A Modified Pixel-Value Differencing Image Steganographic Scheme with Least Significant Bit Substitution Method

Aruna Malik, Geeta Sikka and Harsh Kumar Verma

Department of Computer Science & Engineering, National Institute of Technology, Jalandhar, Punjab, India E-mail: arunacsrke@gmail.com, sikkag@nitj.ac.in, vermah@nitj.ac.in

Abstract—Pixel value differencing is a steganographic technique for gray scaled images. In this paper, we propose a modified pixel value differencing image steganographic scheme with least significant bit substitution method. Our method divides the cover image into the blocks of two consecutive pixels and calculates the absolute difference between the pixels of a block similar to [1, 2]. If the difference is less than a particular threshold, i.e. 15 (in this paper) than 4 bits of secret data are taken and these bits are embedded onto the LSBs of the block's pixels through least significant bit substitution method otherwise the number of bits to be hidden are selected based on some characteristics of the block and hidden. The experimental results show that our method significantly improves the quality of stego image as compared to the [1, 3] and have sufficient payload.

Index Terms—Pixel value differencing, least significant bit, cover image, stego image, peak signal-to-noise ratio.

I. INTRODUCTION

Today, a lot of communication is being done on the internet because it is very convenient for the people being at different places to exchange their views. However, the security has been a major concern because anyone can have access to the data on the internet while being transferred. So, to improve the security, there are mainly two types of technique: cryptography and steganography. Cryptography techniques encode the data in such a way that it can't be read unauthorized person, though data is visible, whereas steganography techniques hides the data into another media so that its existence can't be sensed by unauthorized persons. In today's world, it has many applications like digital copyrights, online transactions and military communication.

The word steganography is a combination of two Greek words *stegano* and *graphy*. The word *stegano* means secret and *graphy* refers to writing hence steganography refers to secret writing. The generic working of the steganography technique is shown in Fig.1. There have been discussed many approaches in literature for hiding secret data into the cover media. Based on the way of embedding secret data these can be divided into two categories as (a) Spatial domain embedding and b) Transform domain embedding.



Fig. 1. Steganography Technique

In spatial domain embedding approach, the secret message is embedded into the intensity of the pixels of the cover image directly, whereas in transform domain the secret message is embedded into the coefficient of the transformed image of frequency domain [1]. Our steganography method lies into the spatial domain based method.

A good steganographic method should possess following three main properties:

Capacity- The amount of the secret data to be embedded without degrading the quality of the cover image.

Robustness- Resistance for probable alteration.

Invisibility- Existence of the secret data must not perceptible by anybody except the receiver.

In this work, the original pixel value differencing scheme is modified so that the quality metrics i.e., hiding capacity and peak signal to noise ratio can be significantly improved.

The rest of the paper is organized as follows. Section II discusses the related work, section III discusses the original PVD method, Section IV discusses the quality metrics, section V introduces the proposed work and in section VI, experimental results are discussed. Finally in section VII, the paper is concluded.

RELATED WORK

One of the most widely used steganography method is least significant bit (LSB) substitution method [4]. In this technique, secret message is embedded onto the LSBs of the elements of the cover media. The number of LSBs used to hide the secret data is determined by the length of the secret data because of the quality of the stego-media after hiding the secret data is directly influenced by the LSBs used. So, the number of LSBs used to hide the secret data in simple LSB substitution method are kept as minimum as possible. This is one of the simplest approaches in data hiding. To overcome the shortcoming of simple LSB substitution method, Optimum Pixel Adjustment Procedure (OPAP) [5] is introduced by Chan & Cheng. It minimizes the distortion in the stego-image caused due to simple LSB substitution. The OPAP adjusts the elements value after hiding the secret message, to improve the cover media quality without altering the bits of the secret data. The OPAP gives better quality cover media, however, when the number of LSBs used to hide the secret data are large, it requires a lot of computation for embedding as well as for extraction.

introduced Amirtharajan [6] an important steganographic method which breaks the cover image into blocks of fixed size and also divide the secret message into segments. One segment of the secret message is selected and embedded onto a block of image and the mean square error is computed. The bits of that segment of the secret message are flipped and further embedded onto that block of the cover image, MSE value is again computed. If the flipped bits secret message has smaller MSE, then the indicator mark is set as '1' and flipped bits secret message is embedded; otherwise the original message is embedded and the indicator mark is set as '0'. This process is repeated for each segment of the secret message. This method provides better quality stego image but suffers from capacity point of view. Another method based on simple LSB substitution was given by Ghosal [7] which calculates difference between the number of 1s and number of 0s of each pixel/element of red component of the image. The computed difference is divided by 2 i.e., the number of remaining channels in case of 24 bit colored image as it has three channels: red, green and blue and the resultant value's equal number of bits of the secret data are embedded in the LSBs of the blue and green channel. This method achieves good quality as well as provides good secret data hiding capacity but from the security point of view, this method is very vulnerable because the secret data is directly embedded into the pixels of blue and green channel.

Khalaf [8] discusses a steganographic method based on LSB substitution. It utilizes first two least significant bits of the pixels of cover image. This method divides or organize the secret message into a two segments: even segment and odd segment. In an even segment the elements of the even positions are placed; and in odd segment, odd position elements are placed. The channels of the color image i.e., 24 bit are also named as index channel, channel-1 and channel-2 as per the choice. Both the channel-1 and the channel-2 are used to hide the secret data and the remaining channel i.e., index channel is used as an indicator channel. The number of 1's in each pixel of the indicator channel is calculated; if it is even, a couple of bits are embedded in the corresponding pixels of channel-1 and channel-2, each taken from the even segment of the secret data. In case the number of 1s is odd, 4 bits from the odd segment are embedded in channel-1 and channel-2 equally. The stego-image quality of this method is good. However, it suffers from the low hiding capacity of the secret data.

The Selected LSB (SLSB) algorithm discussed in [9] embeds secret data into a single color component of the pixels of the cover image. It does not only embed into the LSBs but also selects the color component and the alterable bits of the color component in such a manner that will produce the minimum distortion. It falls in the class of the filtering algorithms as it employs a sample pair analysis filter prior to embedding, to make sure that the only best candidate pixels are chosen for embedding. It embeds at a rate of more than 1 bit per pixels. However, the algorithm suffers from the security point of view because of the alteration of the degree of randomness of the pixels of the image which results into a susceptible image to statistical attacks when used for high degree of embedding. In such types of schemes, characteristics of human visual system have not been explored.

Kekre et al. [10] discuss a steganographic method in which, a secret key of one byte is chosen and it is XORed with all the bytes of the secret message. Each pixel of the cover image is processed for hiding bits from the resultant XORed secret message. For all the pixels of the cover image having value greater than 239; if the bit to be embedded is 1, 5 bits of the resultant secret data are embedded and for embedding bit 0; 4 bits are embedded in LSBs of that pixel. For a pixel having intensity in the range of 224 to 239; if bit to be concealed is 0, 5 bits from the resultant secret data are embedded and for bit 1, 3 bits are embedded. For a pixel having intensity from 192 to 223, 2 bits are embedded otherwise only one bit is embedded in LSB of that pixel. A matrix of pixels whenever 5 bits of the resultant secret data are hidden is maintained. This matrix helps at the time of extraction of the secret data from stego-image. Hence, this method provides decent quality stego-image with a good data hiding capacity. However, the capacity may remain low if there are more low intensity pixels in the cover image. Hussain [11] discusses a method that is an extension of MKA [10]. This method utilizes all the bytes of the cover image. It actually embeds more secret data bits than the MKA into low intensity pixels which satisfy some predefined conditions. A matrix entry is also maintained when 5, 3 or 2 bits of secret data is hidden. This method increases the data hiding capacity to a great extent, but the complete data hiding procedure takes a lot of time when a large amount of the secret data is hidden.

Wu & Tsai [12] discuss Pixel Value Differencing (PVD) scheme which is inspired by the functioning of the human visual system. In this scheme, a range table with a number of contiguous ranges is built and the original

cover image is partitioned into non-overlapping blocks of 2 pixels each. The width of each range in the table is kept in power of 2. Now, the difference of two consecutive pixels of a block is calculated. The block with grater difference value is assumed in the edge area otherwise it is assumed in the smooth area where the small or large values are taken based on some pre-defined threshold value. According to the human visual system, the human eyes are more sensitive to noise in smooth areas than in the edge area. So, this method hides more bits in edge areas, in contrast to smooth areas. In this method, the stego image quality is improved a lot but data hiding capacity is not. Another important method [13] which also exploits the characteristics of the human visual system and makes use of both pixel value differencing (PVD) and least significant bit (LSB) substitution scheme is discussed. In this method, the image is also partitioned into non-overlapping blocks of two consecutive pixels and then the difference value is computed for each block in a similar way as in [12]. On the basis of the difference value, each block is recognized either as a part of smooth region or edge region. This method conceals more secret data bits into the smooth regions by simple LSB substitution method and for edge area the Wu & Tsai's scheme [12] is utilized. Thus, it maximizes the data hiding capacity to a great extent even without disturbing the image quality much. The method discussed in [12, 13] identify the horizontal edges only. However, these methods do not perform to the expectations.

The shortcomings of [12, 13] have been overcome in the Try-Way PVD [14, 15]. This method partitions the image into the blocks of 2×2 pixels and the pixels are arranged in pairs as {top left, top right}, {top left, bottom left} and {top left, bottom right}. The difference is computed between each and every pair of the block, because the possible edge can be vertically, horizontally, or diagonally and more secret data bits are embedded into these pairs. Hence, this method achieves very good quality and also have sufficient payload. In our proposed method, we modify the pixel value differencing scheme in such a way that the caused distortion is reduced and the hiding capacity is increased.

III. REVIEW OF WU & TSAI METHOD (ORIGINAL PVD METHOD)

Wu & Tsai's PVD method is actually inspired by the functioning of the human visual system. This technique hides more secret data bits into the edge area than the smooth area. In this method, a range table with contiguous ranges is designed to fabricate all the ranges. The range values in the range table vary in the range of 0-255 as the pixel intensity can be in the range of 0-255. The image is partitioned into the blocks of two consecutive pixels, namely PX_i and PX_j . The absolute difference value dv_1 is calculated between the pixels of the block. If the difference value is larger than a particular threshold, then the block is considered in the edge area otherwise belongs to smooth area. The logarithmic with base 2 of the difference of upper bound

 ub_k and lower bound lb_k of the range are the number of bits selected from the secret data file. The decimal representation of the selected secret data bits is stored into the decval. A new difference is calculated as $dv_2 = lb_k$ + *decval*. The actual value to be hidden represented by dvis calculated by subtracting dv_2 from dv_1 and half of the dv value is adjusted with PX_i and the remaining half is adjusted with pixel PX_j .

The step wise step procedure of Wu & Tsai scheme is explained below

- 1. Partition the image into the groups of two consecutive pixels stated as PX_i and PX_j horizontally and design a range table with contiguous ranges having width of each range in 2^n where $n \in \{1, 2, 3, ..., n\}$.
- 2. Calculate the difference between the pixels |dv1|=PXi-PXj.
- 3. Select the optimal range Rk from range table such as $ubk \ge |dv1|$ and $|dv1| \ge |bk|$ where ubk, lbk are the upper and lower bound of the range Rk and k $\in \{1,6\}$.
- 4. Calculate the number of bits as n=log2(ubk-lbk+1).
- 5. Extract n number of bits from secret data and calculate their decimal value in decval.
- 6. Calculate the actual embedding value dv as dv = |dv1-dv2| where dv2 = lbk+decval.
- 7. Modify the pixel value PXi and PXj to NPXi and NPXj as follows.
 - $PX_i + ceil (dv / 2), PX_j floor (dv / 2) \text{ if } PX_i >= PX_i \&\& dv_2 >= dv_1$
 - PX_i floor (dv / 2), PX_j + ceil (dv / 2) if PX_i < PX_i && dv₂ > dv₁
 - PX_i ceil (dv / 2), PX_j + floor (dv / 2) if $PX_i >= PX_j \&\& dv_2 <= dv_1$
 - PX_i + ceil (dv / 2), PX_j floor (dv / 2) if PX_i < PX_j && dv₂ <= dv₁
- 8. Repeat the step II to VII for each group of the cover image or until secret data bits are not covered completely.

In the extracting phase of Wu & Tsai scheme the stego image is also partitioned into the groups of two consecutive pixels and difference value is calculates as $Ndv = NPX_i - NPX_j$ now optimal range R_k in which Ndvlying is selected and $d = Ndv - lb_k$ is calculated. The representation of the *d* in binary gives the secret data bits.

Table 1. Range Table

Range (R)	Lower bound (lb)	Upper bound (ub)
R ₁	0	15
R ₂	16	31
R ₃	32	63
R_4	64	127
R ₅	128	255

IV. PROPOSED METHOD

Our proposed method consists of two parts: embedding process and extraction process. These processes are discussed below.

A. Embedding Algorithm

Step 1. Partition the image into the groups of two consecutive pixels stated as PX_i and PX_j horizontally as in PVD scheme [1] and design the range table as Table-1.

Step 2. Calculate the difference between the pixels as $|dv_l|=PX_i-PX_j$ and select the range R_k from range table in which $|dv_l|$ is lying.

Step 3. If $|dv_1| \le 15$ then read 4 bits of secret data and embed these bits on the first 2 LSBs of both the pixels PX_i and PX_j . Now go to step-7.

Step 4. Else if $|dv_1| >= 3lb_k/2$ then

- Read the *n* secret data bits and get their decimal value as decval where $n = log_2(ub_k lb_k + 1) 1$.
- Calculate the actual embedding value as dv= |dv₁-dv₂|, where dv₂= 3lb_k/2-decval-1 and go to step-6

Step 5. Else get the decimal value (*decval*) of *n* secret data bits where $n = log_2(ub_k - lb_k + 1)$ and calculate actual embedding value dv as $dv = |dv_1 - dv_2|$ where $dv_2 = lb_k + decval$.

Step 6. Modify the pixel value PX_i and PX_j to NPX_i and NPX_i as follows.

- if $PXi \ge PXj$ && $dv_2 \ge dv_1$ then PX_i +ceil (dv/2), PX_i -floor(dv/2)
- Else if $PX_i < PX_j$ && $dv_2 > dv_1$ then $PX_i floor$ (dv/2), $PX_j + ceil(dv/2)$
- Elseif $PXi \ge PXj$ && $dv2 \le dv1$ then $PX_i ceil(dv/2, PX_i + floor(dv/2))$
- Else PX_i + ceil (dv/2), PX_i -floor (dv/2)

Step 7. Repeat the step 2 to 6 for each group of the cover image or until secret data bits are not covered completely.

B. Extraction Algorithm

Step 1. Divide the stego image into the blocks of two consecutive pixels.

Step 2. Get the difference dv of pixels NPX_i and NPX_j as $dv = /NPX_i - NPX_i/$.

Step 3. Select the range R_k in which dv lies. If dv <=15 then represent NPX_i and NPX_j in binary form and extract first two LSBs of both the pixels and go to step 6.

Step 4. Else if $dv > 3lb_k/2-1$ then the binary representation of $dv-3lb_k/2-1$ is the actual data embedded into the pixels.

Step 5. Else the binary representation of dv- lb_k is the actual embedded secret data bits.

Step 6. Repeat step 2-5 until the entire block are covered.

V. QUALITY METRICS

We have used two metrics namely PSNR and data hiding capacity to evaluate the performance of the proposed method.

Peak Signal to Noise Ratio (PSNR)

The Peak Signal to Noise Ratio (PSNR) is image quality metric which estimates the quality of stego-image with respect to the original image. It is a very commonly used metric way to estimate image reliability or conformity. The mathematical formula to compute the PSNR value is as follows:

$$PSNR = 20 log_{10} [\frac{MAXPIX}{MSE}]$$

Where MAXPIX is the maximum pixel intensity value and MSE is the Mean Square Error.

In PSNR, 'signal' refers to the original image and 'noise' refers to error in the stego-image. PSNR is a number which generally speaks about quality of the stego-image and is measured in decibel (dB). Mathematically, PSNR is inversely proportional to the MSE, which suggests that the lower the value of MSE higher is its PSNR. In other words, higher Peak Signal to Noise Ratio (PSNR) is better. The MSE is given by the following formula:

$$MSE = \frac{1}{M*N} \sum_{x=1}^{M} \sum_{y=1}^{N} [x(m, n) - y(m, n)]^{2}$$

Where, x and y are the cover and stego-images respectively of size MxN.

Hiding capacity

The number of bits of the secret data hidden into the pixels of the cover image is referred as the hiding capacity.

VI. EXPERIMENTAL RESULTS

In this section, we discuss the experimental results of our proposed steganography method. Most commonly used images in literature that include Lena, Pepper, Baboon, Airplane, Boat and Zelda as shown in Figs 2(a-e) respectively, are used to hide the secret data. The size of each image is 512x512 pixels. We have taken six images as the cover media for covering the maximum variance in the image characteristics. The secret data taken in our experiments is a random bit stream taken from the pseudo random number generator. We have implemented PVD [1], Tri-Way PVD [3] and our proposed scheme in MATLAB7.5 running on the Intel® Core 2 Duo 2.20 GHz CPU, and 3GB RAM hardware platform with Windows 7 operating system. We have taken two quality metrics: peak signal to noise ratio (PSNR) and hiding capacity, for comparing our scheme's results with the Pixel Value Differencing scheme [1] and Try-Way PVD method [3]. The maximum capacity is calculated in bytes. The stego images after hiding the secret data are shown in Fig. 4(a-e).

The performance comparison results are shown in Table II and Table III. It is clearly evident from Table II and Table III that our PSNR values are much better than [1] and [3] schemes and as far as embedding capacity is concerned, the amount of secret data embedded by our proposes method is also much more than PVD but less than the tri-way PVD. For the Baboon image which has a lot of noise, our scheme doesn't perform so well, but still providing better PSNR value than the [1, 3]. The reason of having higher capacity than the PVD [1] of our method is that we are able to embed more bits into the pixels of smooth area and nearly equal bits are embedded into edge area as well. In fact, we try to get advantages of the simple LSB substitution method in smooth areas because the LSB substitution method directly replaces the bits of cover image pixels with the secret data bits. The possibility of replacement of cover pixel bit by the same bit of the secret data are high that's why we are getting much higher PSNR value. In our method, we also minimize the actual data because of that the PSNR value is being positively affected.



Fig. 2. Flow chart of working of proposed embedding scheme

Table 2. Comparison Table of PSNR values (on maximum hiding capacity)

Cover Image	Wu & Tsai scheme [1]	Tri-Way PVD [3]	Proposed Scheme
Lena	41.7158	38.89	45.3473
Baboon	37.3995	33.93	39.5170
Pepper	41.7507	38.50	45.7514
Airplane	40.5694	39.54	44.5143
Boat	41.2547	38.20	45.2022
Zelda	41.3685	38.09	46.0210

Cover Image	Wu & Tsai scheme [1]	Tri-Way PVD [3]	Proposed Scheme
Lena	51219	75836	65541
Baboon	57146	82407	66658
Pepper	50907	75579	65545
Airplane	51545	75544	65734
Boat	50124	75124	65344
Zelda	51754	75687	65528

Table 3. Comparison Table of Hiding Capacity (in bytes)



Fig. 3(a) Lena



Fig. 3(c) Airplane



Fig. 3(b) Baboon



Fig. 3(d) Boat

Fig. 3. Cover images



Fig. 3(c) Pepper



Fig. 3(e) Zelda



Fig. 4(a) Lena



Fig. 4(c) Airplane



Fig. 4(b) Baboon



Fig. 4(d) Boat Fig. 4. Stego-images



Fig. 4(c) Pepper



Fig. 4(e) Zelda

V. CONCLUSIONS

In this paper, we modify the Pixel Value Differencing scheme proposed by Wu & Tsai. Our proposed method hides the secret data in smooth areas of the cover image by simple LSB substitution method because of that the hiding capacity is increased. However, while embedding in edge area, we modify the PVD scheme and hide the secret data using modified scheme. In the modification process, we actually try to minimize the actual embedded data into the pixels of the cover image because of this high PSNR value is achieved. This method does not require the original image while extracting the secret data from stego image similar to the Wu & Tsai scheme.

REFERENCES

- Da-Chun Wu, Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24,1613–1626, 2003.
- [2] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. "Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEEE Proc.-Vis. Image Signal Process., vol. 152, no. 5, October 2005.
- [3] 0Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu,: "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia," vol. 3, no. 2, 2008.
- [4] Chang, C. C., Chen, T.S and Chung, L. Z., "A steganographic method based upon JPEG and quantization table modification", Information Sciences, vol.4, pp. 123-138, 2002.
- [5] http://www.itacs.uow.edu.au/research/smicl/IVM/Digital watermarking_tutorial.htm.
- [6] DC. Wu, W-H. Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters 24 (2003) 1613–1626.
- [7] C-K. Chan, L-M. Chen, "Hiding data in images by simple LSB substitution", Pattern Recognition 37 (3) (2004) 469–474.
- [8] K-C. Chang, C-P. Chang, PS. Huang, and T-M. Tu ,: "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing", Journal of Multimedia, Vol. 3, no. 2, June 2008.
- [9] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. "Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, Oct 2005.
- [10] H. B. Kekre, A. Athawale, P. N. Halarnkar, "Performance Evaluation of Pixel Value Differencing and Kekre's Modified Algorithm for Information Hiding in Images", International Conference on Advances in Computing, Communication and Control, 2009 pp 342-346.
- [11] M. Hussain, M. Hussain., "Pixel Intensity Based High Capacity Data Embedding Method", Information and Emerging Technologies, International conference 978-1-4244-8003 June 2010.
- [12] W. Luo, F. Huang, J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme", Multimedia tools and applications, Vol 52, NO 2-3, PP-407-430, 2010.
- [13] V. Sabeti, S. Samavi, M. Mahdavi, and S. Shirani, "Steganalysis andpayload estimation of embedding in pixel differences using neural networks", Pattern Recognition Letters, Vol. 43, pp. 405-415,2009.

- [14] X. Zhang , S. Wang," Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security", Pattern Recognition Letters, Vol. 25, pp. 331-339, 2004.
- [15] Gulve Avinash K, Joshi Madhuri S,"An Image Steganography Algorithm with Five Pixel Pair Differencing and Gray Code Conversion", IJIGSP, vol.6, no.3, pp.12-20, 2014.

Authors' Profiles



Aruna Malik, received her B.Tech. in Computer Science and Engineering from Utter Pradesh Technical University, Lucknow, India and M.Tech. in Computer Science and Engineering from National Institute of Technology, Jalandhar, Punjab, India. She is pursuing her doctoral degree in Computer Science and Engineering, at

National Institute of Technology, Jalandhar, Punjab, India. Her research areas lie in the area of digital watermarking and image processing.



Geeta Sikka, received her Ph.D in the Department of Computer Science and Engineering, National Institute of Technology, Jalandhar, India. She did her Master's degree in Computer Science from Punjab Agricultural University, Ludhiana. She is presently working as Associate Professor in the Department of

Computer Science and Engineering at Dr. B. R. Ambedkar National Institute of Technology, Jalandhar. India. Her research interests are Software Engineering, Databases and Data mining.



Harsh K Verma, received the Ph.D in Numerical Computing from Punjab Technical University Punjab, India. He is currently a Professor in Computer Science and Engineering Department at Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India. His research interest includes in numerical computing,

information security and computer networks. He has published various papers in national and international journal and conferences. He has attended various national and international workshop training schools and other technical activity during his academic carrier.