Pixel Value Differencing a Steganographic method: A Survey

Jagruti Salunkhe
University of Pune
Marathwada MitraMandals
College of Engineering, Pune

Sumedha Sirsikar
University of Pune
Maharashtra Institute of
Technology, Pune

ABSTRACT

Information (or data) hiding process embeds data into digital media for the purpose of security. In spatial or frequency domain several Steganographic algorithms have been proposed for embedding data in digital images as cover media. These criteria have been used to evaluate the effectiveness of a Steganographic method to measure how it is secure against detection. Other criteria include embedding capacity and invisibility to human eyes. To increase the capacity of the hidden secret information as well as to provide a stego-image imperceptible to human vision, a novel steganographic approach based on pixel-value differencing is used. In this paper various methods of PVD are discussed and proposed method combines all the features of these methods.

General Terms

Security, Information Hiding.

Keywords

LSB, OPAP, PVD, ZZTS

1. INTRODUCTION

Today secret data transfer is a basic need of communication with one another. There are two approaches to covert exchanges of information. Firstly, to communicate in a way that it is understandable by the intended parties, but not to eavesdroppers. And second approach is to communicate safely, so no other party bothers to eavesdrop. Naturally both of these methods can be used concurrently to enhance privacy or secrecy.

Nowadays, Internet has become popular medium for data transmission due to a fast development of the modern technology. Establishing hidden communication is necessary to avoid security attack using data hiding. That embeds secret data into the cover media such as image, audio and video without the notice of interceptors. This is called as Steganography. General mechanism is shown in Fig. 1

One of the reasons, that intruders can be successful is that most of the information they acquire from a system is in a form that they can easily read and understand. Intruders may disclose the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One of the solutions to this problem is to use Steganography.

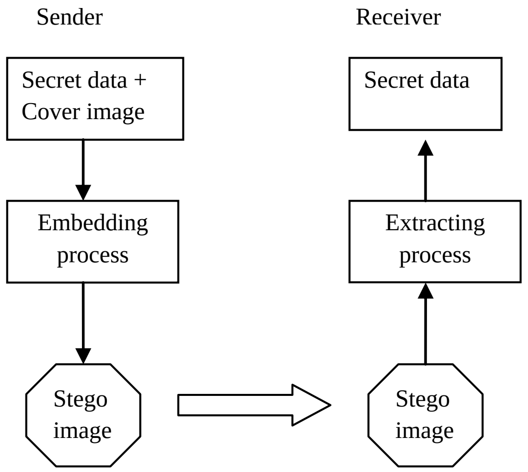


Fig.1. General steganography mechanism

Steganography is a technique of hiding information in digital media. [1]. There are various techniques like Least Significant Bit, Optimal Pixel Adjustment Procedure (OPAP), and Pixel value differencing (PVD) etc. are used for information hiding.

Conventional LSB insertion method is the basic concept for Steganographic techniques. It embeds secret bits in LSB(s) of the cover image. A pixel which carries a fraction of secret data is called a target pixel. To find the most appropriate capacity value more surrounding pixels around a target pixel are utilized. LSB proves that discovering the best capacity value brings about an improvement in terms of imperceptibility [2]. LSB embedding is used for smooth regions to increase capacity of hidden data. Most of the Steganographic techniques use either three or four adjacent pixels around a target pixel so that imperceptibility value becomes high.

This paper provides review and comparative analysis of various available methods for PVD. An exhaustive study of Steganographic methods that uses PVD is carried out. The proposed method provides the same hiding capacity as of the original PVD method with acceptable stego- image quality.

The paper is organized in different sections. Section 2 is about the basic concept of PVD. Section 3 describes the solution for falling-off boundary problem of PVD. In section 4 Zig Zag traversing method is described. Section 5 describes Adaptive method of PVD and in section 6 various PVD methods are summarized.

2. PIXEL VALUE DIFFERENCING METHOD

The PVD method is proposed by Wu and Tsai can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-images [3]. The PVD method divides the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding.

To estimate how many secret bits will be embedded into pixel, the largest difference value between the other three and/or four pixels close to the target pixel is calculated as shown in fig.2.

PVD is designed in such a way that the pixel modification does not violate gray scale range interval. The selection of the range intervals is based on the characteristics of human vision sensitivity to gray value (0-255) varies from smoothness to contrast. It provides an easy way to produce a more imperceptible result than simple LSB replacement methods [4]. The embedded secret message can be extracted from the resulting stego-image without referencing the original cover image. Moreover, to achieve secrecy protection of hidden data a pseudo-random mechanism may be used [3]. If secret data is stored randomly it is difficult to understand by the intruder.

PVD embedding is used for edged areas to increase image quality. It is also used to hide message into gray scale as well as in color image.

g(x-1,y-1) top left pixel	g(x-1,y) top pixel
g(x,y-1) left pixel	g(x,y) target pixel

Fig. 2 A target pixel with 3 neighboring pixels

2.1 Proposed PVD with bit flipping:

- In the embedding process of a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels.
- A difference value is calculated from these values of the two pixels in each block.
- All possible difference values are classified into a number of ranges.
- The calculated difference value then replaced by a new value to embed the value of a sub-stream of the secret message.
- The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to [5].

The PVD method was proposed to hide secret messages into 256 gray-valued images. It can embed large amount of data without much degradation in the image quality and thus are hardly noticeable by human eyes. It is based on the fact that human eyes can easily observe small changes in the gray values of smooth areas in the image but they cannot observe relatively larger changes at the edges areas. Fig.3 (a) and (b) shows data embedding process of PVD. Here the gray values of a sample two-pixel block are assumed to be (90; 110). The difference value is 20, which is in the range of 16 through 32. The width of the range is16 = 2^4, which means that a difference value in the range can be used to embed four bits of secret data. Assume that the four leading bits of the secret data are 1100. The value of this bit stream is 12. It is added to the lower bound value 16 of the range to yield the new difference value 28. Finally, the values (86; 114) are computed for use as the gray values in the stego-image. Note that 114-86=28. [3]

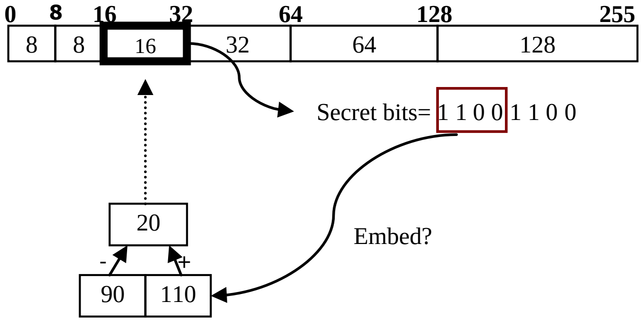


Fig. 3(a) Embedding process

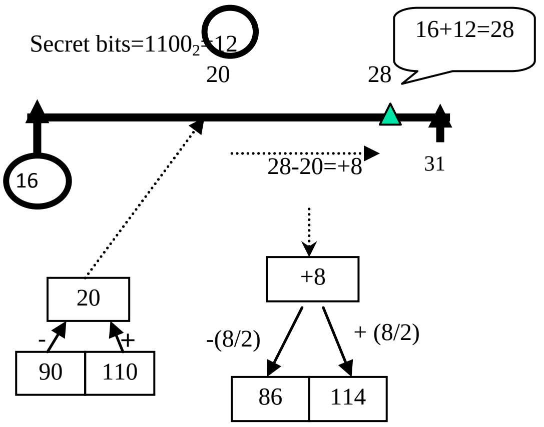


Fig. 3 (b) Embedding process

2.2 PVD with OPAP:

A modified version of PVD removes the shortcomings of basic PVD. In this method, instead of fixed ranges used in the original PVD method, variable ranges are used [6]. This method uses original PVD for embedding data by applying OPAP using target pixel with 3 surrounding pixel as shown in Fig. 2.

Capacity of embedding data in target pixel can be determined by calculating the largest pixel value differencing between the other three pixels close to the target pixel. If the pixel is in an edge area, more bits can be placed in the pixel than those in a smooth area. To enhance the image qualities of the stego-images, optimal pixel adjustment process (OPAP) is used. It also minimizes the embedding error. OPAP reduces the distortion caused by the LSB substitution method [7]. Further the pixel value is adjusted after hiding the secret data to improve the quality of the stego image without disturbing the hidden data as shown in Fig.4.

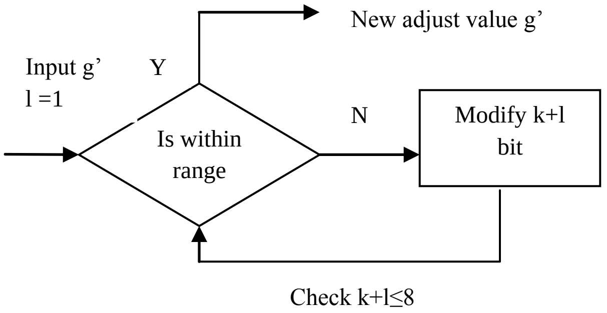


Fig. 4 pixel value adjusting method

In PVD, after embedding the K-bits of message into the gray value **g** of pixel and new gray value **g'** may go outside the range [8].

For example, range is 0-64. Assume the gray value g of the pixel is 01000000 in binary forms (64 in Decimal). Consider value [K] is 3 and bits to be inserted are 111. The gray value **g'** of pixel is 01000111 (70 in Decimal) and is outside the range. To make within the range 0-64, K+1 bits of **g'** are changed from 0 to 1 or vice-versa. This process is repeated until **g'** value falls within the range. For example, 01000111-01001111- 01011111- 01111111- 00111111.

Method represented by author use same process as discussed above, except using 3 surrounding pixel author uses 4 pixels [9]. Gray values of 4-pixels be g(x-1, y-1), g(x-1, y), g(x-1, y+1), g(x, y-1) surrounding the target pixel g(x, y) to implement the previous PVD algorithm shown in Fig. 5. Imperceptibility varies directly with number of neighboring pixel.

g(x-1,y-1) top left pixel	g(x-1,y) top pixel	g(x-1,y+1) top right pixel
g(x,y-1) left pixel	g(x,y) target pixel	

Fig. 5 A target pixel with 4 neighboring pixels

3. SOLUTION TO FALLING-OFF BOUNDARY PROBLEMS

In the PVD, some of the calculations may cause the two consecutive pixels to fall outside the boundaries of the range [0-255] is called falling-off boundary problem.

3.1 Modulus function and optimal approach:

Wang proposed a solution to falling-off-boundary problem using PVD and the modulus function [10]. In this method less secret data is hidden in smooth area and the more secret data in edge area. Hence, the stego-image quality degradation is more imperceptible to the human eye. Modulus function and optimal approach is used to alter the remainder so as to greatly reduce the alteration in original image by hiding of the secret data.

This method derives a difference value from two consecutive pixels by utilizing the original PVD. The hiding capacity of the two consecutive pixels depends on the difference value. Method computes the remainder of the two consecutive pixels by using the modulus operation to embed the secret data. The values of the two consecutive pixels are scarcely changed after the embedding of the secret message by optimal alteration algorithm. Instead of the difference value like Wu and Tsai's method, this method modifies the remainder of two consecutive pixels for better stego-image quality.

3.2 LSB replacement for 24-bit color images by applying condition on MSB:

Author proposed PVD for gray scale images where two consecutive pixel pairs are formed and embedding capacity is decided based on difference in their values like original PVD [11]. Author also proposed modified algorithm which extended PVD to 24-bit color images and also a new improved version of LSB method is applied on 24-bit color images.

In the embedding process a difference value is computed from every RED, GREEN and BLUE (R, G, B) component of non-overlapping block of two consecutive pixels of a given cover image. The way of partitioning the cover image into two-pixel blocks runs through all the rows of the image.

The original Kekre's method made use of up to four LSB's for embedding information. Selected number of LSB's depends on pixel value to control the error. Author modified this to include fifth LSB matching to increase capacity further.

Before embedding the data, 8-bit secret key(S) and message (M) is XOR'ed. And Message is recovered by XOR operation of the same 8-bit key.

S XOR M= E'
E' XOR S=M

Every pixel value in this image is analyzed and the checking process is employed on MSB bits.

Condition 1: If the value of the pixel g_i is in the range between 240 to255, then check for the message bit to be embedded (m).

- If m=1 then utilize the fifth bit of the pixel value.
- If m ≠ 1 then embed 4 bits of secret data into the 4 LSB's of the pixel.
- This can be done by observing the first 4 MSB's. If they are all 1's then the remaining 4 LSB's can be used for embedding data.

Condition 2: If the value of g_i (First 3 MSB's are all 1's), is in the range between 224 to 239 then check for the message bit to be embedded (m)

- If m=0 then utilize 5 bits of the pixel value.
- If m ≠ 0 then embed 3 bits of secret data into the 3 LSB's of the pixel.

Condition 3: If the value of g_i (First 2 MSB's are all 1's), is in the range between 192 to 223 then embed 2 bits of secret

data into the 2 LSB's of the pixel.

Condition 4: All other cases for the values in the range 0 to192 embed 1 bit of secret data in to 1 LSB of the pixel.

The embedding process maintains a matrix to keep a track of the pixels where 5 bits are utilized for embedding process. This helps in the retrieving the secret message. The retrieving process is very simple by observing the MSB and using the matrix maintained.

In PVD during the embedding phase there is a possibility that the gray values of the two- Pixel block may fall off the boundary value which needs a checking process to be employed in the embedding phase and incase of value fall off the boundary value the block is discontinued for inserting the secret data. The same checking process is again repeated in the retrieval phase. Due to this there can be certain blocks which are not utilized for embedding secret data. This checking process is tedious and takes more time both for embedding and retrieval of the message. In the modified Kekre's method there is no such checking process required making it faster than PVD. This method also utilizes every pixel of the image to embed the secret data. Hence, method is simple for implementation compared to PVD method and achieves a high embedding capacity and good imperceptibility.

3.3 Multiple LSB algorithms:

Author presented PVD and Kekre's Multiple LSB Algorithms (KMLA) [12]. The Scheme based on KMLA+PVD method can embed secret data larger than the PVD and KMLA (described in above method) method. This technique is proposed to improve the image capacity.

In this proposed technique two methods are combined (KMLA + PVD).The image is divided into non overlapping two pixel block. The difference of the block is calculated. If the difference is between values of 0-191 then embed the secret data using PVD approach. Else, utilize the KMLA method .The proposed technique overcomes the shortcoming of KMLA method where the gray value between 0-191 embeds only 1-bit of secret message.

KMLA and PVD methods have lesser capacity than the proposed technique. If KMLA and PVD approaches are used in combination then there is increase in the capacity.

3.4 Quantization of difference of gray values:

Author presented, embedding process by using Quantization of difference of gray values of two-pixel blocks and falling of boundary check techniques [13].

Falling of Boundary check: In the inverse calculation, some of the calculations may cause the two consecutive pixels to fall off the boundaries of the range [0,255]. Falling off-boundary checking proceeds by producing a pair of non-overlapping pixel from the inverse calculation of the value of the function f ((gi,gi+1), uk,„Ÿd). Since uk is the maximum value in the range from lk to uk, the resulting pair of (gi, gi+1) produced by the use of uk will yield the maximum difference. If either of gi or gi+1 fall off the boundary of 0 or 255, then abandon the block for embedding data.

This method, partitions the image, calculates the difference and selects the range interval same as original PVD. The process of extracting the embedded message proceeds by using the zigzag scanning as in the embedding process described in next method. Apply the same falling-off boundary checking to find out whether the block was used or not in the embedding process.

4. ZIG ZAG TRAVERSING

Author apply Zig-Zag traversing scheme (ZZTS) to PVD as shown in Fig 6. This method enhances security and the quality of image inspite of high capacity of concealed information [14]. PVD method adapts the number of embedded bits to the gray scale or color changes in consecutive pixels. This achieves increase in the embedding capacity without significant loss of image quality.

Zig-Zag PVD uses the difference of each pair of pixels to determine the number of message bits that can be embedded into that pixel pair. It starts at the upper-left corner of the cover image and scans the image in a Zig-Zag manner.

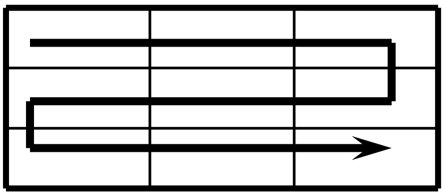
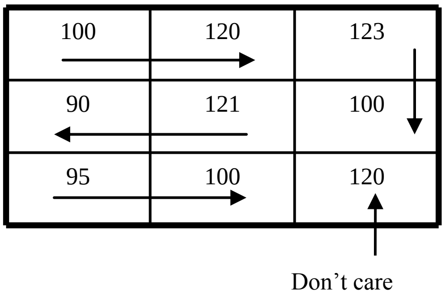


Fig. 6. ZIG-ZAG scans of image

Then, it partitions the resulting sequence into blocks where each block consists of two consecutive non overlapping pixels like original PVD. The differences of the two-pixel blocks are used to categorize the smoothness properties of the cover image. The larger the difference, the more the bits that can be embedded into that pixel pair. Example shown in Fig.7 returns the value as, (+20, -23, -31, +5).



100	120	123
90	121	100
95	100	120

Fig. 7 Example of ZIG-ZAG PVD

The Zig Zag method exploits the ability of the PVD and betters PVD in terms of predictability. Since the scanning process is random, it will not be possible for attackers to even determine the method of scanning, so that their attack, if any, fails.

5. ADAPTIVE PVD

Author proposed an adaptive Steganography based modified PVD through management of pixel values within the range of gray scale. [15] PVD method is used and checks whether the pixel value exceeds the range on embedding. If the pixel exceeds the boundary [0-255] then position of that pixel has been marked and handled delicately to keep the value within the range. Range is managed, using PVD.

In APVD method a gray scale digital image has been used as a cover image where pixel values ranged between 0 and 255 and the pixel values of stego-image will not exceed the gray scale range. In PVD method pixel values in the stego image may exceed the gray scale range which is not desirable as it may leads to improper visualization of the stego image. APVD is used to overcome this problem.

5.1 Zig-Zag for gray image:

1. If any pixel value exceeds the range, then check the bit-stream‘t’ to be hidden.
2. If MSB of the selected bit stream‘t’=1 then embed one less number of bits, where MSB position is discarded from t; otherwise the bit number of hidden data depends on w_i .
3. If pixel value exceeds the range and t=101, then set t=01 and embed it.
4. If pixel value again exceeds the range, then embed the value at one pixel, rather than both pixels (of the pixel block), which will not exceed the range after embedding; where the other pixel is kept unchanged.
5. It will keep the pixel values within the range because both pixels of a block cannot exceed at the same time as per the original PVD method.
6. Keep the information within each block, whether one less bit is embedded or not, as overhead.

In this method, data hiding by using pixel value differencing guarantees that no pixel value will exceed the range 0 to 255 in stego-image. Using original PVD method where pixel value does not cross the range, it gives same hiding capacity as the original PVD with acceptable stego-image quality. Zig-Zag method provides with identical payload and visual fidelity of stego-image compared to the PVD method.

5.2 Zig-Zag for color image:

Author proposed above method for color images, where author considers all three basic colors [16]. Every pixel in a color image composed of three colors (channels) i.e. Red, Green and Blue. So, every pixel contains 24 bits where 8 bits for red component, 8 bits for green and 8 bits for blue component in a pixel. In the proposed technique, all the three components have been used for data embedding.

First, each color component is separated from a pixel and get three separate M*N matrix, one for each component color, where the original image size is M*N. Then apply PVD method for data hiding in each matrix separately, but in a sequencing manner. First embed bits in 1st pixel block of the red component matrix, then in 1st block of green component matrix and lastly in blue component matrix, then again 2nd block of red matrix and so on. In this way secret data is embedded into the total image. Further embed different number of bits for different component pixel blocks for increasing security as well as improving the visual quality of the stego-image.

6. SUMMARY OF VARIOUS PVD METHODS

PVD method provides both high embedding capacity and outstanding imperceptibility for the stego-images. Data hiding is performed by taking difference value of three and two neighboring pixels by adapting Zig-Zag traversing scheme (ZZTS). This method enhances security and the quality of image inspite of high capacity of concealed information. Error correction mechanism using hamming code is applied to ensure reliable secret communication. Modulus function with PVD avoids the falling-off boundary problem, Optimal Pixel Adjustment Procedure (OPAP) is used to minimize embedding error. Adaptive method is used to avoid overflow problem of pixel in gray images and color images. Summary of various PVD methods are shown in Table 1.

Table1. Summary of existing PVD methods

	Implementation	**Algorithm**	**Falling-off boundary problem**	**Image quality**	**Capacity of secret data**
PVD with bit flipping	Moderate	Original PVD	-	High	Increase
PVD with OPAP	More Flexible than original PVD	OPAP	Avoid	Higher	Highly increased
Modulus function plus OPAP	More Flexible than first method	OPAP + modulus function	Avoid using reminder of modulus function	Higher	Highly increased than original PVD
LSB replacement on 24-bit color image	Faster than PVD	Color PVD + Kekres algorithm	Not required	Excellent	Higher than above PVD method
Multiple LSB algo.	More secure	KMLA + PVD	Not required	Higher	Highly increased
Quantization technique	Complicated for color image	Quantization	falling off boundary checking technique	High	Increase
Zig Zag Traversing	Reliable security using hamming code	ZZTS + Hamming code	Not required	Higher	Highly increased
Adaptive PVD for Gray image	Faster than PVD	Adaptive PVD	Not required	Excellent	Same as Original PVD
Adaptive PVD for color image	More secure than original PVD	Adaptive PVD	Not required	Excellent	Same as Original PVD

7. CONCLUSION

Over a last decade the Steganographic methods using Pixel Value Differencing have developed remarkably. The various techniques like LSB, OPAP, Modulus function, and adaptive method apply with PVD to improve the quality of stego image and increase the capacity of secret message. In our proposed work combination of two or more techniques are used to improve the quality of the image and capacity of hidden data. Proposed embedding algorithm would generate stego image without significant degradation or loss of perceptual quality of the cover. Combination of all flavors of existing PVDs in our method would result into robustness of embedded data and increase in complexity of encoding and decoding.

8. ACKNOWLEDGMENTS

The authors wish to thank the anonymous reviewers for their useful suggestions that helped in improving the quality of this paper. This work was supported in part by MAEER.s MIT, Pune.

9. REFERENCES

[1] Muhalim Mohamed Amin, Saurabh Ibrahim, Mazleena Salleh, Mohd. Rozi Katmin, "Information hiding using steganography",Vol71847 ,2003

[2] Masoud Afrakhteh, Subariah Ibrahim "Adaptive steganography scheme Using More Surrounding Pixels", International Conference On Computer Design And Applications (ICCDA 2010), Vol.1, V1225-V1229

[3] Wu,Tsai, "A steganographic method for images by pixel-value differencing" ,Volume 24, Issues 9-10, June 2003, pages 1613-1626

[4] A. E. Mustafa, A.M.F. ElGamal, M.E. ElAlmi, Ahmed.BD, "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit", *Issue No. 21, April. 2011*

[5] H.C.Wu, Tsai, Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proc-vis. Image signal process, vol. 152, no.5, October 2005, 611-615

[6] Han-ling ZHANG, Guang-zhi GENG, Cai-qiong Xing, 2009."Image Steganography using Pixel-Value Differencing", IEEE DOI 10.1109/ISECS.2009.139), 109–112.

[7] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution",Pattern Recognition Society. Published by Elsevier Ltd. All rights reserved.doi:10.1016/j.patcog.2003.08.007.

[8] Yogendra Kumar Jain, R.R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security vol. (4), issue (1), pg no. 40-49.

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

[10] Chung - Ming Wang , Nan-I Wu , Chwei - Shyong Tsai, Min-Shiang Hwang ,"A high quality steganographic method with pixel-value differencing and modulus function",J.Syst.Software(2007),doi:10.1016/j.jss. 2007.01.049

[11] H.B. Kekre, Archana Athawale, Pallavi 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 (ICAC3'09)

[12] Dr H.B Kekre, Ms Pallavi Halarnkar, Kahkashan Ansari, Parakh Jindal, Yash Chaturvedi," Information hiding with increased capacity using KMLA+PVD approach", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.2, April 2012

[13] A.L.Khade. B.G.Hogde, V B Gaikwad. "Secret Communication via Image Hiding In Image by Pixel Value Differencing", ICWET', February 2010, 437-438.

[14] M.Padmaa,Dr.Y.Venkataramani,"ZIG-ZAG PVD – A Nontraditional Approach", International Journal of Computer Applications (0975 – 8887),Volume 5– No.7, August 2010

[15] J. K. Mandal 1 and Debashis Das," Steganography Using Adaptive Pixel Value Differencing(APVD) of Gray Images Through Exclusion of Overflow/Underflow", The second International Conference on Computer Science, engineering and applications (CCSEA-2012) , May 2012

[16] J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, 83-93