PVD Blend with Pixel Indicator - OPAP Composite for High Fidelity Steganography

R.Amirtharajan
Assistant Professor
School of Electrical & Electronics Engineering
SASTRA University

Adharsh.D
Dept of ECE
School of Electrical & Electronics Engineering
SASTRA University

Vignesh.V
Dept of ECE
School of Electrical & Electronics Engineering
SASTRA University

R.John Bosco Balaguru
Associate Dean Research
School of Electrical & Electronics Engineering
SASTRA University

ABSTRACT
The defense researchers have started concentrating on the info-wars, which now has become a new plausible area of interest in the electronic epoch. Valuable secret information could be sabotaged, manipulated or even sold thereby, posing a threat to the very essence of confidentiality. Steganography has been playing a remarkable role in prevention of info-sabotage by adopting a principle of undetectable secret sharing. This technique camouflages the secret data into an unsuspecting image, thereby protecting the very existence of it. The security can be enhanced by cleverly embedding the data, taking care not to affect the quality of the image, along with a random choice of 'plane of embedding', in case of a colour image. The MSE can be decreased by using Optimal Pixel Adjustment Process, thereby making the secret information more secure and conceited. In this paper the Optimum Pixel Adjustment Process (OPAP) coupled with Pixel Indicator (PI) technique and Pixel value differencing (PVD) in the colour image, is proposed for enhanced stego-image quality and fortified security. The colour cover image, split into three layers namely Red, Blue and Green, act as an embedding platform by adapting Raster scan. While embedding, PI technique, followed by PVD is used to decide the number of bits embedded in a target pixel and finally OPAP technique is employed to enhance the image quality. In order to prove the efficiency of the proposed composite stego, Mean square error (MSE),and Peak Signal to Noise Ratio (PSNR) of the stego image have been reported.

General Terms
Information Security, Information hiding.

Keywords
Steganography, OPAP, Pixel indicator(PI), Pixel value differencing (PVD).

1. INTRODUCTION
Espionage, financial theft, infringement and cross border crimes are deterrent to social and legal systems which amass a great a great deal of secret and highly confidential information. High profile secrets if revealed can lead to disastrous confusion. Therefore with people's iniquity sky rocketing every day, the need to keep secrets as a secret for social and ethical needs has become all the more important. Most of the precedent algorithms have been mangled easily by hackers thus necessitating the quest for an impregnable algorithm. In this context, steganography extends its helping hand to protect secrets by hiding information in video, audio, digital image, etc. [1, 3 , 5, 11] which in turn is very hard to be hacked or cracked. Digital Steganography an enthralling field of research falls under the aegis of security systems. It has been instrumental in protecting secrets by hiding information in video, audio, digital image, etc. [1, 3 , 5, 11] which are invincible. Cryptography differs from Steganography[1, 14] in the sense that the former focuses on keeping the contents of a message secret through scrambling and its meaning meaningless, while the later focuses on keeping the existence of a message secret.

Steganography and cryptography are both ways to protect information from intruders but neither technology alone is perfect and can be compromised. Two other technologies that are closely related to steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography.

The purpose of steganography is partly defeated when the presence of hidden information is revealed or even suspected[11], however its strength can be aggrandized by combining it with cryptography. In watermarking [11] all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting [11] on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties.

In watermarking and fingerprinting [11] the fact that information is hidden inside the files may be public knowledge sometimes it may even be visible, while in steganography the imperceptibility of the information is crucial .A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it.

2. Review on literature
In image steganography the cover object, an image which may be color [1, 10], grayscale [3, 4] or binary [5], is the embedding

platform for the information . A stego image is a derivative of the cover image after the secret message is embedded using an algorithm that slightly modifies it. Out of the numerous steganographic methods proposed, Least Significant Bits (LSB) substitution[7] is the most popular and simple method that utilizes the least bits of a pixel in the cover image for embedding.

The main reasons for the LSB Substitution method to be popular are as follows [1, 2, 3, 4, 6, 7, 8, 10, 11, 12, 13]. Firstly, the ease of computation is very high because of its straight forward implementation. Secondly, large amount of information or payload can be hidden in the cover image without distorting it. Human eye is sensitive only to the changes made in the smooth areas of an image. It overlooks or cannot perceive the alterations made to the less sensitive edge areas of the image [8, 17-19].

But Traditional LSB substitution method has disadvantages:

- Since the LSB substitution method is a well known method, the message embedded using this method is vulnerable.
- The number of message bits embedded in each pixel is same for all the pixels. Hence the decoding of the embedded is very easy and security of the message is at stake.
- Visual degradation is possible if more number of message bits is embedded in the edge areas of the image, hence for fully embedded image visual degradation will be high.
- The payload is average

Pixel Indicator based stego system proposed by Adnan Gutub[2] Based on Randomization principle using LSB [6, 7], where the secret is hidden in the least significant bits of the pixels, with more randomization in selection of the number of bits used and the color channels that are used. This randomization is expected to increase the capacity and the security of the system. This technique could be applied to color images where each pixel is represented by three bytes to indicate the intensity of Red, Green, and Blue in that pixel. But the problem with Pixel indicator methodology it's relally hard to predict the embedding capacity[12].

A method using PVD has been proposed by Padmaa[13] in ZIG-ZAG PVD – A Nontraditional Approach which enhances security and the quality of image in spite of high capacity of concealed information with error correction mechanism to ensure reliable secret communication.

In this purported paper a blend of PVD, PI and OPAP has been proposed to implement a complex random steganography method. The paper is arranged into the following sessions: section 3: steganographic algorithm for color image. Section 4: Error metrics. Section5. Experimental results and discussion and Section 6: conclusion.

3. The Proposed Methodology

This proposed combinational methodology uses Pixel Indicator methodology [2, 12] to select a pixel as given in Table I. The number of bits embedded in the selected pixel will be decided by PVD [19] which in turn enhances the quality of the stego image by adapting OPAP algorithm [7]. The observations made with various images using the proposed scheme validate the same

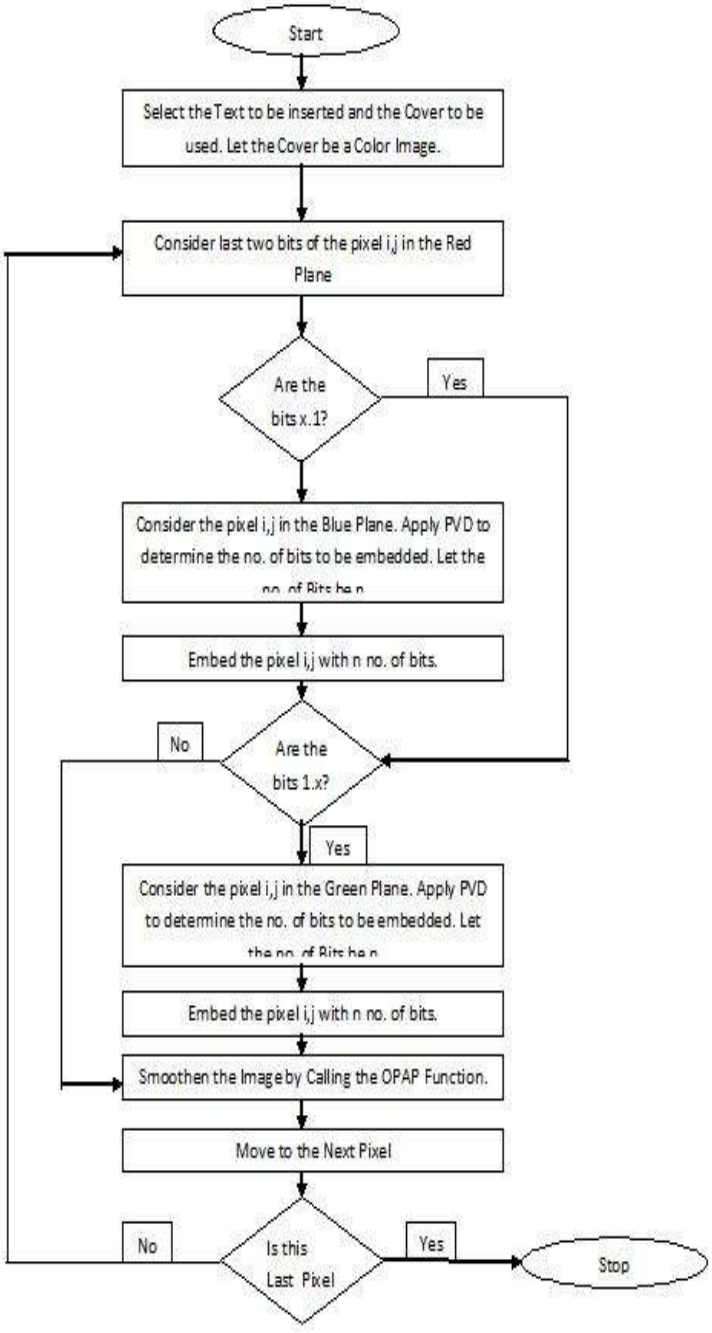

Figure 1 : Flowchart for the proposed system.

To further extend the overall capacity of the proposed algorithm [19], a procedure "largest difference value between the immediate four pixels" is adopted to determine how many bits to be inserted into a target pixel. Additionally OPAP modular operation is also implemented to ameliorate the image quality. This method is experimentally found to have more efficiency

compared to the existing methods and the quality image is also remains undistorted.

Table 1. Meaning of indicator values

INDICATOR	CHANNEL 1	CHANNEL 2
00	No data embedded	No data embedded
01	No data embedded	n bits of data embedded obtained by PVD
10	n bits of data embedded obtained by PVD	No data embedded
11	n bits of data embedded obtained by PVD	n bits of data embedded obtained by PVD

3.1 The Proposed Algorithm

Case-1 : PVD with Tri-Colour Random Image Steganography

3.1.1 Embedding Algorithm:

Inputs : Secret Data(D), Cover Image(C)
Output: Stego image(S) with secret data embedded in it.

1. Convert the Secret Data (D) into binary format.
2. Split the cover image C into Red,Green and Blue Planes.(R,G and B respectively)
3. For each pixel in R, do the following:
   3.1. Let b[0]=LSB of the current pixel in R
   3.2. Let b[1]=Next LSB of the current pixel in R
   3.3. If b=00 then
        Go to next pixel.
      Else if b=01 then
        Call PVD Embedding to embed secret data in current pixel of G.
      Else if b=10 then
        Call PVD Embedding to embed secret data in current pixel of B.
      Else
        Call PVD Embedding to embed secret data in current pixel of both G and B.
   3.4. If all secret data is embedded, then
        Go to step-4
4. Store the resulting image as Stego Image (S) after applying OPAP.

3.1.2Recovery Algorithm:

Input : Stego Image(S)
Output:Secret Data (D)

1. Split the stego image S into Red,Green and Blue Planes.(R,G and B respectively)
2. For each pixel in R, do the following:
   2.1. Let b[0]=LSB of the current pixel in R
   2.2. Let b[1]=Next LSB of the current pixel in R
   2.3. If b=00 then
        Go to next pixel.
      Else if b=01 then
        Call PVD Recovery to recover secret data from current pixel of G.
      Else if b=10 then
        Call PVD Recovery to recover secret data from current pixel of B.
      Else
        Call PVD Recovery to recovery secret data from current pixel of both G and B.
3. Store the resulting recovered data as Secret Data (D)

3. 2 The Proposed Algorithm

Case-2 : PVD with Custom-indicator-plane Tri-Colour Random Image Steganography

3.2. 1 Embedding Algorithm:

Inputs : Secret Data(D), Cover Image(C), Indicator-plane Index(I)
Output: Stego image(S) with secret data embedded in it.

1. Convert the Secret Data (D) into binary format.
2. Split the cover image C into Red,Green and Blue Planes.(R,G and B respectively)
3. If I=1 then,
      P[1]=R, P[2]=G, P[3]=B
   Else if I=2, then

 P[1]=G, P[2]=R, P[3]=B
   Else if I=3, then

 P[1]=B, P[2]=R, P[3]=G

4. For each pixel in P[1], do the following:
   4.1. Let b[0]=LSB of the current pixel in P[1]
   4.2. Let b[1]=Next LSB of the current pixel in P[1]
   4.3. If b=00 then
        Go to next pixel.
      Else if b=01 then
        Call PVD Embedding to embed secret data in current pixel of P[2].
      Else if b=10 then
        Call PVD Embedding to embed secret data in current pixel of P[3].
      Else
        Call PVD Embedding to embed secret data in current pixel of both P[2] and P[3].
   4.4. If all secret data is embedded, then
        Go to step-5
5. Store the resulting image as Stego Image (S) after applying OPAP.

3.2. 2 Recovery Algorithm:

Input : Stego Image(S), Indicator-plane index (I)
Output:Secret Data (D)

1. Split the stego image S into Red,Green and Blue Planes.(R,G and B respectively)
2. If I=1 then,

P[1]=R, P[2]=G, P[3]=B
Else if I=2, then

P[1]=G, P[2]=R, P[3]=B
Else if I=3, then

P[1]=B, P[2]=R, P[3]=G

3. For each pixel in P[1], do the following:
3.1. Let b[0]=LSB of the current pixel in P[1]
3.2. Let b[1]=Next LSB of the current pixel in P[1]
3.3. If b=00 then
Go to next pixel.
Else if b=01 then
Call PVD Recovery to recover secret data from current pixel of P[2].
Else if b=10 then
Call PVD Recovery to recover secret data from current pixel of P[3].
Else
Call PVD Recovery to recover secret data in current pixel of both P[2] and P[3].
4. Store the resulting data as Secret Data (D).

3. 3 The Proposed Algorithm

Case-3: PVD with Cyclic-indicator-plane Tri-Colour Random Image Steganography

3.3.1 Embedding Algorithm003A

Inputs : Secret Data(D), Cover Image(C)
Output: Stego image(S) with secret data embedded in it.

1. Convert the Secret Data (D) into binary format.
2. Split the cover image C into Red,Green and Blue Planes.(R,G and B respectively)
3. Let index i=1.
4. For each pixel in P[1], do the following:
4.1. If (i mod 3) =1 then,
I[i]=1
Else if (i mod 3)=2 then,
I[i]=2
Else
I[i]=3
4.2. Set i=i+1
5. Let index j=0
6. For each pixel in P[1], do the following:
6.1. If I[j]=1 then,
P[1]=R[i], P[2]=G[i], P[3]=B[i]
Else if I[j]=2, then

P[1]=G[i], P[2]=R[i], P[3]=B[i]
Else if I[j]=3, then

P[1]=B[i], P[2]=R[i], P[3]=G[i]

6.2. Let b[0]=LSB of P[1]
6.3. Let b[1]=Next LSB of P[1]
6.4. If b=00 then
Go to next pixel
Else if b=01 then
Call PVD Embedding to embed secret data in P[2].
Else if b=10 then
Call PVD Embedding to embed secret data in P[3].
Else
Call PVD Embedding to embed secret data in both P[2] and P[3].
6.5. If all secret data is embedded, then
Go to step-7
Else
j = j+1
7. Store the resulting image as Stego Image (S) after applying OPAP.

3.3.2 Recovery Algorithm:

Input : Stego Image(S)
Output:Secret Data (D)

1. Split the stego image S into Red,Green and Blue Planes.(R,G and B respectively)
2. Let index i=1.
3. For each pixel in P[1], do the following:
4.1. If (i mod 3) =1 then,
I[i]=1
Else if (i mod 3)=2 then,
I[i]=2
Else
I[i]=3
4.2. Set i=i+1
4. Let index j=0
5. For each pixel in P[1], do the following:
5.1. If I[j]=1 then,
P[1]=R[i], P[2]=G[i], P[3]=B[i]
Else if I[j]=2, then

P[1]=G[i], P[2]=R[i], P[3]=B[i]
Else if I[j]=3, then

P[1]=B[i], P[2]=R[i], P[3]=G[i]

5.2. Let b[0]=LSB of P[1]
5.3. Let b[1]=Next LSB of P[1]
5.4. If b=00 then
Go to next pixel
Else if b=01 then
Call PVD Recovery to embed secret data from P[2].
Else if b=10 then
Call PVD Recovery to embed secret data from P[3].
Else
Call PVD Recovery to embed secret data from both P[2] and P[3].

6. Store the resulting data as Secret Data (D)

4. Error metrics

Distortion in the stego image is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

The MSE is calculated by using the equation,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[X_{i,j} - Y_{i,j}\right]^2 \quad (1)$$

where *M* and *N* denote the total number of pixels in the horizontal and the vertical dimensions of the image *Xi, j* represents the pixels in the original image and *Yi, j,* represents the pixels of the stego-image.

The Peak Signal to Noise Ratio (PSNR) is expressed as

The PSNR is calculated using the equation,

$$PSNR = 10\log_{10}\left(\frac{I_{\max}^2}{MSE}\right)dB \quad (2)$$

where I_{max} is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher the value of PSNR better the image quality

Distortion Analysis of stego image using the software based secret sharing algorithm with 100% embedding of data gave the following results.

5. Experimental Results and Discussion

In this present implementation Lena, baboon, Gandhi and Temple of 256 × 256 color digital images has been taken as cover images as shown in Figure 2 a, b, c & d and tested for full embedding capacity. The effectiveness of the stego process proposed has been studied by calculating MSE and PSNR for all the four digital images in RGB planes using the proposed three method is given in Table I, II and III

Figure 2 a. Lena b. Baboon c. Gandhi d. Big Temple

The corresponding stego images after full embedding capacity by adapting all the methodologies has been given in Figure 3, 4 and 5

TABLE- I
ESTIMATION PARAMETERS OF THE PROPOSED EMBEDDING SCHEME I

Cover Image	Channel I Red		Channel II Green		Channel III Blue		BPP (Bits Per Pixel)
	MSE	PSNR	MSE	PSNR	MSE	PSNR	RGB
Lena	0	∞	1.57	46.18	1.52	46.31	1.42
Baboon	0	∞	2.65	43.88	2.72	43.77	1.47
Gandhi	0	∞	1.30	47.07	1.24	47.15	1.38
Temple	0	∞	1.76	45.66	1.63	46.00	1.60

TABLE- II
ESTIMATION PARAMETERS OF THE PROPOSED EMBEDDING SCHEME II

Cover Image	Channel I Red		Channel II Green		Channel III Blue		BPP (Bits Per Pixel)
	MSE	PSNR	MSE	PSNR	MSE	PSNR	RGB
Lena	0	∞	1.57	46.18	1.52	46.31	1.38
Baboon	2.61	43.96	0	∞	2.72	43.77	1.63
Gandhi	1.34	46.83	1.30	47.07	0	∞	1.36
Temple	1.85	45.45	0	∞	1.63	46.00	1.54

TABLE- I
ESTIMATION PARAMETERS OF THE PROPOSED EMBEDDING SCHEME III

Cover Image	Channel I Red		Channel II Green		Channel III Blue		BPP (Bits Per Pixel)
	MSE	PSNR	MSE	PSNR	MSE	PSNR	RGB
Lena	1.68	45.89	1.57	46.18	1.52	46.31	2.13
Baboon	2.61	43.96	2.65	43.88	2.72	43.77	2.51
Gandhi	1.34	46.83	1.30	47.07	1.24	47.15	2.07
Temple	1.85	45.45	1.76	45.66	1.63	46.00	2.30

In the first phase RED plane has been considered as an indicator channel and the result are presented in Table I. The drawback in the first implementation is RED characteristics are always same with the cover statistics so it may give a clue to the intruders. Hence in the second implementation user has been given with the liberalization to select the indicator channel still it give the same clue and both implementation never improve the capacity. The third methodology offers no clue to the intruders, because the secret message is evenly distributed in the entire channel and significantly improves the hiding capacity.

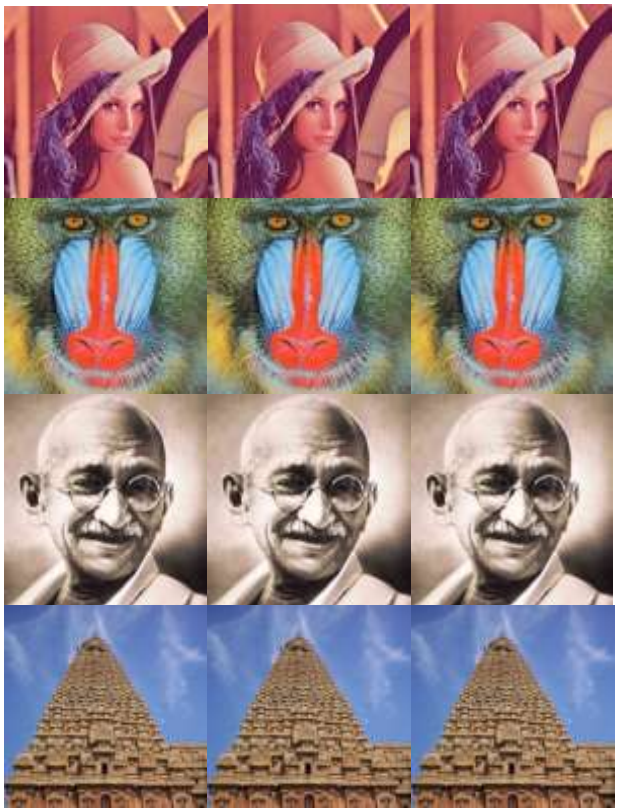

Figure 3 Method I Figure 4 Method II Figure 5 Method III

The corresponding histogram for Big Temple Tanjore by adapting method 1 is given in the following figure 6 and shows that there is no variation in RED plane and slight variation other two planes.

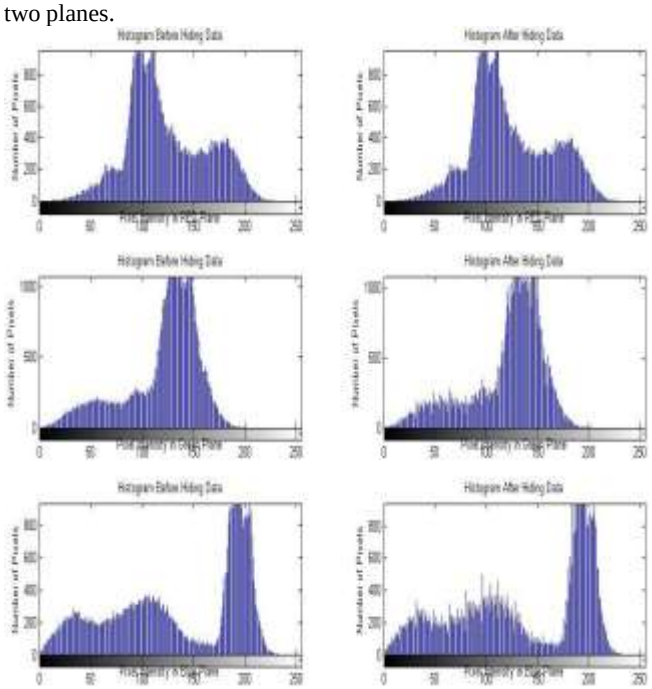

Figure 6 Histogram Big Temple Tanjore by adapting method I

The corresponding histogram for Big Temple Tanjore by adapting method II AND Green as indicator plane is given in the following Figure 7 and shows that there is no variation in GREEN plane and slight variation on other two planes.

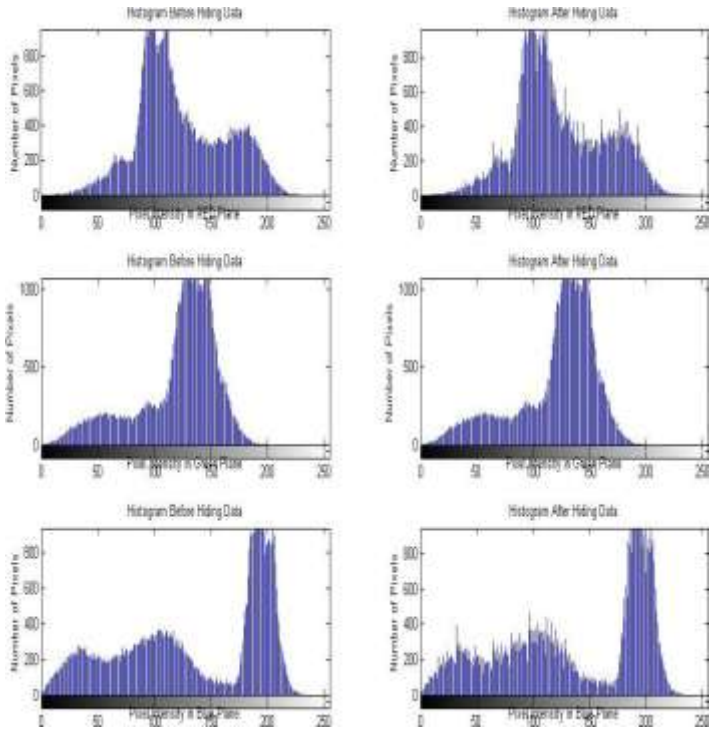

Figure 7 Histogram Big Temple Tanjore by adapting method II

The corresponding histogram for Big Temple Tanjore by adapting method III is given in the following Figure 8 and shows that there is a slight variation in all the three planes.

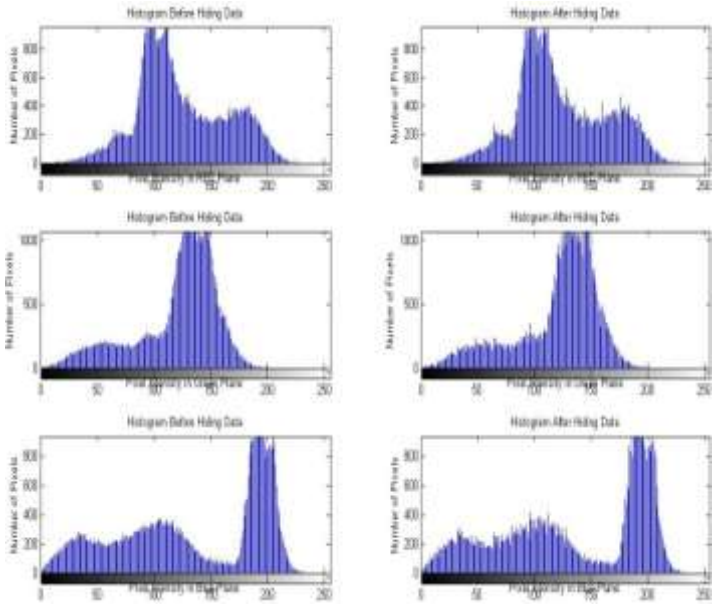

Figure 8 Histogram Big Temple Tanjore by adapting method III

6. CONCLUSION

The process of embedding secret data based on indicator-plane increases the embedding entropy considerably. The Pixel Value Differencing process performs intelligent embedding thereby optimally preserving the quality of the stego-image. The Optimal Pixel Adjustment Process decreases the Mean Square Error (MSE) thus making the stego image indistinguishable with the cover. Thus, the proposed method, which is an amalgam of the above mentioned three methods, it incorporates reduction of detectability and increase of entropy at the same time

7. ACKNOWLEDGMENTS

The authors wish to thank Dr.R.Varadharajan, Professor / ECE and Dr. K.Thenmozhi Associate Dean ECE / SEEE/ SASTRA University for their valuable guidance and support.

8. REFERENCES

[1]. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods Signal Processing 90 (2010) 727–752

[2]. Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, and Aleem Alvi, "Pixel Indicator high capacity Technique for RGB image Based Steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008

[3]. R.Amirtharajan.R.Akila. P.Deepikachowdavarapu Article: A Comparative Analysis of ImageSteganography. *International Journal of Computer Applications* 2(3)(2010) 41–47.

[4]. R.Amirtharajan, Krishnendra Nathella and J Harish, "Info Hide – A Cluster Cover Approach" International Journal of Computer Applications 3(5) (2010) 11–18.

[5]. R.Amirtharajan, Venkata Abhiram Murarisetty and R.John Bosco Balaguru, "Binary in Binary for Secret Writing - A Cryptic's Cousin Approach" International Journal of Computer Applications 5(11) (2010) 41–47.

[6]. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3&4) (1996) 313–336.

[7]. C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.

[8]. Chang, C.C., Tseng, H.W., 2004. A steganographic method for digital images using side match. Pattern Recognition Letter 25 (September), 1431–1437.

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

[10]. Fridrich, J., Goljan, M., Du, R., 2001. Reliable detection of LSB steganography in color and grayscale images. In: Proceedings of ACM Workshop on Multimedia and Security, pp. 27–30.

[11]. S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000

[12]. Nabarun Bagchi. Article: Secure BMP Image Steganography Using Dual Security Model (I.D.E.A, image intensity and Bit Randomization)and Max-Bit Algorithm.. *International Journal of Computer Applications* 1(21)(2010):18–22

[13]. M.Padmaa Dr.Y.Venkataramani." ZIG-ZAG PVD - A Nontraditional Approach". *International Journal of Computer Applications* 5(7)(2010) 5–10

[14]. F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding—a survey, Proc. IEEE 87 (7) (1999) 1062–1078.

[15]. C.C. Thien, J.C. Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recognition 36 (11) (2003) 2875–2881

[16]. R.Z. Wang, C.F. Lin, J.C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2000) 671–683.

[17]. Wu, D.C., Tsai, W.H., 2003. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters 24 (June), 1613–1626.

[18]. Wu, H.C., Wu, N.I., Tsai, C.S., Hwang, M.S., 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings – Vision Image and Signal Processing 152 (October), 611–615.

[19]. Young-Ran Park, Hyun-Ho Kang, Sang-Uk Shin, and Ki-Ryong Kwon, An Image Steganography Using Pixel Characteristics Y. Hao et al. (Eds.): CIS 2005, Part II, Springer-Verlag Berlin Heidelberg LNAI 3802, (2005) 581–588.