# A High Capacity Steganographic Technique based on LSB and PVD Modulus Methods

Manjunath Gadiparthi
Associate Professor & Head,
CSE, JNIT
Hyderabad, India

Keshav Sagar
08BAIA0513, B.Tech,
CSE, JNIT
Hyderabad, India

Divya Sahukari
08BAIA0505, B.Tech,
CSE, JNIT
Hyderabad, India

Rakesh Chowdary
08BAIA0528, B.Tech,
CSE, JNIT
Hyderabad, India

## ABSTRACT
Though many novel image steganographic techniques have been proposed in the recent years, PVD modulus method produces high quality stego images, when compared with other methods. But a significant drawback of PVD modulus method is low capacity. The hiding capacity is extremely low in PVD modulus method, when compared with other methods like LSB, etc. The reason for the low hiding capacity is that, with PVD modulus method we divide the pixel blocks in to smooth blocks where, the pixel value difference is low and edge blocks where the pixel value difference is high. In this paper, we propose a technique, which is a combination of PVD modulus and LSB method. As per the experimental results hiding capacity increases enormously.

## Keywords
Steganography, LSB Method, PVD Modulus Method.

## 1. INTRODUCTION
The term steganography is derived from the Greek language and means covert writing. Steganography is defined as the practice of undetectably altering a Work to embed a secret message. "Steganography is defined as the practice of undetectably altering a Work to embed a secret message".[2].

Many steganographic methods have been proposed to hide secret data into an image. The most common method is called least-significant-bits (LSB), which utilizes some least bits of pixels in the cover image to embed secret data[7] . Wang et al. proposed a method of exhaustive least significant- bit substitution to improve the security and the quality of the stego-image[8] . Furthermore, Chang et al. proposed an efficient method of dynamic programming strategy[9]. According to the characteristics of the human visual system, embedding the variable sizes of the LSBs was presented in [10]. Fu and Au proposed some data hiding methods for halftone images that not only can embed a large amount of secret data but also maintain good visual image quality[11] . To raise the capacity of hiding, and to ensure more security,better quality of stego-image for embedding data into binary image is presented in[12,13]. Wu and Tsai[14]utilized the difference between the two consecutive pixels in the cover image to determine what size the secret message is to be hidden. And their method provided the stego-image has an imperceptible quality. From the above-mentioned various methods we can evaluate a steganographic technique by two benchmarks the secret message capacity of hiding and the quality of the stego-image. In general, if we can embed a great deal of secret data into a cover image and maintain a high similarity between the cover image and the stego-image, it will not be easily suspected by illegal users when carrying out the process of the information delivered. Wu and Tsai,s scheme possesses both high capacity of secret data and high quality of the stego-image. Nevertheless, we consider it can embed much greater amounts of secret data, if the high quality of the stego-image is disregarded. In Wu and Tsai's method, a pixel-value differencing (PVD) method is used to discriminate between edged areas and smooth areas. The capacity of hidden data in edged areas is higher than that of smooth areas. A better method which produces high quality stego images has been proposed by C.M.Wang et –al. [15], called PVD modulus method. Though the quality of stego-image in this method is superior to the Wu and Tsai's scheme, nevertheless the hiding capacity is same in both the methods. So we present a method that can hide double the capacity of the secret and Valuable data in PVD modulus method with an acceptable quality of the stego-image.

## 2. REVIEW OF PVD MODULUS METHOD
In 2098 Wang et al. proposed a refined version of Wu and Tsai scheme, Pixel Value Differencing with Modulus function. In this method the modulus of two consecutive pixels is modified to embed the secret data instead of the difference of the pixel values. Instead of the difference value, the proposed scheme modifies the remainder of two consecutive pixels P(i,x) and P(i,y) for better stego-image quality. The proposed embedding and extracting algorithms are presented in the subsections below.

To determine the limitations and flexibility of available software, we evaluated several steganographic packages. Here we discuss only three: StegoDos, White Noise Storm, and S-Tools for Windows. For details on other tools, see the sidebar "For More Information." First, we selected message and cover files. In some cases, we had to alter the selected images to fit into the constraints of the software or had to use other cover images

First the given image is scanned in zigzag manner to obtain the pixels. Blocks of two consecutive pixels are obtained.Given a sub-block Fi composed of two continuous pixels P (i,x) and P(i,y) from the cover image, obtain the difference value di, the sub-range Rj such that Rj belongs to [lj,uj], the width

wj = uj - lj + 1, the hiding capacity ti bits, and the decimal value v of ti for each Fi.

The remainder values Prem(i,x), Prem(i,y) and F*rem(i)* of P(i,x), P(i,y) and sub-block Fi are computed respectively by using the Following equations:

Prem(i,x) = P(i,x) mod v

Prem(i,y) = P(i,y) mod v

Frem(i) = (P(i,x) + P(i,y)) mod v

where v is the width of the suitable range.

**t**i bits of secret data are embedded into sub block

Fi by altering P(i,x) and P(i,y) such that. Frem(i) = v .

The optimal approach to altering the P(i,x) and P(i,y) to achieve the minimum distortion is as follows:

Case1:

$$F_{rem(i)} > v \text{ and } m \le \frac{2^{t_1}}{2} \text{ and } p_{(i,x)} \ge p_{(i,y)}$$

$$p^*_{(i,x)} = p_{(i,x)} - \left\lceil \frac{m}{2} \right\rceil \quad p^*_{(i,y)} = p_{(i,y)} - \left\lfloor \frac{m}{2} \right\rfloor$$

Case 2:

$$F_{rem(i)} > v \text{ and } m \le \frac{2^{t_1}}{2} \text{ and } p_{(i,x)} \le p_{(i,y)}$$

$$p^*_{(i,x)} = p_{(i,x)} - \left\lfloor \frac{m}{2} \right\rfloor \quad p^*_{(i,y)} = p_{(i,y)} - \left\lceil \frac{m}{2} \right\rceil$$

Case 3:

$$F_{rem(i)} > v \text{ and } m > \frac{2^{t_1}}{2} \text{ and } p_{(i,x)} \ge p_{(i,y)}$$

$$p^*_{(i,x)} = p_{(i,x)} + \left\lfloor \frac{m_1}{2} \right\rfloor \quad p^*_{(i,y)} = p_{(i,y)} + \left\lceil \frac{m_1}{2} \right\rceil$$

Case 4:

$$F_{rem(i)} > v \text{ and } m > \frac{2^{t_1}}{2} \text{ and } p_{(i,x)} < p_{(i,y)}$$

$$p^*_{(i,x)} = p_{(i,x)} + \left\lceil \frac{m_1}{2} \right\rceil \quad p^*_{(i,y)} = p_{(i,y)} + \left\lfloor \frac{m_1}{2} \right\rfloor$$

Case 5:

$$F_{rem(i)} \le v \text{ and } m \le \frac{2^{t_1}}{2} \text{ and } p_{(i,x)} \ge p_{(i,y)}$$

$$p^*_{(i,x)} = p_{(i,x)} + \left\lfloor \frac{m}{2} \right\rfloor \quad p^*_{(i,y)} = p_{(i,y)} + \left\lceil \frac{m}{2} \right\rceil$$

Case 6:

$$F_{rem(i)} \le v \text{ and } m \le \frac{2^{t_1}}{2} \text{ and } p_{(i,x)} < p_{(i,y)}$$

$$p^*_{(i,x)} = p_{(i,x)} + \left\lceil \frac{m}{2} \right\rceil \quad p^*_{(i,y)} = p_{(i,y)} + \left\lfloor \frac{m}{2} \right\rfloor$$

## 3. PROPOSED METHOD

Low hiding capacity in PVD modulus method owes to mainly hiding in smooth areas. For example if pixel value difference is 3, if the corresponding range width is 8, only 3 bits can be embedded in a pair of pixels. Where as in 3-bit LSB replacement method 6 bits can be embedded. In our method we aim to use LSB method for smooth areas and PVD modulus method for edge area pixel pairs. We define a threshold to determine whether a pixel pair falls in smooth area or edge area.

### 3.1. Embedding Algorithm

The embedding algorithm takes the following steps.

*Step 1:* Calculate the Pixel value difference of pixel pair

$$D = \left| p_{(i,y)} - p_{(i,y)} \right|$$

Step 2: If the d <= threshold, LSB replacement method. Else use PVD modulus method which was discussed in previous section.

#### *3.1.1 LSB replacement Method:*

Convert the pixel value in to a number binary and replace the three least significant bits by the bits of secret data. So six bits can hidden in a pair of two pixels.

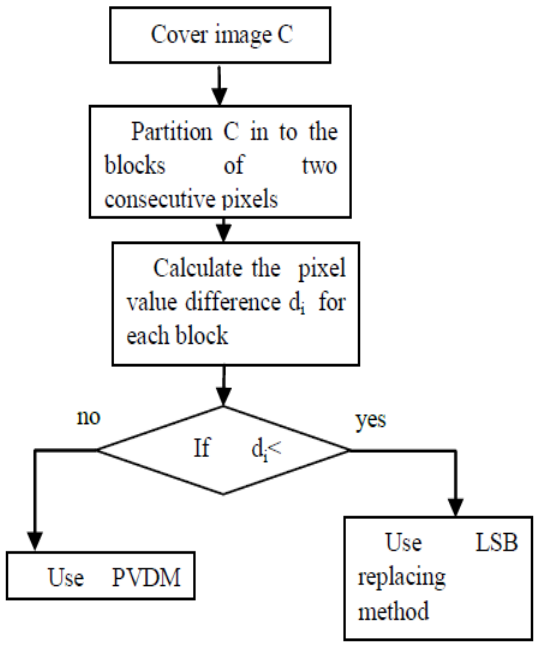


Fig 1: Block diagram of proposed method.

## 3.2 Extraction Algorithm

Consider a Stego image pixel pair.

***Step1****:* Calculate the pixel value difference of the pair under consideration.

***Step2****:* If the difference value is less than are equal to the threshold LSB method is applied. So the secret data is the three least significant bits of both the pixels.( 6 bits)

***Step3****:* If the difference is greater than the threshold, PVD modulus method is employed. Locate suitable range for that difference from the range table. From the width of the range table number of bits embedded can be determined.

$$N = \log_2 |widthofrange|$$

***Step4****:* Calculate Frem(i) = (P(i,x) + P(i,y)) mod v

Where v is the width of the suitable range in which the difference falls. This Frem(i) is the decimal value of the secret data. Express it in binary bits (the number of bits is computed from width of the range).

## 4. EXPERIMENTAL RESULTS AND ANALYSIS

A stegonagraphic method can be evaluated by the amount of data that can be hidden (hiding capacity) and the quality of stego-image. Quality of stego-image is expressed in terms of PSNR (Peak Signal-to-Noise Ratio). PSNR in decibels (dB) is computed by using

$$PNSR = 10 \log_2 \frac{225}{MSE}$$

$$\text{Where } MSE = \frac{\sum f(i,j) - F(i,j)^2}{N^2}$$

It is assumed that we are given a source image f(i,j) that contains N x N pixels and a reconstructed image F(i,j) where F is reconstructed by decoding the encoded version of cover image.

The following table shows the comparison of PVD Modulus method and proposed method, in terms hiding capacity in bits.

TABLE 1: HIDING CAPACITY

| | PVD mod | Proposed | %increase |
|---|---|---|---|
| Baboon | 717585 | 457296 | 57 |
| Couple | 762352 | 412832 | 85 |
| Elaine | 775765 | 400168 | 94 |
| Jet | 769597 | 410408 | 88 |
| Leena | 765874 | 409864 | 87 |
| Man | 746116 | 431520 | 73 |

Above results show that, though PSNR value decreases in the proposed method, still the stego images are of acceptable quality as PSNR value is above 35 dB. The following figure shows the stego images produced by the PVD modulus method and the proposed methods. Pvdm method Proposed methods.

a) Elaine

B) Jet

c) Man

d) Couple

Fig2: Stego images

## 5. CONCLUSION

The proposed method, which is a combination of PVD modulus and LSB replacement methods produces images with acceptable quality and embeds more data in to the cover image than the PVD modulus method.

## 6. REFERENCES

[1] Johnson, N. and Jajodia, S. Exploring steganography: Seeing the unseen, IEEE Computers. Vol.31, 1998, pp.26–34.

[2] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, Digital Watermarking and Steganography 2nd Edition, Morgan Kaufmann Publishers, 2008.

[3] Nan-I Wu and Min-Shiang Hwang, Data Hiding: Current Status and Key Issues, International Journal of Network Security, Vol.4, No.1, 2007 PP.1–9

[4] C.-C. Chang and W.-C. Wu, Hiding secret data adaptively in vector quantization index tables, IEEE Proceedings -Vison and Image Signal Processing, Vol. 153, 2006, pp.589-597

[5] Artz, D., Digital Steganography: Hiding Data within Data, IEEE Internet Computing Journal, June2001

[6] Bao, P., and Ma, X.: Image adaptive watermarking using wavelet domain singular value decomposition, IEEE Trans. Circuits Syst. Video Technol., vol.15, 2005, pp. 96–102

[7] Walton, S,Image authentication for a slippery new age, Dr. Dobbs J., 1995, 20, (4), pp. 18–26

[8] Wang, R.Z., Lin, C.F., and Lin, J.C.: Image hiding by optimal LSB substitution and genetic algorithm‟, Pattern Recognition., 2001, 34, (3),pp. 671–683

[9] Chang, C.C., Hsiao, J.Y., and Chan, C.S.: „Finding optimal least significant- bit substitution in image hiding by dynamic programming strategy‟ , Pattern Recognition., 2003, 36, (7), pp. 1583–1595

[10] Lee, Y.K., and Chen, L.H.: „High capacity steganographic model, IEE Proc., Vis. Image Signal Process., 2000, 147, (3), pp. 288–294

[11] Fu, M.S., and Au, O.C.: „Data hiding watermarking for halftone images‟ , IEEE Trans. Image Process., 2002, [12] Tseng, Y.C., Chen, Y.Y., and Pan, H.K.: „A secure data hiding scheme for binary images, IEEE Trans. Commun., 2002, 50, pp. 1227–123.

## 7. AUTHORS PROFILE

**Manjunath Gadiparthi** is working as an Associate Professor and Head Department of Computer Science in JAWAHARLAL NEHRU INSTITUTE OF TECHNOLOGY (JNIT). He received his B.Tech Degree in Computer Science & Engineering from Narasaraopeta Engineering College Andhra Pradesh. He received his M.Tech Degree in Computer Science & Engineering from RVR & JC College of Engineering

**Mr Keshav Sagar** was born in 1990 in Hyderabad and is presently pursuing his B.tech 4th yr in CSE stream from JAWAHARLAL NEHRU INSTITUTE OF TECHNOLOGY. He has been an intelligent student who believes that practical knowledge is more important than theoretical knowledge. His aim is to become a software professional

**Ms Divya Sahukari** was born in 1991 in Hyderabad and is presently pursuing her Btech 4th year in CSE stream from JAWAHARLAL NEHRU INSTITUTE OF TECHNOLOGY. She has been outstanding in her studies throughout her career who believes that hardwork never fails and her aim is to become an software engineer

**Mr Rakesh Chowdary** was born in 1990 in Hyderabad and is presently pursuing his Btech 4th year in JAWAHARLAL NEHRU ISTITUTE OS TECHNOLOGY in CSE stream.He has been a genious since childhood who has exceptional knowledge and his aim is to become a software engineer