International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 12, December 2015

Image Steganography Using Variable-Rate LSB Approach

[1] **Hemshikha Joshi** [2] **Rahul Agarwal**
Department of Computer Science & Engineering
Engineering College Bikaner, Rajasthan, India
[1]*hemshikhajoshi@gmail.com* [2] *rahul16agarwal@gmail.com*

Abstract- Steganography is the art of hiding facts where communication is taking place, by hiding information in another information. **The purpose of Steganography is to maintain secret communication between two parties.** ***Many different file format carrier can be used, but the digital image are the most popular bacause of their frequency on the internet. In this paper a*** **new algorithm is described for hiding a secret image in the least significant bits of a cover image. Least Significant-Bit (LSB) based approach is most popular steganographic techniques in spatial domain due to its simplicity and hiding capacity. This method supports both type of images colour and gray scale image. How many LSB hides the secret information is decided by the exclusive-or (XOR) operation of a pixel's neighbour.** ***Here result is sensitive to the smothness of the neighbour pixel.***

Keywords: **Image steganography, ex-or operation, least significant bit, stego-image.**

I.INTRODUCTION

Steganography is the process of hiding one file into another such that others can neither identify the meaning of the embedded object, nor even recognize it,s existence. With the rapid growth of Internet technologies digital media can be transmitted conveniently over the network. So there is a need to protect data during transmission. Steganography is a technique for information hiding. Steganography means, cover writing it's origin is old and backs to Golden age of Greece when people at that time had different practices to hide writing for e.g. writing on a wooden tablet and then covering it by wax, making a tattoo on a messenger head after shaving his hair and let his hair grows up again and then send him to the receiver where his hair was shaved there again to get the message. Other steganography techniques like using invisible ink for writing between lines, microdots and using character arrangement are also used. It aims to embed secret data into a digital cover media, such as digital audio, image , video, etc [1]. Without being suspicious. Steganography is all about creating a form of secret communication between two parties and it is a complement of cryptography. In this paper, a new algorithm is presented to hide information in the least significant bits (LSBs) of image pixels . The algorithm uses a variable number of hiding bits for each pixel, the number of variable bits depends on the xor of the neighbour pixels. The amount of visible degradaytion is expected to be higher for smooth areas, so the number of hiding bits is chosen to be proportional to the exclusive -or (XOR) of the pixel's neighbors[2]. Analysis showed effectiveness of the algorithm in minimizing degradation while it was sensitive to the smoothness of cover images.

II.BACKGROUND AND RELATED WORK

Surveys of different steganography techniques were presented in previous work. When an image is chosen to be used for hiding information, it is called a cover image. A cover image containing the secret information is called a stego image. Steganography can be categorized into four categories: audio, video, image and text. For hiding information usually Least Significant Bit (LSB) method is used [3]. In the LSB method the 8th bit of every byte of the carrier file is substituted by one bit of the secret information. This method works fine in the image carriers because if the least significant bit is changed from 0 to 1 or vice versa, there is hardly any change in the appearance of the colour of that pixel. Instead of hiding a fixed number of bits in the LSBs of each pixel, one can also embed different number of bits in LSBs of different pixels based on pixel value range calculation. In general if the pixels are located in edge areas they can tolerate larger changes than those in smooth areas.

Wu and Tsai proposed a pixel value differencing method, where a cover image is partitioned into non overlapping blocks of two consecutive pixels. A difference value is calculated from the value of the two pixels in each block. Secret data is covert into a cover image by replacing the difference values of the two pixel blocks of the cover image with similar ones, in which bits of embedded data are included. Zhang and Wang found that pixel value differencing steganography is vulnerable to histogram based attacks and proposed a modification for enhanced security. Chang and Tseng employed two sided, three sided and four sided side match methods [4] . The two sided side match method uses the side information of the upper and left neighbouring pixels in order to make estimates . The three sided side match method uses upper and left neighbouring pixels, and one of the other neighbouring pixels. The four sided side match method uses the upper, left, right and

below neighbours. Chang et al. proposed a three way pixel value differencing method. Zhang et al. proposed a pixel value differencing technique by using the largest difference value among the other three pixels close to the target pixel to estimate how many secret bits will be embedded into the pixel [5], [6] . Generally, the related privious work did not focus on hiding images inside other images . In addition, related image steganography research was usually limited to either gray scale or Red-Green-Blue images . The new algorithm of this paper handles hiding diffferent images inside other images of various types.

III.PROPOSED WORK THE HIDING AL GORITHM

Least Significant Bit image steganography is most commnely used algorithm in which least bit is replaced with MSB of secret message. But there are some disadvantage using the simple LSB technique so that we use random variable number of LSB technique. Here algorithm uses a variable number of LSBs from each pixel of the cover image for hiding . A gray scale image consists of only one colour matrix. A Red-Green-Blue (RGB) colour image consists of three matrices representing the three colour. The number of bits chosen from each pixel colour (red, green, and blue) is different. The actual number of bits changes according to neighbourhood information of each pixel colour. The number of bits used for hiding is chosen to be proportional to the neighbours XOR value for each pixel colour entry. Pixels that are reside on the boarder of cover image not used for the hiding information, so almost 50% of pixels are used for hiding the values. The algorithm for hiding image shown in

Figure 1.

In this algorithm stegoC may be stegoR, stegoG or stegoB represent as red, green or blue colour matrix. Each colour is treated separately. But in the gray scale image stegoC describe as single colour matrix. In this method we do not hide information at the boarder of the image. The XOR is computed for the value of each one of these pixels' four neighbours left, right, above, and below as shown in figure2.This comparison measures the smoothness of the pixels neighbourhoods so that the number of hiding bits can be determined. This process will continue running till whole secret image is not finished. So by using this technique we can hide our secret image into cover image at random selection of LSB. The condition for hiding image is that the size ratio between the cover and secret image should be (n*m)/ (p*q)>=6. Where n*m is the size of cover image and p*q is the size of secret image.

```
row=2
while(row<=n-2) and (secret image not
finished)
col-col+(row Mod 2)
while col<=m-2
x= stegoC(row-1,col) xor stegoC(row+1,col)
xor stegoC(row, col-1) xor stegoC(row,
col+1)
if x<=α
numLSBs = 1
else
numLSBs = ceil(x/2)
endif
replace LSBs of stegoC(row, col) with the
next numLSBs bits from secret image
col = col+2
endwhile
row = row+1
endwhile
```

Fig: 1 Hiding Algorithm

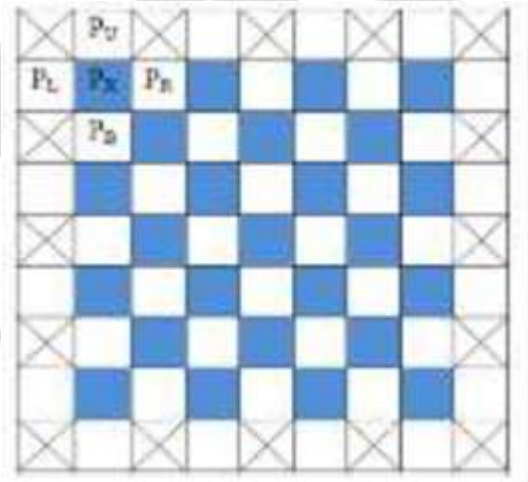

Fig.2: Neighbourhood [ixels for ex-or operation

If the XOR value is less than a given threshold α, only one LSB is used for hiding. Otherwise, the number of LSBs (numLSBs) used will be the ceiling of one-half of the XOR value. In the implementation of this paper, α was set to 9 and the maximum number of LSBs used for hiding in any pixel colour was 4. The extraction process searches each of the three colour matrices (Red, Green, and Blue), going through all lines and every other column as in the hiding procedure. The number of bits used for hiding in an entry, stegoC (row, col), is also determined by examining x; the XOR of the four neighbours as in the hiding process. All extracted hidden values are concatenated and grouped into bytes to form the original secret image.

IV. RESULT AND ANALYSIS

The algorithm was applied different images of different types and sizes for hiding. The sizes of these secret images ranged from 55*110 to 175*148 pixels. Three different cover images were used: Office (3001*2375 pixels) and light-house (2560*1920). The analysis of the results focus on two aspects: difficulty to detect the hidden image existence in the stego image and sensitivity to the smoothness of the cover image. Recall that only non-adjacent pixels are used for hiding. These are approximately 50% of the pixels in the image. Figure 3 and 4 shows one sample secret image (penguins), which is 148*175 pixels, and the two cover images. Figure 5 shows the three stego images where each of them is hiding a copy of the Penguin image. As seen in the figures, the difference between the original images and the stego images is not visible to the human eye. The peak siganal-to-noise ratio (PSNR) values were the highest for the light-house cover image. This cover image has mostly smooth areas, which caused the algorithm to choose only one bit for hiding in each of 84.6% of the pixel entries used for hiding, as seen in TABLE I. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB.

Fig. 3: Secret images

Fig. 4: cover images (office and light-house image)

Fig. 5: Stego images (office and light-house image)

COVER IMAGE	PSNR (db)	1 Bit %	2 Bit %	3 Bit %	4 Bit %
Office	62.701	84.6	11.3	2.9	1.2
light-house	62.72	36.9	32.0	27.1	4.0

Table 1: Result for the Penguin Test Image

V.CONCLUSION

The performance of various steganographic methods can be rated by the three parameters: security, hiding capacity, and imperceptibility. The steganographic methods proposed in this paper are very secure as variable number of bits are hidden in different target pixels. The hiding capacity is totally depend on the smothness of the neighbour pixel area. Test results represent that the new algorithm keeps the hidden image difficult to recognize, as shown by the high PSNR and correlation values for stego images. The algorithm must hide less information in images containing more smooth areas to keep avoiding detection. This indicates that hiding in such images would be a poor choice.

Future Work

The presented algorithm may be modified easily to work with more security. This paper explore only a small part of science of steganography. There is great deal more research and devlopment to do. Here in this paper we used only steganography technique. before hiding the secret image if we encrpt that image using a secret key than security will be more. By combine both the technique using steganography and encrption more security provided to the information. This same methos can also apply on the video stegnography. Where each single frame of video is treated as image.

REFERENCES

[1] Arvind Kumar, K m Pooja, "Steganography-A Data Hiding Technique", International Journal of Computer Applications, Vol. 9-No.7, November 2010.

[2] Abdelfatah A. Tamimi, Ayman M. Abdalla, Omaima Al-Allaf "Hiding an Image inside another Image using Variable-Rate Steganography" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 10, 2013

[3] G. Chhajed, K. Deshmukh and T. Kulkarni, "Review on binary image steganography and watermarking," Int. J. Comput. Sci. & Eng. vol. 3, no. 11, pp. 3645-3651, 2011.

[4]Y. K. Lee. and L. H.Chen. High capacity image steganographic model. IEE Proc.-Vision, Image and Signal Processing, 147:288–294, 2000.

[5] A. Pradhan, D. Sharma and G. Swain, "Variable rate steganography in digital images using two, three and four neighbour pixels," Indian J. Comput. Sci. & Eng., pp. 457 463, 2012.

[6] Zhang, X.; Wang, S. (2004): Vulnerability of Pixel Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security, Pattern Recognition Letters, vol.25, pp. 331-339.

[7] Kim, K. J.; Jung, K. H.; Yoo, K.Y. (2008): Image Steganographic Method with Variable Embedding Length, International Symposium on Ubiquitous Computing, pp. 210-213.