A Secured Method for Image Steganography Based On Pixel Values

Tarun Gulati[#], Sanskriti Gupta[*]

[#] *Associate Professor, Electronics and Communication Engineering Department, MMEC, M.M.U., Mullana, Ambala, Haryana, India*

[*] *Research Scholar, Electronics and Communication Engineering Department, MMEC, M.M.U., Mullana, Ambala, Haryana, India*

Abstract: Steganography is the science of communication that hides secret information inside the multimedia signal in such a way that the existence of secret information is concealed. In this paper image steganography is done. The text string is concealed in the cover image as a payload. The technique is based on pixel value differencing and pixel value sum. A secret key is used to control the message embedding process. At the receiver stego image is manipulated to get the text out of it. PSNR and capacity are used to measure the stego image quality.

Keywords — *Steganography, Pixel Value Differencing, Pixel Value Sum, Security.*

I. INTRODUCTION

During the last few decades, internet is becoming a very popular medium for communication. But data security during transfer through it has become a major challenge. There are two approaches [1] to send the information. One is cryptography, in which the information is transferred in form of unintelligible text. But in cryptography, intruder can easily detect the presence of some secret information by observing it. Also, intruder can apply the cryptanalysis to obtain the information. Another approach is steganography. Steganography makes communication unintelligible for the intruder. In steganography, the secret message is hidden inside the another carrier so that it looks innocent as it is not hiding any secret message. Only the authorized recipient can detect the presence of some intelligible information.

Steganography [2] is art and science of secret communication which hides the existence of the secret data inside another data to protect it from unauthorized users. Many different carriers such as audio, video and digital images can be used, but digital images are mostly used because of their frequency over the internet. In image steganography information can be exclusively stored in image. The image used for hiding the secret information is called cover image. Steganography hides the information in the cover image [3] and the final image so formed is called stego image. Also, the reverse of this i.e. breaking of steganography is called steganalysis. It is important that the stego image must be free from noticeable change, so that the third party will not be able to detect any changes and treat this cover image as usual image and secret data send through this cover image remains safe.

Steganography can be done using different methods like

- Least Significant Bit Substitution method,
- Pixel Value Differencing Method,
- Pixel Value Sum and Differencing.

In the processing of LSB substitution [4], the secret data is embedded in the LSB of the pixels in the cover image. PVD technique [5] is a steganographic method based on difference of the two consecutive pixels. It hides the secret data inside the image in the non-overlapping consecutive pixels by changing the difference value. On the other hand PVS deals with the sum of the two consecutive pixels in the cover image. The methods are implemented in order to obtain the high embedding capacity, more security and the visual effects of the image file remains preserve. The proposed method of image steganography is an improvement to PVS and PVD technique [6] by inserting a secret key inside it to make the system more secured [7].

This paper is organized as follows. In section II previous work done for both PVD and LSB is presented. In section III methodology used for hiding secret data along with security key is described. In section IV results of all the techniques described in this paper are compared and finally conclusions are given in section IV.

II. PREVIOUS WORK

Work has been done in the field of image steganography and authors have proposed various algorithms:

A. Least significant bit substitution Method

The LSB is the lowest significant bit in the byte of each pixel in the image. This steganography embeds the secret information in the least significant bits of pixel values of the cover image. This type of embedding procedure is quite simple. It requires eight bytes of the pixels to store 1 byte of the secret data i.e. LSB. Rest of the bits in the pixels remains the same.

Suppose the first eight pixels of the original image have the following gray scale values: 11010010 01001010 10010111 10001100 00010101 01010111 00100110 01000011. The letter C whose binary value is 1000001. To hide this binary value it can replace the LSBs of these pixels to have the following new gray scale values: 11010011 01001010 10010110 10001100 00010100 01010110 00100111 01000011. In this example, the underlined LSB's of the pixel values has been changed. The difference between the cover (i.e. original) image and the stego image is difficult to observe by human eye.

Many algorithms have been proposed in the literature based on LSB. Although LSB substitution is the simplest steganography approach so far but it is not efficient in terms of security as it is predictable. A very well-known LSB approach is presented in [8] and proposed an adaptive method based on inter pixel relationship. This approach produces very attractive results but its retrieval is very easy by applying retrieval method. There is no need of any secret information or key before retrieval. This makes it vulnerable to attacks. Another efficient approach is presented in [9] which used neighbourhood information to calculate the amount of data that can be hidden in pixels of cover image. In this approach, some pixels are overloaded with data while some pixels remain unchanged. In this approach also, secret information can be easily retrieved easily. There is another efficient approach presented in [10] in which secret key is used only to decide whether the secret information bits will be hidden in green or blue. After deciding this, secret information bits hides in LSB of either blue or green. Although, this approach initially promises security but after that hiding secret bits in LSB is again not secure and secret data can be extracted after putting some effort.

The major limitation of LSB is small size of data which can be embedded in such type of images using only LSB. The LSB is extremely vulnerable to attacks.

B. Pixel Value Differencing Method

In this method, the secret data is embedding in the cover image. The cover image pixels and secret data is given. To hide the data by PVD, the difference value d_i is calculated from the two consecutive pixel values p_i and p_{i+1} i.e. $d_i = p_i + p_{i+1}$. Then the various ranges is defined for 0-255 value such that R_i $[l_i, u_i]$ and $l_i<d_i<u_i$. Then the width of the range is calculated whose logarithm will give the number of secret data bits(t) that will be hide in this range. Then a new difference value is calculated as $d'_i = b + l_i$, where b is the decimal value of t bits of secret data.

The pixel value p_i and p_{i+1} can be modified as:

$$(p'_i, p'_{i+1}) = \begin{cases} p_i + \left[\frac{m}{2}\right], p_{i+1} - \left[\frac{m}{2}\right], if\ p_i \geq p_{i+1} and\ d'_i > d_i \\ p_i - \left[\frac{m}{2}\right], p_{i+1} + \left[\frac{m}{2}\right], if\ p_i < p_{i+1} and\ d'_i > d_i \\ p_i - \left[\frac{m}{2}\right], p_{i+1} + \left[\frac{m}{2}\right], if\ p_i \geq p_{i+1} and\ d'_i \leq d_i \\ p_i + \left[\frac{m}{2}\right], p_{i+1} - \left[\frac{m}{2}\right], if\ p_i < p_{i+1} and\ d'_i \leq d_i \end{cases}$$

Where $m = |di' - di|$

All the pixel values according to the difference value are set and hence the secret data is embedded. The pixel value differencing method is proposed previously by using different approaches.

Wu and Tsai [11] proposed a steganographic scheme for gray level images in 2002 to improve the quality of the stego-image, which utilized the Human Visual System sensitivity to intensity variations from smoothness to high contrast by the selection of the width of the range which the difference value of two neighbour pixels belongs to. Mandal and Das [12] proposed a method which improves the visual quality of the PVD method. It also estimate the falling off problem.PVD issued for secret data embedding for each component(Red, Green and Blue) separately. Variable number of bits are embedded in each pixel for proving the secured transmission. Himakshi et al. [13] provide the another steganographic method which is based on the pixel value differencing scheme discussed in [11] and [12]. The data is embedded in this method by embedding the secret message in odd pixel pairs and the additional details were stored in even pixel pair. This method improved the image quality and also the compression ratio. Han ling et al. [14] proposed a method for steganography which uses the largest pixel value between the other three pixels close to target pixel to estimate the no of bits that can be embedded in that target pixel. The method enhances the image quality and increased embedding capacity.

C. Pixel Value sum Differencing Method

In this method, the sum s_i of the two consecutive pixel values is calculated. If $s_i > 255$, then the embedding is done using Pixel Value Differencing. For $s_i < 255$, the range of s_i is searched such that r_i $[l_i,u_i]$ in the same manner as in PVD, the number of t secret bits can be obtained using formula-log(w)+1. And then transform t bits of secret data into decimal value b. The new sum value is calculated using $s'_i = l_i + b$.

The pixel values p_i and p_{i+1} can be modified as:

$$(p'_i, p'_{i+1}) = \begin{cases} p_i + \left\lceil \frac{m}{2} \right\rceil, p_{i+1} + \left\lceil \frac{m}{2} \right\rceil, if\ s'_i > s_i \\ p_i - \left\lceil \frac{m}{2} \right\rceil, p_{i+1} - \left\lceil \frac{m}{2} \right\rceil, if\ s'_i < s_i \end{cases}$$

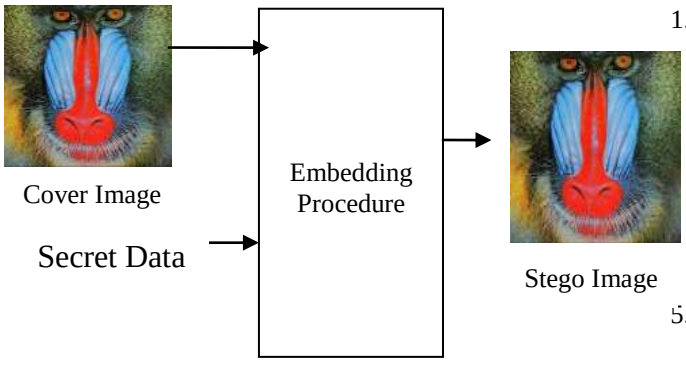
$$m = |s'_i - s_i|$$

III. METHODOLOGY

The method is based on pixel value differencing and pixel value sum [6]. It is modified to give a highly secured and high capacity data as in PVD.

An image baboon.jpg as in fig1 is a cover image that embed the text stream. A stego image is sent to the receiver having information and finally the text message is extracted from the stego image as illustrated below.

At Sender,



At Reciever,

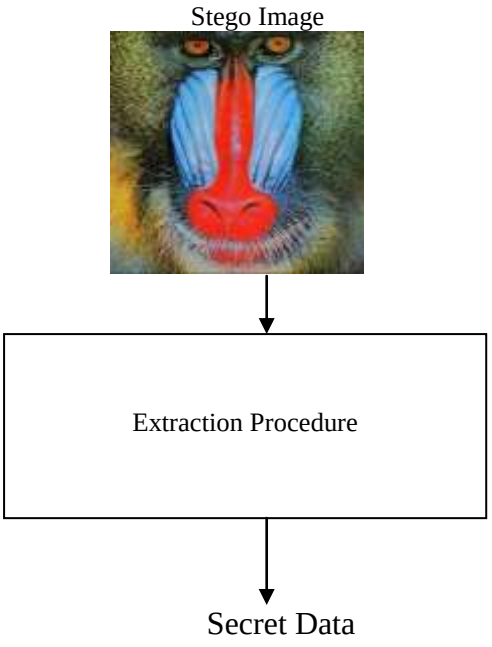


Fig. 1 Illustration of Steganography

A. Data Embedding

1. Read the cover image and partition it into non-overlapping blocks of two consecutive pixels.
2. Insert the secret key by XORing the LSB with the 7th bit in each pixel.
3. Determine the capacity of pixels in the image.
4. If there is a match i.e. the XOR value is 0. Embed the n bits of secret message directly using Pixel value sum and Differencing.
5. Otherwise data is inverted before embedding.
6. Repeat the procedure until all the secret data bits is embedded.
7. Data is written in the form of image file to obtain a Stego-image.

B. Data Extraction

1. Open the stego-image and again partition it into non-overlapping blocks of two consecutive pixels.

   Apply the secret key.

   XOR the LSB with 7th bit of each pixel.

   If the XOR value is 0. Extract the n bits of the secret data directly.

5. Otherwise the data is first extracted and the reverse of the string is done in order get the correct data.
6. Repeat the procedure until all the bits of the secret data are extracted.

IV. RESULTS

To evaluate the performance of proposed method an image of Taj of size 256 X 256 is taken as cover image as age shown in Fig. 2. The secret data stream is generated randomly. Firstly the proposed method is applied on the gray image and then on the colored image. The algorithm is tested for the visual distortion and capacity of the cover image.

RGB GRAY SCALE

Fig. 2 Cover Image

The cover image distortion produced due to secret data embedding can be measured in terms of Mean Square Error and Peak Signal to Noise Ratio.

These are defined as:

$$MSE = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[I_1(i,j) - I_2(i,j)]^2$$

$$PSNR = 10\ log_{10}(\frac{m*n}{MSE})$$

Where I_1 and I_2 in the MSE equation are the pixel values in the cover and stego image respectively and m, n are the dimensions of the cover image along the horizontal and vertical axes. The MSE value for RGB images is calculated for each colour plane of the image and then the average of the MSE of all the planes gives the Mean Squared Error between Cover and stego image.

Capacity is another parameter. It is the size of the data in a cover image. Capacity depends on the total number of bits per pixel and the number of bits embedded in each pixel of the image. Capacity is represented by bits per pixel (bpp).

The experimental data presented in Table1 and 2 indicate the Capacity and PSNR respectively of image for proposed scheme. The aforesaid table also provide comperative data for the other methods.

Table 1. CAPACITY

Image	Proposed Scheme	PVD and PVS	PVD
RGB	432524	432524	350899
Gray scale	138700	138700	117183

Table 2.PSNR

Image	Proposed Scheme	PVD and PVS	PVD
RGB	40.5684	43.6898	49.2001
Gray scale	25.1795	25.1795	49.1696

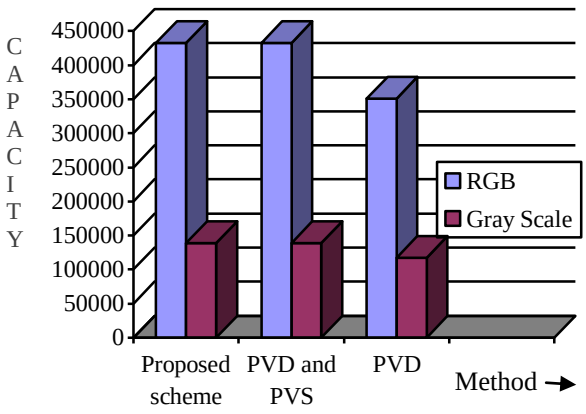


Fig. 3 Variation in Capacity

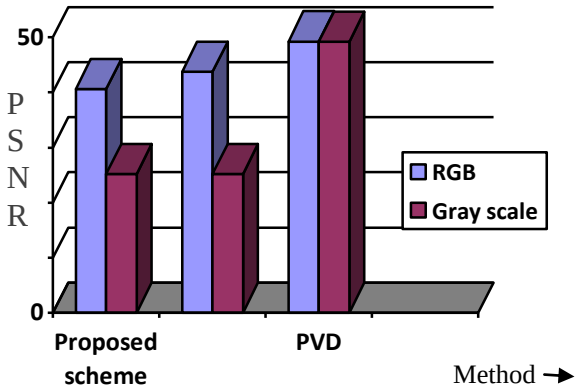


Fig. 4 Variation in PSNR

RGB GRAY SCALE

Fig. 5 Stego Image

The stego image is obtained from cover image by embedding secret data stream to it. The secret key is also used for the secured transmission of the message to protect it from intruders attack. Stego images corresponding to the cover images is shown in Fig. 5. The images look similar and are imperceptible to human eye.

V. Conclusion

In this paper, a technique for image steganography have been studied. This technique utilizes the sum or difference values for a particular pixel along with the secret key for better security. By the experimental results it has been concluded that the proposed method has good capacity and good visual fidelity. The PSNR value and capacity is compared for different techniques discussed in this paper. The secret key is required to keep the privacy of the data. The low PSNR value of the image does not change the visuality of the image and also by seeing the image intruder will not get to know the presence of some useful information. A trade off between these three terms is required while selecting a steganographic scheme.

References

[1] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6, pp. 57-68, December 2012.

[2] Liping Ji, Xiaolong Li, Bin Yang and Zhihong Liu, " A further study on a PVD-based steganography," Proceeding of IEEE conference 2010.

[3] Chin-ChenChanga ,Ju-YuanHsiaob and Chi-ShiangChana "Finding optimal least-significant-bit substitution in image

hiding by dynamic programming strategy" Pattern Recognition Society, Published by Elsevier Science,2002.

[4] Champakamala, B.S, Padmini.K and Radhika DK "Least Significant Bit algorithm for image steganography" IJACT Vol 3, No. 4, pp. 34-38, 2011.

[5] V. S. Shirguppi, "A Novel Approach for hiding data in Image Steganography by using Three Pixel Pair Differencing Method", International Journal of Advanced Research in Electronics and Communication Engineering , Vol. 4(12), pp. 2886-89, 2015.

[6] A. Tyagi, R. Roy, S. Changder, "High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum," Proceeding of IEEE, 2015.

[7] Ankita Sancheti "Pixel Value Differencing Image Steganography Using Secret Key" IJITEE, Vol. 2(1), Dec. 2012.

[8] Na-I Wu, "A Study on Data Hiding/or Gray-Level and Binary Images."

[9] M. Hossain, SA Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation", Proceedings of International Conference on Computer and Information Technology , Bangladesh, 2009.

[10] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography Using Secret Key", Proceedings of 14th International Conference on Computer and InformationTechnology, Bangladesh, 2011.

[11] Da-Chun Wu , Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing" Pattern Recognition Society, Published by Elsevier Science,pp. 1613-26, 2003.

[12] J . K. Mandal and Debashis Das "Colour Image Steganography Based On Pixel Value Differencing In Spatial Domain" IJIST Vol.2, No.4, July 2012.

[13] Himakshi, Verma,H.K., Singh, R.K., Singh,C.K., " Bi-Directional pixel-value differencing approach for RGB Color Image.",Proceeding of IEEE, 2013.

[14] Han-ling Zhang , Guang-zhi Geng and Cai-qiong Xiong " Image Steganography using Pixel-Value Differencing" Second International Symposium on Electronic Commerce and Security ,IEEE, 2009.