IMAGE STEGANOGRAPHY USING MIXED CHANNEL REPLACEMENT

Tejinderpal Singh[1] and Simpel Jindal[2]
[1]*Department of Computer Engineering,*
Yadavindra College of Engineering, Talwandi Sabo, Punjab.
er.tejindersidhu@yahoo.com, simpel_jindal@rediffmail.com

Abstract: *Steganography is a method of hiding information in other information. In this paper, we proposed a new image steganography scheme which is a kind of spatial domain technique. The mixed channel replacement technique is used to hide secret data in cover image. Techniques used so far focuses only on the two or four bits of a pixel in a image (at the most five bits at the edge of an image) which results in less peak to signal noise ratio and high root mean square error. In this technique, each character of secret message is divided into three blocks. Each block is embedded in different components (R,G and B) of pixels. This scheme can embed more data than previous schemes and shows better image quality. Various experiments are performed to test this scheme and it is found that there are no visual distortions in the image.*

Keywords: *Image, spatial domain, mean square error, peak signal to noise ratio, stegano-graphy.*

I. INTRODUCTION

Today, the security of information is regarded as one of the most important factors of Information Technology and communication. Accordingly, we need to take measures which protect the secret information.

The secret information may be hidden in one of two ways, such as cryptography and stegano-graphy. The method of cryptography makes the

data unintelligible to outsiders by various transformations, whereas the methods of steganography hide the existence of messages. The word steganography is derived from Greek words meaning “covered writing” and as such it centers on the concept of hiding a message. As defined by Cachin [1], steganography is the art and science of communicating in such a way that the presence of message is detected. Steganography is very old method used. Around 440 B.C., Histiaeus shaved the head of his most trusted slave and tattooed it with a message which disappeared after the hair had regrown. The purpose of this message was to instigate a revolt against the Persians. Another slave could be used to send a reply. During the American Revolution, invisible ink which would glow over a flame was used by both the British and Americans to communicate secretly.

Steganography can be of many types, like image steganography, audio steganography, video steganography, text steganography and protocol steganography. Among the methods of steganography, the most common thing is to use images for steganography. This is called image steganography. In this image hiding method, the pixels of images are changed in order to hide the secret data so as not to be visible to users, and the changes applied in the image are not tangible. The image used to hide the secret data is called the cover-image while the cover image with the secret data embedded in it is called the stego image. Image steganographic techniques can be divided into two groups [2]: the Spatial Domain technique group, and the Transform Domain technique group. The Spatial domain technique embeds information in the intensity of the pixels directly, while the Transform domain technique embeds information in frequency domain of previously transformed image. Our proposed technique is a type of the spatial domain techniques.

II. RELATED WORKS

A. Review of Least Significant Bit Substitution (LSB) Scheme

LSB substitution is the most popular method used for steganography due to its ease of application and less perceptual impact. This method is probably the easiest way of hiding information in an image. In the LSB technique, the LSB of the pixels is replaced by the message to be sent. The

secret message is converted to a bit stream and each bit of the message is embedded into the LSB of the pixels of the image. This ensures that the pixel value changes almost by one, which does not result in a significant change in the image quality perceptually. The message bits are permuted before embedding, which has the effect of distributing the bits evenly, thus on average only half of the LSB's will be modified and hence no change to the image is made. Using this method it is possible to embed a significant amount of information with no visible degradation of the cover image [8].

B. Pixel-Value Differencing (PVD) technique

Pixel-value differencing (PVD) method is used to discriminate between edged areas and smooth areas. The number of insertion bits is dependent on whether the pixel is on edge area or smooth area. In edge area the difference between the adjacent pixels is more, whereas in smooth area it is less. The capacity of hidden data in edged areas is higher than that of smooth areas. While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more sensitive to changes in the smooth areas. With this concept, Wu and Tsai proposed a novel steganography technique using the pixel-value differencing (PVD) method to distinguish edge and smooth areas. The PVD technique can embed more data in the edge area which guarantees high imperceptibility [4].

C. Review of Lie-Chang's scheme

The Steganographic technique has to possess two important properties. These are good imperceptibility and sufficient data capacity. Lie-Chang proposed a scheme which satisfied both these properties. The scheme is an Adaptive LSB technique using Human Visual System (HVS). HVS has the following characteristics: Just Noticable Difference (JND), Contrast Sensitivity Function (CSF), Masking and Spectral Sensitivity. The characteristic of HVS used by Lie-Chang is JND (also known as the visual increment threshold or the luminance difference threshold). In this scheme, JND is defined as the amount of light ΔI necessary to add to a visual field of intensity I such that it can be distinguished from the background. In HVS,

the curve for ΔI versus I can be analytically and mathematically modeled [2].

The JND technique is simple and has a higher embedding capacity than other schemes. Also, this technique has high embedding capacity about overall bright images and has high distortion of a cover image when the embedding capacity is increased, but does not concern overall dark images.

D. Jae-Gil Yu et al.'s scheme

This scheme is a type of spatial domain technique. This is an MSB3 edge-detection which uses part information of each pixel-value. In this method, Jae-Gil Yu et al. used the just noticeable difference (JND) technique and method of contrast sensitivity function (CSF). In order to have better imperceptibility, a mathematical method which is the 2^k correction is used. If one supposes the secret data is hidden at a pixel of cover image, some differences occurred between cover-pixel and stego-pixel. Because of these differences, the cover image is distorted and the quality of cover image is dropped. 2^k correction corrects each pixel-value as 2^k. That is, supposing that *k*-bits are embedded in a pixel value, the method adds or subtracts 2^k to each pixel-value, and finally the corrected pixel value becomes closer to the original-pixel. Hence, the secret data in the stego-pixel is not changed. This scheme can embed more data than previous schemes, and shows better imperceptibility. The method is an edge detection which only uses 3-bits from MSB of each pixel value. In this method, data embedment depends on the value received from each pixel value whether it is on the edge or on other part of an image. If it is on the edge it embed data in the cover image based on the value of k, value of k is decided on the pixel position whether it is on the edge or not. This method modifies the stego pixel value near to the cover pixel using 2k correction mathematical formula [6].

III. Proposed Technique

In this section, a new image steganography scheme based on mixed channel replacement technique is proposed. In a computer, images are represented as arrays of values. These values represent the intensities of the three colors R (Red), G (Green) and B (Blue), where a value for each of

three colors describes a pixel. Each pixel is combination of three components (R, G, and B).

In this scheme, the bits of all components of pixels of image have been used to hide data bits, which are applied only when valid key is used. We are going to hide the data at spatial domain (operation at the pixel level) .We are proposed the new technique to hide the data in the image by making three proposed blocks. ASCII value of each character is divided into three blocks. First block will be bitwise EX-OR with Red channel. Second block will be bitwise EX-OR with Green channel. Remain Block will be added in the Blue Channel. Blue channel is selected because the visual perception of intensely blue objects is less distinct that the perception of objects of red and green.

A. Algorithm for hiding the secret message

Input: A cover image & secret text message

Output: Stego image

Step 1. Input the cover image and the secret message.

Step 2. Convert the cover image into the matrix of pixel values.

Step 3. Convert the secret message into ASCII code. Extract the message length and store it into L.

Step 4. Input secret key.

Step 5. Obtain the R, G, B pixel matrices and make the blocks for R, G, B.

Step 6. Split the ASCII code of single character of message into three blocks. First block contains 8. Second block contains 8. Third block contains the remaining value (Total value -16)

Step 7. Repeat the steps 6 & 7 till L > 0. Substitution scheme as follows.

Step 7.1 Select first block and bitwise EX-OR with channel Red (This will make the minimal effect with add up of one bit).

Step 7.2 Select second block and Bitwise EX- OR with channel Green.

Step 7.3 Third Block will be added in the Blue channel (Blue channel adds always lesser effect to human visualization).

Step 7.4 Set L = L - 1

Step 8. Place zero to next pixel indicate the end of data.
Step 9. Save the image & say it the stego image.

B. Algorithm for Extracting the secret message

Input: Stego image

Output: Secret text message

Step 1. Read the stego image.
Step 2. Input key to find the characters from image.
Step 3. Convert the stego image into the matrix of pixel values.
Step 4. Repeat the steps 5 to 8 till we find pixel with RGB = 0.
Step 5. Get the R & G matrix values. Check the 4^{th} bit of R & G matrix values.
Step 5.1 If it is 0, then add 8 to the given matrix value and perform AND operation with 8.
Step 5.2 If it is 1 then perform the AND operation of R & G values with 8.
Step 6. Get the B matrix value from the given image.
Step 7. Add the values got from R, G & B matrices to get a single value.
Step 8. Convert this value into ASCII character. Go to step 4.

IV. RESULTS

In this, the algorithm is tested on many BMP images. The images are tested by various methods and then tested by a proposed technique. Firstly, the proposed scheme is applied to Lena's image as a test image. Different results have been observed with RGB components by changing mixed components to embed data in it.

The performance is evaluated on two metrics: Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). We used these metrics to measure image quality of the proposed scheme.

Fig. 1 Lena Cover Image

Fig. 2 Lena Stego Image

The results are then compared with various methods as shown in the table. The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image, the higher the PSNR, the better the quality of the compressed or reconstructed image. The MSE (Mean Square Error) represents the cumulative squared error between the compressed and the original image, the lower the value of MSE, the lower the error [7]. In this paper we have shown the results for the technique by using lena.bmp as cover image. Fig. 1 shows the cover image and Fig. 2 shows stego image.

We can see from the fig.1 and fig.2 that there are no visual distortions in the images. The results are then compared with various steganography methods as shown in the following table. We can see from the table1 that PSNR of our technique is higher than all related techniques.

Table 1. Comparison of PSNR achieved by different techniques on Lena.bmp

Lena Image	LSB3	PVD	Lie Chang's	Jae-Gill Yu	Proposed technique
PSNR	37.92	41.48	37.53	38.98	66.94

V. Conclusion

In this paper we proposed a new image based steganography technique, which makes the use of all components of pixel to store one character of the secret message. This leads to very high data hiding capacity. It is a kind of spatial domain technique. The mixed channel replacement techn-ique is used to hide secret data in cover-image. Techniques used so far focuses only on the two or four bits of a pixel in a image (at most five bits at the edge of an image.) which results less peak to signal noise ratio and high root mean square error i.e. less than 45 PSNR value. Proposed work is concentrated on all three components of a pixel, resulting better image quality. Proposed scheme can embed more data than previous schemes [4, 2, 6] and shows better imperceptibility. Various experiments are performed to test this scheme and the experimental results are compared with the related previous works. The results proved that the proposed scheme is better than the related previous works.

References

[1] C. Cachin, "An Information-Theoretic Model for Steganography," Proceedings of 2nd Workshops on Information Hiding, MIT Laboratory for Computer Science, May 1998.

[2] W. N. Lie and L. C. Chang, "Data hiding in images with adaptive number of least significant bits based on the human visual system", Proc. ICIP '99, 1:286–290, 1999.

[3] W. Stallings, "Cryptography and Network Security – principles and practices", Pearson Education, Inc., 2003.

[4] D. C. Wu and W. H. Tsai., "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, 24:1613–1626, 2003.

[5] T. Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography", in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/ July 2005.

[6] Jae-Gil Yu, Eun-Joon Yoon, Sang-Ho Shin and Kee-Young Yoo., "A New Image Steganography Based on 2^k Correction and Edge-Detection", ITNG Proceedings of the Fifth International Conference on Information Technology: New Generations, Pages 563-568, 2008.

[7] K.S. Babu, K.B. Raja,K.K. Kiran,Manjula Devi T.H.,Venugopal K.R., Patnaik, L.M, "Authenti-cation of Secret Information in Image Steganography", TENCON 2008, pages 1-6, Nov. 2008.

[8] R.Amirtharajan, R. Akila, P.Deepikachowdava-rapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications (0975 – 8887) Volume 2 – No.3, May 2010.