A Steganographic method by using Adaptive Algorithm for gray scale images

[1]Shintre Sandip Sadashiv, [2]P.V. Rao

[1,2]Dept of ECE, Rajarajeswari College Of Engineering, Bangalore-74
Email: [1]Sandipshintre410@Gmail.Com, [2]Raopachara@Gmail.Com/Pachararao@Gmail.Com

Abstract -This paper reviewed the image steganographic technique capable of producing a secret embedded image which is called stego image. This image is totally indistinguishable from the cover image by human eye. The data hiding techniques for a gray scale image for adaptive is usespixel value differencing and modulus function. This algorithm is based on concept of human vision sensitivity. The entire image is partitioned in to number of blocks. In a smoother block, we embed lesser number of bits compared to edged block. The error block does not contain any secret data. Here, we can hide a secret data in the form of message bits as well as data bits according to application. In this method after applying 'error reduction technique' we get a high visual quality for stego image. The obtained results show that the significant improvement with respect to the previous work.

Keywords:Steganography, Embedding, Adaptive, Modulus function.

I. INTRODUCTION

Internet is a popular communication channel nowadays. However, message transmissions over the Internet still have to face some problems, such as data security, copyright control, etc. Thus we need safe and sound secret communication methods for transmitting message over the Internet [5]. Encryption may give a secure way, which transforms data into a cipher-text via cipher algorithms. However, encryption makes the message unreadable, but making message suspicious enough to attract eavesdropper's attention. For overcome to this difficulty, we must employ of data hiding techniques which hide the secret data behind a cover media.

Steganography is a data hiding technique which embeds secret data into a cover media such as text, image, audio and video, so that the result does not notice any third's attention. The image into which a massage is hidden is called a cover image and the final result is known as stego image. Intention of the data hiding can be used in military, commercial and anti-criminal depended application, transmission of confidential documents between international governments and be anonymous in internet.

In an adaptive system we consider the position, where each embedding change was done. In first category, a well-known steganographic method is the Least Significant Bit (LSB) substitution method, which embeds secret data by replacing k LSBs of a pixel with k secret bits directly. Three criteria are used to evaluate the performance of data hiding schemes: the embedding capacity, the visual quality of the stego image and the security.

An adaptive steganographic scheme that uses average differencing value of four neighborhood pixels and modulus function [8]. This adaptive scheme is based on the concept of human vision sensitivity, so that it is more difficult to notice changes at the edge area of original image than those in smooth area. Accordingly, the number of bits to be embedded into each block is variable and deter-mined by the correlation between neighborhood pixels into its block. In adaptive scheme, the average differencing value of a four-pixel block and a threshold secret key T are used for detecting the edge or smooth areas, according to the local complication of a cover image. The number of bits to hide in the edge blocks is more than of those to hide in smooth blocks. This method produces slightest amount distortion for the stego image.

In adaptive algorithm, problem of overflow and underflow will not be occurred. Experimental outcome show that the proposed adaptive algorithm significantly is superior to the currently existing scheme, in terms of stego image visual quality, embedding capacity, level of security.

II. LITERATURE SURVEY

Chin–FengLee, Hsing-Ling Chen [1]In this paper, four criteria are generally used to evaluate the performance of data hiding scheme. The embedding capacity the visual quality of stego image, the security and the complexity of data hiding data embedding algorithm. This paper proposes a novel data hiding scheme that uses simple modulus function to address all the performance criteria listed above. According to input secret keys, the encoder and decoder use the same set of generation functions Hr( ) and Hc( )to first generate two sets Kr and Kc. A variant Cartesian product is then created using Kr and Kc. Each cover pixel then forms

the a pixel group with its neighbouring pixel by exploiting an efficient modulus function the secret data then embedded or extracted via a mapping process between the variant of the Cartesian product and each pixel group.

Chung-Ming Wang , Nan-I Wu , Chwei-Shyong Tsai, Min-Shiang Hwang [2]In this paper, a new stenographic technique capable of producing a secret-embedded image that is totally indistinguishable from the original image by human eye. In addition this new method avoids the falling of boundary problem by using the pixel value differencing and modulus function. First derive a difference value from two consecutive pixels by utilizing the pixel value differencing technique. Second the reminder of two consecutive pixels can compute by using the modulus operation. The secret data can be embedded into the two pixels by modifying their remainder.

Yang CH, Weng CY, Wang SJ, Sun HM [12] This paper proposes a new adaptive least significant bit stenographic method using pixel value differencing that provides a larger embedding capacity and imperceptible stegoiages. The method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into two pixels. Pixels located in the edge areas are embedded by k-bit LSB substitution method with a larger value of k than that of the pixels located in smooth areas. The range of difference values is adaptively divided into lower level, middle level, and higher level. For any pair of consecutive pixels, both pixels are embedded by k- bit LSB substitution method.

III. PROPOSED METHOD

Transmitter Section

In Transmitter section there are 3 parts:

(1) Input cover Images

(2) Encoder section

(3) Output Stego Image

There are 11 cover images used for the proposed scheme to be taken as an input Original cover Image which is used for embedding secret data in it.

Encoder unit is composed of Generation function and secret keys. Encoder determines whether it is smooth area or edged area depending upon the threshold value. In smooth area small number of bits embedding compared to edged area.

Finally at the transmitter section Stego image is generated which is a combination of secret keys and cover images.

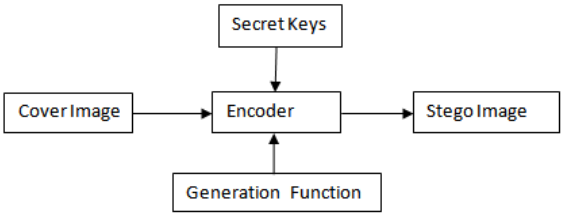

Figure 1: The block diagram Transmitter section

Encoder unit is composed of Generation function and secret keys. Encoder determines whether it is smooth area or edged area depending upon the threshold value. In smooth area small number of bits embedding compared to edged area.

Finally at the transmitter section Stego image is generated which is a combination of secret keys and cover images.

Receiver Section

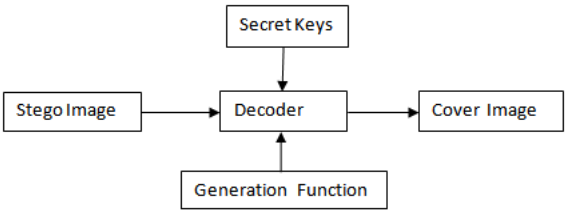

Figure 2: The block diagram Receiver section

In Receiver section there are 3 parts:

(1) Input Stego Images

(2) Decoder section

(3) Output Cover Image

The Stego Image is taken as an input to the receiver side. The Stego image is decoded correctly by using secret keys and generation function to obtain the cover image.

The secret keys used in both the transmitter and receiver side are same. Pixels in the edge areas are embedded by Q-bit of secret data with a larger value of Q than that of pixels placed in smooth areas.

IV. PROJECT METHODOLOGY

4.1 The proposed adaptive scheme:-

There are five secret keys namely R1, R2, v1, v2, T and 1 6 v1, 1 6 v2, (v1 + v2) < 6. The average different values of a four-pixel block are utilized to classify the block as a smooth area or an edge area. The range of average different value is partitioned into two different levels, smooth level and edge level. Q-bit of the secret data is embedded in Pixels located in the block, where Q is decided by the level in which the average different values belong to. In the embedding process of secret data, according to the secret keys v1 and v2, the smooth level will use lower value v1 while the edge level uses greater value v1 + v2. The data embedding process is

given in Section 4.1.1 and the extracting phase is described in Section 4.1.2.

4.1.1 The embedding phase in proposed adaptive scheme

The cover image is partitioned into non-overlapping four-pixel blocks. For each block, there are four neighboring pixels Pi, j, Pi,j+1, Pi+1,j, Pi+1,j+1 and their corresponding gray values are y0, y1,y2,y3, respectively.

The detailed embedding steps are as follows:

Step 1: Generate Two sets Kr and Kc using threshold Hr (R1, v1) and Hc (R2, v2), respectively. Via sets Kr and Kc form a variant of a Cartesian product namely, Kr _ Kc. Set Kr _ Kc generates an ordered set of combinations of Kr and Kc with 2v1 • 2v2 = 2v1+v2 elements (Eq. (1)).

$Kr*Kc=\{Kri\,||\,Kcj\,|,Kri€Kr,Kcj€Kc\ ,\ i=1,2,3...2^{v1}\}$

$=1,2,3.....2^{v2}$….(1)

Step 2: Calculate the average difference value D, Which is determined by

$D = 1/3 \sum_{i=0}^{3}(yi - ymin)$....(2)Where ymin is:ymin=min {y0, y1, y2, y3}

Step 3: Using Threshold T and D find smooth block, Edge block and error block.

i.e.

a) If D<=T, D belongs to Smooth block.

b) If D>T, D belongs to Edge block.

c) If D<=T and (ymax- ymin)> 2*T+2, D belongs to Error block.

Step 4: Repeat step 3 for full image

Step 5: Capacity= ((edge block*(v1+v2)) + smooth block*v1))*4.

Step 6: For smooth block obtain i using Kr & Secret data and find‘d’.

For edge block:-

$d=2^{v2}\times(i-1)+j$ ….(3)

For smooth block:-

$d=i$ ….(4)

Step 7: Create pixel group using 'n=2^Q’.

$f(yi)=yimodn+1$ ….(5)

Step 8: Using pixel group embed the Secrets bits

Step 9: If No Of Secret Data=Capacity, go to step 10 else step 6.

Step 10: Apply error reducing procedure for minimizing perceptual distortion between cover&stego image.

FLOWCHART:

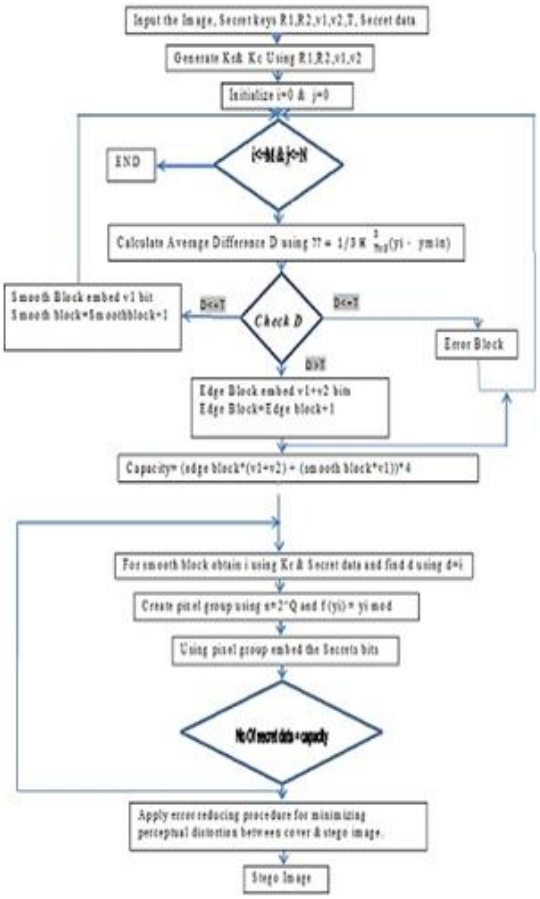

Figure 3: Adaptive Algorithm

4.1.2 The extracting phase in proposed adaptive scheme

Like the embedding process, Partition the stego-image into four-pixel blocks.

The following steps are executed to extract the secret data.

Step 1: Input Stego Image, Secret keys R1, R2, v1,

v2, T

Step2: Generate Kr&Kc Using R1, R2, v1, v2

Step3: Initialize i=0 & j=0

Step 4: if i<=M & j<=N, go to step 5 else stop.

Step 5: Calculate Average Diff ‘D’ using eq. (2)

Step 6: Using Threshold ‘T’ and ‘D’ find smooth

block, Edge block and error block.

i.e.

a) If D<=T, D belongs to Smooth block.

b) If D>T, D belongs to Edge block.

c) If D<=T and (ymax-ymin)> 2*T+2, D

belongs to Error block.

Step 7: Create pixel group using n=2^Q and

f(yi)=yi mod n+1

Step 8: Determine position information'd'.

Step 9: From'd' extract secret data.

V. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents experimental results obtained for original images. This images consist of 'couple', 'children', 'town' and 'light house' each of 512*512 pixel in 2-D format as shown in following figure.

Figure 4: Cover Images

Several experiments are performed to evaluate our proposed methods. By using proposed Adaptive method we get following results:

Original Image is applied as a Cover Image after error reduction procedure we get final Stego Image.

Figure 5: Cover Image

Figure 6: Before Error Reduction Procedure

Figure 7: Final Stego Image

We used a series of pseudo-random numbers as the secret data to be embedded into the cover images and also utilized the peak signal-to-noise ratio (PSNR) value to evaluate the stego-images quality.

The PSNR is defined as follows:

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - q_{ij})^2} (dB) \quad \text{....(6)}$$

PSNR for Couple image before error reduction is 34.8731 and after error reduction we get enhanced PSNR value 36.8457 in dB is calculated by eq.(6).

The following table shows PSNR for 'couple', 'children', 'town' and 'light house' images for different threshold and secret key values.

Table 1: Experimental Results with different threshold and secret key values.

Cover Images	V1 = 1 V2 = 3 T = 5		V1 = 2 V2 = 3 T = 9		V1 = 2 V2= 1 T=17		V1 = 3 V2 = 2 T = 25	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Boys	351760	43.5356	575252	39.7164	531756	45.9059	793968	39.8208
Town	540552	43.2063	778524	33.5650	556496	45.3128	811620	38.3834
Couple	735096	36.9557	812248	33.0604	510768	44.6954	837984	36.8471
lighthouse	784912	36.5308	904508	31.8901	590136	44.0518	866100	35.6639

VI. CONCLUSION

In this paper an adaptive steganographic method that uses average differencing value of four neighborhood pixels. This method is based on the concept of human vision sensitivity, so that it is very complicated to detect changes at the edge area of original image than those in smooth area. The number of bits to be embedded into each block is variable depending upon whether it is smooth block or edged block. In proposed method the average differencing value of a four-pixel block and a threshold secret key T are used to detect the edge or smooth blocks, according to the local complexity of a cover image. The number of bits to hide in the edge blocks is larger than of those to hide in smooth blocks. The problem of overflow and underflow will not be occurred in our adaptive algorithm. Experimental results indicate that the proposed adaptive algorithm significantly is better than currently existing scheme, in terms of stego-image visual quality, hiding capacity and level of security.

This algorithm is safe and scalable, depending on the requirements of the application. Also, these allowed the clients to hide a variety of huge secret messages as well as data bits, while at the same time sustain the general appearance of any cover image used. In the proposed methods in this scholar, detecting secret data is extremely complicated for malicious, because of the large permutations. Also with our schemes having several secret keys, their security level is high.

REFERENCES

[1] Lee CF, Chen HL. A novel data hiding scheme based on modulus function. J Syst Software 2010;83:832–43

[2] Mielikainen J. LSB matching revisited. IEEE Signal Process Lett 2006;13(5):285–7.

[3] Hartung F, Kutter M. Information hiding – a survey. ProcIEEE 1999;87:1062–78.

[4] Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Pattern Recognit 2004;37(March):469–74

[5] Zhang X, Wang S. Efficient steganographic embedding by exploiting modification direction. IEEE CommunLett 2006;10(11): 781–3.

[6] Bender DW, Gruhl NM, Lu A. Techniques for data hiding. IBM Sys J 1996;35:313–6

[7] Fridrich J, Goljan M, Du R. Reliable detection of LSB steganography in color and grayscale images. In: Proceedings of ACM workshop on multimedia and security; 2001. p. 27–30

[8] Wu DC, Tsai WH. A steganographic method for images by pixel- value differencing. Pattern RecognitLett 2003;24:1613–26.

[9] Liao X, Wen QY, Zhang J. A steganographic method for digital images with four-pixel differencing and modified LSB substitu- tion. J Vis Commun Image R 2010;1–8.

[10] Hsiao Ju-Yuan, Chang Chieh-Tse. An adaptive steganographic method based on the measurement of just noticeable distortion profile. Original Res Article Image Vision Comput 2011;29(2–):155–66

[11] MeenaManoj Kumar, Kumar Shiv, Gupta Neetesh. Image steganography tool using adaptive encoding approach to maxi- mize image hiding capacity. Int J Soft ComputEng (IJSCE) 2011;1(2):7–11.

[12] Yang CH, Weng CY, A steganographic method for digital images by multi pixel differencing. In: Proceedings of international computer symposium, Taipei, Taiwan, R.O.C.; 2006. p. 831–6.