the same.

4) The best approximation to the original pixel value, Pi', (i.e. the optimal candidate) is found by the following formula:

$$p''_i = \begin{cases} p'_i, & if\,|p_i - p'_i| \le |p_i - p'_-| \le |p_i - p'_+| \\ p'_+, & if\,|p_i - p'_+| \le |p_i - p'_i| \le |p_i - p'_-| \\ p'_-, & if\,|p_i - p'_-| \le |p_i - p'_i| \le |p_i - p'_+| \end{cases}$$

Finally, all the optimal candidates for Pi' replace the original pixel values Pi and the embedding algorithm come to its end.

III. THE PROPOSED METHOD

Many algorithms are proposed by researchers to solve the problems of simple LSB and increase the imperceptibility of stego-image But the proposed method (Optimal Embedding) has a higher imperceptibility of the stego-image by using more characteristics of cover image. The proposed approach searches a pixel to find a match between original pixel bits and secret bits. In conventional LSB method, the hidden information were embedded sequentially and started to embed from first LSB of each pixel.

On the other hand, in our method depending on pixel value if there is a match between secret bits and original cover pixel's bits, there is no need to embed and we just have to identify the starting bits of found match. The bits where the secret bits are embedded will be combined together to form a stream of bits. This stream of bits is used as a stego-key that needs to be communicated to the receiver for extracting the secret message. Experiment shows that the method produces no image distortion and the imperceptibility increases significantly.

For embedding process, first we have to know the embedding rate (number of bits we embed per pixel). Since the 8-bit colour image is selected as cover image, the embedding rate is simply obtained by dividing number of secret bits to number of pixels. For example, we have 1048576 secret bits and size of cover image is 512 X 512 So by dividing 1048576 to 262144 the embedding rate would be four which means four bits should be embedded in each pixel of cover image. Using sample pixels of cover image and sample secret bits is useful to explain the process of embedding in detail .

1010,0101,1110,0100

Secret bits (1*2)

01101001	11001110
01010100	10101000

Cover image (2*2)

Fig . 2 : Image bits of Secret and Cover Image

In Fig 2 ,The embedding process starts from the leftmost pixel of the first row and moving to the right of the same row before continuing to the subsequent rows of the image. The first secret bits to embed are "1010" and the cover pixel value is"01101001". We can notice that the four bits after third LSB are the same as the secret bits. Therefore no embedment is required in this case. Hence, we do not cause any image distortion because we did not change any of original bits. We need to identify that the four bits of this pixel are secret bits and inform the receiver for extraction process. To embed the next secret bits ("0101") in respective cover pixel, again we need to search for a match in the corresponding pixel. Since there is no match between secret

bits and cover bits, we used the four LSBs of cover pixel to embed the secret bits by using OPA algorithm. The stego-key is generated by determining the first bit position where the leftmost bit of secret bits is embedded . as shown in fig 3 the stego key for the sample secret bit is “10000001”.

The receiver extracts the secret bits by using the stego -key and the stego-image. According to Fig. 3, first bits of stego-image’s pixel are “01101001” and the first two bits of

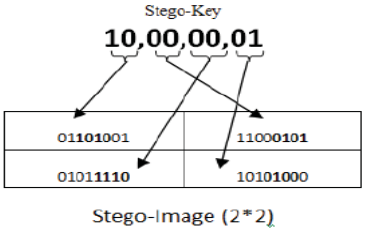

Fig 3: Generation of Stego-key

stego-key are”10” . It means that our secret bits are the four bits after second LSB of stego-pixel. So for extracting the secret data we take four bits of the modified pixel, starting from third LSB which are”1010”. The second two bits of stego-key are”00” and this means extract the bits from the second pixel by starting first LSB which are”0101”. Then repeat the extracting process for the rest of the pixels. Rest of extracting process will be done like this.[3,4,5]

IV. EXPERIMENTAL RESULTS

Methods that provide high embedding capacity were described in section I and II. These methods are Simple LSB, Optimal LSB. This section presents the comparison of these methods and the proposed method. The images used as cover and secret images are 8 bit images. The standard image Lena with the size of 512 X 512 which is shown in Fig.4 is used as cover image. Fig. 5(a,b,c) shows three secret images Barbara, and Airplane-F16 which are used as secret images. The size of each secret image is 512 X 256

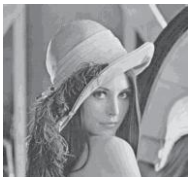

Fig No 4: Cover Image Lena with the size of 512 * 512

(a) (b)

(c)

Fig 5: Secret image with the size of 512 * 256 a: Barbara b: AirplaneF-16,c: Yard

To evaluate the imperceptibility of the stego-image after embedding and also to compare with previous works, PSNR (Peak Signal-to-Noise Ratio) metric is used. As we know the higher stego-image quality, the more imperceptibility of the hidden message. The PSNR is the very first metric which can judge imperceptibility very well. The formula is as follows:

$$PSNR = 10\ log_{10} \frac{255^2}{MSE}\ dB$$

$$MSE = \left(\frac{1}{M * N}\right) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (P(x,y) - P'(x,y))^2$$

where M and N represent the image size. In the formula,P(x,y) stands for the original pixel value and P’(x,y) represents the pixel value in position (x,y) with the secret data already hidden in. A greater PSNR value means a lower degree of image distortion after embedding process of the secret data. For example, given a gray scale image as the cover image to hide secret data in, it is hard for any human being to perceive any difference between the cover image and the stego-image if the PNSR value of the stego-image goes beyond 36 db.Fig 6 shows the experimental result window of hiding the data in an image .

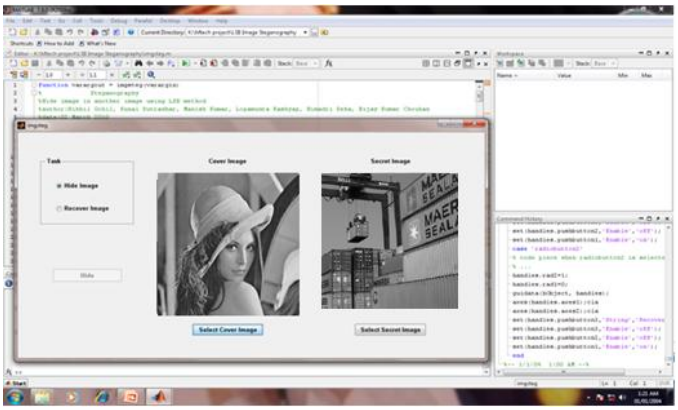

Fig 6:Experimental Hiding an Recover Secret Image Window

Table 1 shows the result of embedding 1048576 bits (four bits per pixel) in cover image Lena by Simple LSB,Optimal Pixel Adjustment,and Optimal Embedding. The results show that the value of PSNR by Optimal Embedding and then by OPA. We assume 8 bits of cover pixel’s are presented as C1C2C3C4C5C6C7C8. If n=1 the algorithm checks the first two layers of cover pixel (C5C6C7C8 and C4c5C6C7) to find the match for secret bits which needs one bit to identify these two layers. When n=2 the first four layers arechecked (C5C6C7C8,C4C5C6C7,C3C4C5C6,C2C3C4C5) As shown in Table 1, there is a significant improvement of PSNR value by Adaptive Optimal Embedding method. When n=2 the probability of finding the desired match of secret bits in cover bits is two times higher than when=1, so the quality of stego-image is significantlybetter by applying n=2.

However by using one bit as stego-key for each pixel (n=1) the results obtained byAdaptive Optimal Embedding is still better than other methods. Adaptive Optimal Embedding since the embedding process is simple and even sometimes there is no need to embed any bits (in situations that match is found) the time of applying our algorithm is nearly the same as simple LSB and OPA.

Embedding Method /Secrete Image	Barbara	Airplane F-16	Yard
Simple LSB	31.3074	30.8879	31.3781
Optimal Pixel adjustment (OPA)	33.7976	33.8214	33.8145
Optimal Embedding Method (Proposed Method) if n=1	34.1640	34.0638	34.1736
n=2	34.7923	34.7327	34.7084

Table 1: The result of Embedding Secret Image into Cover Image Lena

Method /Size of Secrete Data	Simple LSB	OPA	Optimal Embedding method (n=1)	Optimal Embedding method (n=2)
524288 bits (2 bit/pixel)	42.7914	44.8978	46.5645	48.2356
786432 bits (3 bit/pixel)	35.8999	38.1201	40.1011	41.0212
1048576 bits (4 bit/pixel)	30.5889	32.0211	34.0101	35.1401

Table 2 : The Result of Embeding Different amount of Secret data with different 'N'in cover image Lena

In Table 2 our algorithm is tested by different payloads by embedding two, three and four bits per pixel. As shown inTable 2, the results obtained by Optimal Embedding method are still better than the OPA algorithm.By embedding two bits per pixel, the difference between Optimal Embedding and OPA is more than whenwe embed three bits per pixel with the same "n" Becausewhen the embedding rate is two, the probability of findingthe match is higher than when the embedding rate is three,because we are looking for a specific series of two bits (assecret bit) in population of four different values representedby two bits. So the probability of finding is 1/4. But whenwe embed three bits, we look for a series of three bits in eight values (represented by three bits) and the probability of finding this series is 1/8 . The reason of smaller difference in PSNR value between Adaptive Optimal Embedding and other methods by embedding four bits and three bits is the same.

As discussed earlier, the best PSNR is obtained by our method and then by OPA. Although in our method size of the stego-key is large, but since the experiments show, most of the values of stego-key in this method are the same and they are zero.The probability of finding a 4-bit matchbetween

(a) (b)

Fig 6:a: Lena Image without content of Secret Image , b: Lena Image with content of Secret Image

a bit stream is 1/16 because we are looking for four special bits in a population of four bits which can showsixteen different values. For instance we look for "1101"in four bits and these for bits can show a value of "0000" to "1111". In the proposed algorithm, the more bits we use for searching in cover pixel ("n"), the more chance to find a match. But since the chance of finding the match is not much, most of the bits are embedded in LSB. Therefore, by using a compression algorithm like Huffman which is so suitable here, the size of stego-key decreases significantly.

V. CONCLUSION

A new approach is presented to resolve the most important problem of image steganography which is imperceptibility of the stego-image without losing the embedding capacity. To solve this problem, the proposed method embeds secret message bits in the next LSBs of some certain pixels of cover image. The image distortion is decreased by using OPA technique. In order to enhance the effectiveness of the proposed method, it is recommended to apply some algorithms either to decrease the size of stego-key such as Huffman or embedding the stego-key in another cover image .

VI. REFERENCES

[1] Morkel T *et al.* AN OVERVIEW OF IMAGE STEGANOGRAPHY[J]. Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005),2005.

[2] Lee Yeuan-kuen *et al.* An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding[J]. 2009 [3] Lee Yeuan-Kuen,Chen Ling-Hwei.

[3][1] Zanganeh, Omid; Ibrahim, Subariah; , "Image steganography based on adaptive optimal embedding," *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on* , vol., no., pp.600-605, Nov. 30 2010-Dec. 2 2010 [4]Sutaone, M.S.; Khandare, M.V.; , "Image based steganography using LSB insertion technique," *Wireless, Mobile and Multimedia Networks, 2008. IET International Conference on* , vol., no., pp.146-151, 11-12 Jan. 2008

[5]Tao Zhang; Yan Zhang; Xijian Ping; Mingwu Song; , "Detection of LSB Steganography based on Image Smoothness," *Multimedia and Expo, 2006 IEEE International Conference on* , vol., no., pp.1377-1380, 9-12 July 2006