IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

A Steganographic Approach Using New Pixel Selection Combined With Hash Function for Secure Data Transmission in e-Banking

Atanu Sarkar[1*], Sunil Karforma[2]

[1]Dept. of computer Science, University of Burdwan, Burdwan, West Bengal, India
[2]Dept. of computer Science, University of Burdwan, Burdwan, West Bengal, India

[*]*Corresponding Author: atanu.sk@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 13/Aug/2018, Published: 31/Aug/2018

***Abstract*−** A new pixel selection technique has been introduced where data embedding starts from middle region (one or more than one pixel) of the image. Successively, diagonal pixels of middle region are selected for further embedding the data. The diagonal pixels form a quadrilateral where data are embedded through four edges of quadrilateral with clockwise manner. A hash based method is also initiated for embedding the data into the pixel of an image taking one bit position out of four LSB bits where one bit of secret data is embedded. We propose a variable hash key function for the selection of bit position so that intruder cannot guess the actual bit position of secret information easily. Our proposed method has achieved good PSNR and high capacity of secret information compared to different pixel value differencing method (PVD).

***Keywords*:** LSB, middle region, Cryptography, Image Steganography, e-Banking.

I. INTRODUCTION

We are living in information age where large amount of valuable information is communicating through internet. Our goal is that how to secure the information from unwanted intruder. In this digital world people are getting habituated with e-Banking transaction through internet. People are getting various services through e –Banking such as opening an account, money transfer from one account to another account, bill payment, product purchasing etc. So, customer information has to be secured during the transaction through internet. Cryptography and steganography are the two popular method by which we can provide the security of information.

Cryptography [1], a word with Greek origins, means "Secret writing". We use the term to refer to the science and art of transforming messages to make them secure and immune to attack. Although in the past era cryptography referred only to the encryption and decryption of messages using secret keys, today it is defined as involving three distinct mechanisms : symmetric-key encipherment, asymmetric-key encipherment and hashing.

Steganography [2] is an art of concealment of information through different cover media such as audio, video, text and image. Image steganography is a method where large amount of information is stored into images keeping its visual quality intact with original image. Image steganography is applied in two domain – spatial domain and frequency domain. Our proposed method is focused in spatial domain with colour image.

II. RELATED WORK

There are lot of research works on steganography which have been carried out by researchers. One of the methods is the LSB steganography [3, 4] method where one bit of secret data is embedded into least significant bit position of an image pixel. This approach is very popular for its less time complexity and high capacity of storing secret data into stego image. But this method is very hacking prone. A. Sarkar and S. Karforma [5] have tried to improve the security level of LSB image steganography by selecting the middle region as the beginning pixel and successive diagonal pixel of middle region for further embedding of data through edges of quadrilateral (formed by diagonal pixel) so, that an intruder cannot guess the actual bit position. Data can be hidden into pixel of an image by pixel value differencing [6, 7, 8] method. In this approach capacity of keeping secret bit into stego images depends on pixel value. Through another way we can increase the security of LSB method by hash technique [9]. Here secret bit is stored in different bit position out of four least significant bits using hash key. A number of researchers have tried to introduce steganography method combined with cryptography [10]. In this method data bits are encrypted by different encryption technique and embedded into least significant bit positions. These methods achieve good security level as well as high capacity of storing data in stego image. It is observed that of cryptography combined with steganography takes much higher time than simple LSB method. Visual quality

considerably decreases if multiple bits are embedded into an image pixel. In this case optimization [11] can be applied for better visual quality of a stego image. GA [12] and PSO [13] based optimization have been applied to improve PSNR value for multiple bits embedding process. In this method good capacity can be achieved but complexity has increased much higher than other algorithm. Our proposed method has used two stages security level by selecting middle region based pixel combine with hash function. High capacity and good visual quality of stego image can be achieved by our proposed method.

III. PROPOSED METHOD

Our proposed method may be applied on e-Banking environment where customers transact various secure financial documents through internet. When a customer registers his or her account through e-Banking customer portal, several cover images are sent via e-Banking server for future communication. For Financial transaction our proposed method selects cover image randomly which are already stored into customer portal for embedding the document. After embedding, it produces stego image which is communicated through internet. At the server end secret document are retrieved from stego image with help of original cover image.

Our proposed method has used two technique – pixel selection technique and hash technique for improving security of financial document in e-Banking. The techniques are described as follows.

A. *Pixel Selection Method.*

We have applied our proposed method on 24 bit colour image. We have embedded three bit for each pixel i.e. one bit for each red, green and blue pixel. We have introduced a novel pixel selection method where secret message are embedded. We first select middle region of an image which is a collection of pixels. We proposed a technique for selection of middle region. We consider the four cases depending upon height (row) and width (column) of an image. Height (row) and width (column) may be odd-odd, even-even, odd-even and even -odd. Each case can be further divided into two sub cases depending upon height (row) greater than width (column) or width (column) greater than height (row). We select red colour as middle region which is depicted in fig. 2-3. If height (row) or width (column) is odd then we select single column or single row as a middle region respectively. If height (row) or width (column) is even then we select two columns or two rows as middle region. After selection of middle region we embed the data bit into the middle region. Next we select four

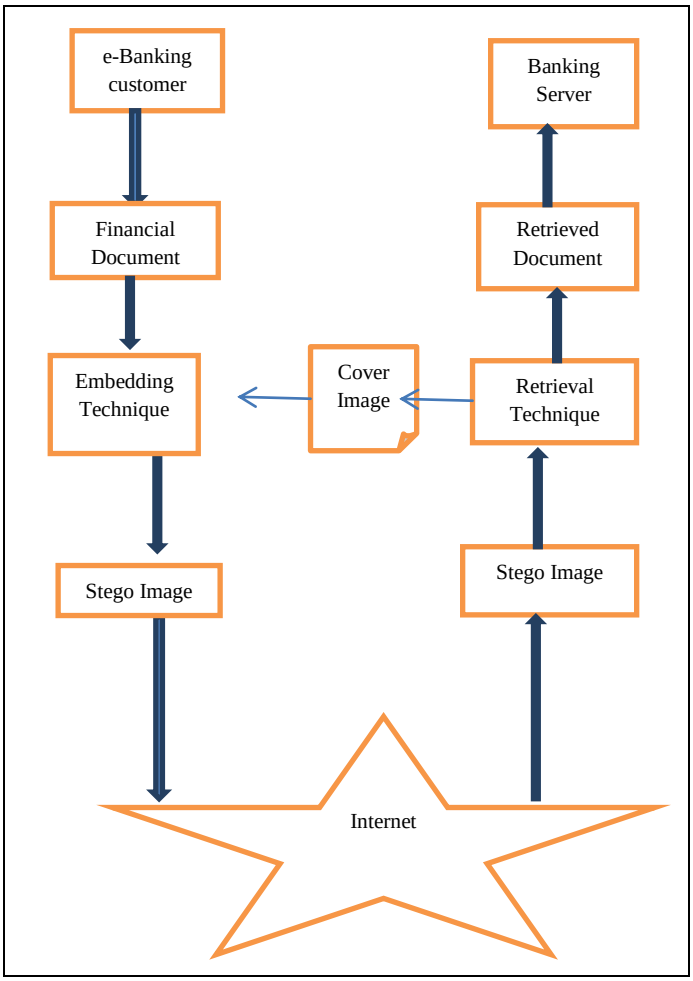


Figure 1. Proposed Model

diagonal pixel of middle region .Here (x1, y1), (x2, y2), (x3, y3) and (x4, y4) are four diagonal pixels. We embed the secret bit from (x1, y1) to (x2, y2), (x2, y2) to (x3, y3), (x3, y3) to (x4, y4) and(x4, y4) to (x1, y1).Again we select four diagonal pixels and embed the data bit into the pixels same way. Green and blue region depicts the successive region.

Examples

Here we consider two examples among eight cases.

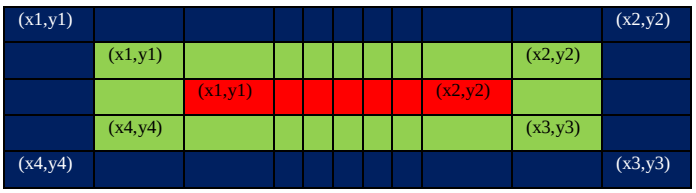


Figure 2. row=5, column=11 and column > row

From fig. 2 row=5, column=11 and column > row. Single row is selected as middle region. Here pixel counting starts from upper left corner as (1, 1).For red region the starting pixel x1=ceil (N/2), y1=Ceil (N/2) .N=row i.e. N=5 and x1=3, y1=3.The end pixel is End pixel x2=N/2, y2=Ceil

(N/2) +p. Here p=column-row i.e. p=6 and x2=3, y2=9.Next diagonal pixels are (x1,y1)=(2,2),(x2,y2)=(2,4),(x3,y3)=(3,3) and(x4,y4)=(4,3).

From fig 3 row =9 and column=6 and row > column. Here pixel counting starts from upper left corner as (1, 1). Two columns are selected as middle region. Here N=6 and p=3. .For red region starting pixels are x1=3, y1=3 and x2=3, y2=4. End pixel corresponding to (x1, y1) is x4=7, y4=3. End pixel corresponding to (x1, y1) is x3=7, y3=4.Next diagonal pixels are (x1,y1)=(2,2),(x2,y2)=(2,4),(x3,y3)=(8,5),(x4,y4)=(8,2).

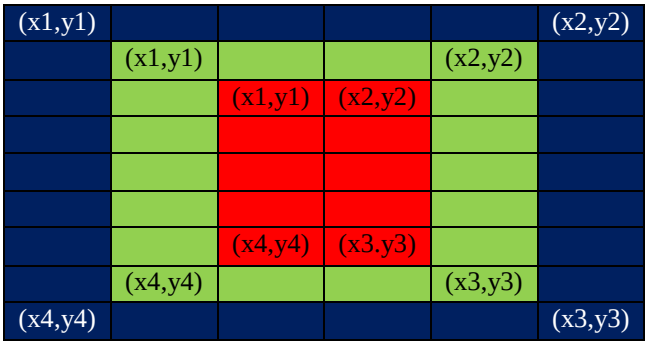


Figure 3. row=9, column=6 and row>column.

B. *Hash Technique*

After selection of the pixel of an image we have used variable hash key for the detecting LSB bit position (up to 4 bit) where secret bit are embedded. We have used following hash function to calculate bit position.

Pixel value % hash key=bit position

We select hash key two (2) for pixel value 0 to 64, three (3) for pixel value 65 to 128 and four (4) for pixel value 129 to 256. So we obtain (0, 1) bit position for pixel value 0 to 64, (0, 1, 2) bit position for pixel value 65 to 128 and (0, 1, 2, 3) bit position for pixel value 129 to 256.

C. *Embedding Algorithm*

Step 1: if row > column
N=column
P=row-column
Else
N=row
P=column-row
Step 2: If N is odd then go to case I otherwise (even) go to case II

Case I:
Start pixel x1=ceil (N/2), y1=ceil (N/2)
If row >= column
End pixel x2=ceil (N/2) +p, y2=N/2
Else
End pixel x2=N/2, y2=ceil (N/2) +p
(Here single row or column will be selected as a middle region)
(HASH KEY SELECTION)
If (pixel value>=0 to pixel value<=64)
Hash key=2
Bit position=pixel value % hash key
Else If (pixel value>=65 to pixel value<=128)
Hash key=3
Bit position=pixel value % hash key
If (pixel value>=129 to pixel value<=256)
Hash key=4
Bit position=pixel value % hash key
Embed the secret data into the bit position of an image from start to end pixel.
Select next four diagonal pixels of the middle region.

Case II:
If row >=column
(Here two consecutive column are selected as middle region)
Start pixel x1=N/2, y1=N/2.
Another start pixel x2=N/2, y2=N/2+1
End pixel corresponding to (x1, y1) is x4=N/2+p+1, y4=N/2
End pixel corresponding to (x2, y2) is x3=N/2+p+1, y3=N/2+1
Else
(Here two consecutive rows are selected as middle region)
Start pixel x1=N/2, y1=N/2
Another Start pixel x4=N/2+1, y4=N/2
End pixel corresponding to (x1, y1) is x2=N/2, y2=N/2+p+1
End pixel corresponding to (x4, y4) is x3=N/2+1, y3=N/2+p+1
(HASH KEY SELECTION)
If (pixel value>=0 to pixel value<=64)
Hash key=2
Bit position=pixel value % hash key
Else If (pixel value>=65 to pixel value<=128)
Hash key=3
Bit position=pixel value % hash key
If (pixel value>=129 to pixel value<=256)
Hash key=4
Bit position=pixel value % hash key
Embed the secret data into the bit position of an image from start to end pixel (either consecutive two rows or two columns).
Select next four diagonal pixels of the middle region.
Step 3: Select the pixel that covers four edge of quadrilateral through corners (x1, y1), (x2, y2), (x3, y3) and (x4, y4) clockwise and use above hash key selection technique for embed the data.
Step 4: Increment each four pixel diagonally and go to step 3 until end of row or column is reached or end of secret bits is reached.

D. *Retrieval algorithm*

(Receiver keeps original image or when a customer open an account using e-banking, the server already send some images for its communication)

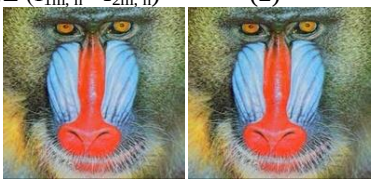
Step1: we select middle region of an original image as embedding algorithm and retrieve the secret bits from bit position of a pixel using hash key method with help of original cover image which already store into Banking server.
Step 2: select four diagonal pixels and retrieve the secret bits from bit position of a pixel using hash key method.
Step 3: process continue until the all the secret bits are retrieve.

IV. RESULT AND ANALYSIS

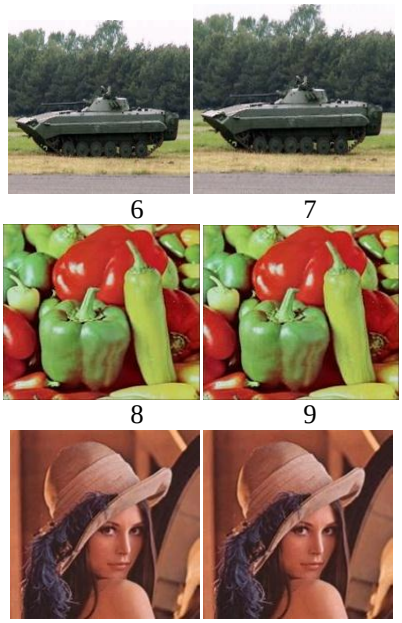
This section represents the results; discussion in terms of visual interpretation, peak signal to noise ratio and histogram analysis and extensive analysis has been made on various images using our hash based LSB method. Here we use four bmp images of different size namely Lena, Baboon, Pepper and Tank. Fig. 4-11 shows the host images and corresponding stego images. Fig. 12-19 shows Luminosity histogram of four images. Here we use text as input data to embed into cover images. Table 1 shows different capacity value of cover image in bits with PSNR of various size images. Table 2 shows PSNR values of Lena image with different capacity. It is observed that PSNR varies with different capacity of secret bits. Lower capacity means higher PSNR and higher capacity means lower PSNR. Fig. 20-23 shows the Luminosity histogram of Lena image with variable capacity of secret bits. We can obtain optimized PSNR (50-55) by embedding bits with ranging from 20000 to 40000.Table 3 shows capacity (bits) comparison analysis of proposed method with PVD [6] and PVD [7]. Table 4 shows PSNR comparison of proposed method with PVD [6] and PVD [7]. From the above results it is seen that a high capacity of embedding has been achieved in terms of good PSNR. It is also observed that the capacity of stego image is variable from one image to other image of same size in case of PVD [6] and PVD [7] whereas in our proposed method the capacity remains unchanged from one image to other image of same size. Fig.23 shows 2-D diagrammatic representation of capacity of PVD [6] and PVD [7] with proposed method. Fig 24 shows the 2-D diagrammatic representation of PSNR values of PVD [6] and PVD [7] with proposed method.
The Equation (1) and Equation (2) are used to calculate PSNR and MSE.

$$PSNR=10 \log (\max (I_{m,n}^2)/MSE) \quad (1)$$

$$MSE=1/M*N\Sigma (I_{1m,n}- I_{2m,n})^2 \quad (2)$$



4 5



6 7 8 9 10 11

Figure 4. (Baboon), 6 (Tank), 8 (Pepper), 10 (Lena) are cover image and 5, 7, 9, 11 are the corresponding stego images.

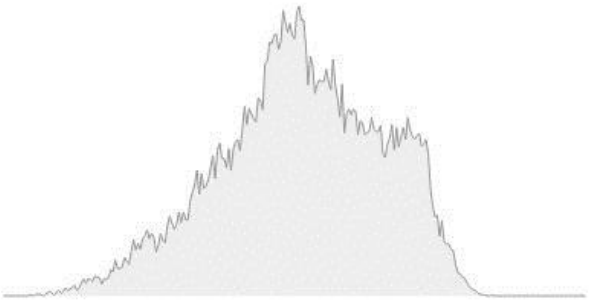


Figure 12. Luminosity histogram for Baboon cover image.

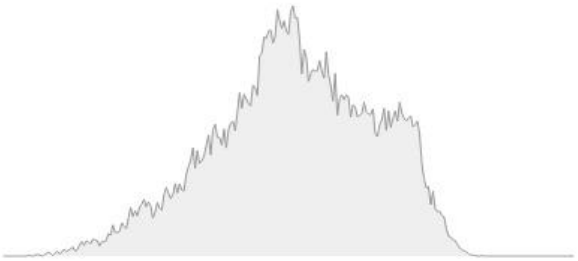


Figure 13. Luminosity histogram for Baboon stego image (98% embedding).

Figure 14. Luminosity histogram for Lena cover image.

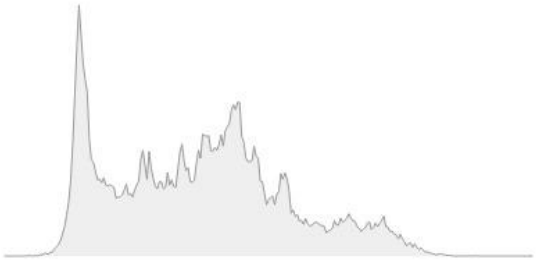


Figure 15. Luminosity histogram for Lena stego image (98% embedding).

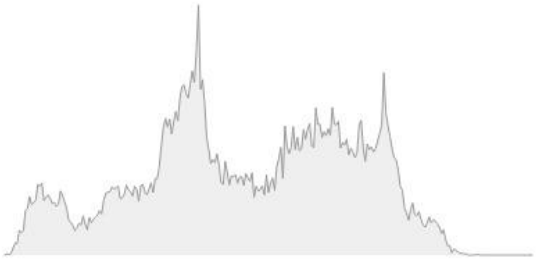


Figure 16. Luminosity histogram for Pepper cover image.

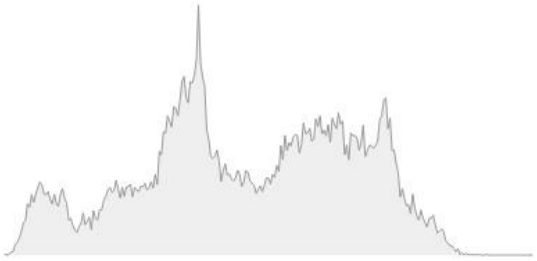


Figure 17. Luminosity histogram for Pepper stego image (98% embedding).

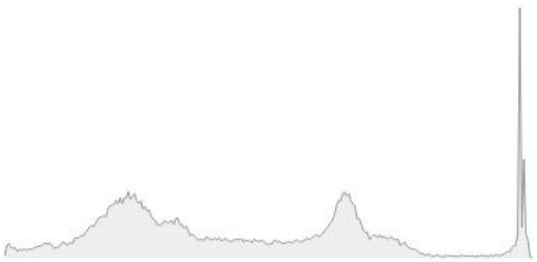


Figure 18. Luminosity histogram for Tank cover image.

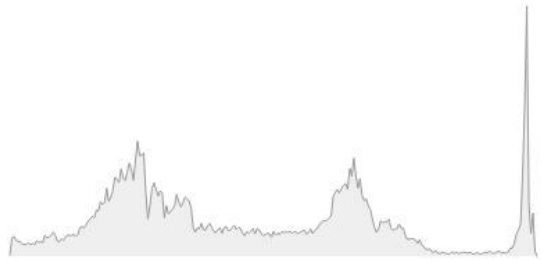


Figure 19. Luminosity histogram for Tank stego image.

Table 1: Capacity, Size, PSNR Values of Stego Images

Image name	Dimension	Image Size(kb)	No of bits to be embedded	Percentage(%) of embedding	PSNR
Tank	281×202	168	85756	50	48.94
			167400	98	44.21
Baboon	196×185	106	52820	50	46.45
			105641	98	43.65
Lena	255×255	191	97537	50	48.48
			192027	98	45.01
Pepper	185×165	89.7	45787	50	46.52
			89487	98	44.32

Table 2: PSNR Values of Lena Stego Images with Different Capacity

Image name	Dimension	Image Size(kb)	No of bits to be embedded	PSNR
Lena	255×255	191	10000	58.58
			20000	55.52
			40000	52.32
			80000	49.40
			120000	47.29
			160000	45.83

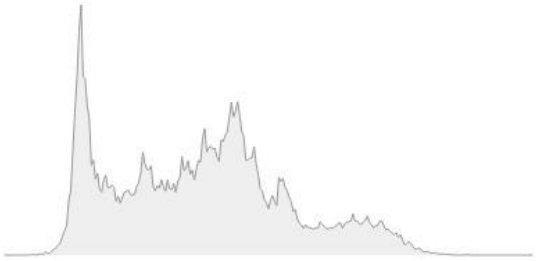


Figure 20. Luminosity histogram for Lena stego image (20000 bits embedding).

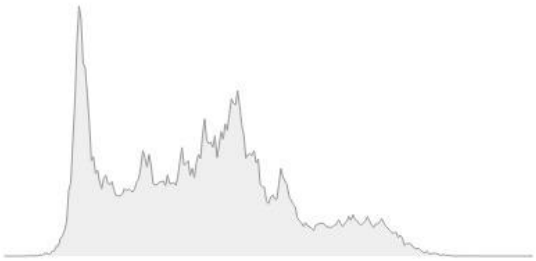


Figure 21. Luminosity histogram for Lena stego image (80000 bits embedding).

Figure 22. Luminosity histogram for Lena stego image (120000 bits embedding).

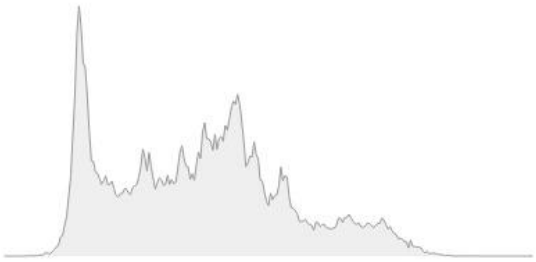


Figure 23. Luminosity histogram for Lena stego image (160000 bits embedding).

Table 3: Capacity Comparison of PVD [6] & PVD [7] with Proposed Method.

Cover image Size 512 × 512	Maximum Capacity (bits) of PVD [6] Method	Maximum Capacity (bits) of PVD [7] Method	Maximum Capacity (bits) of Proposed Method
Lena	50960	145787	784432
Baboon	56291	144916	784432
Pepper	50685	145995	784432

Table 4: PSNR Comparison of PVD [6] & PVD [7] with Proposed Method.

Cover image Size 512 × 512	PSNR(dB) values of PVD[6] Method	PSNR(dB) values of PVD[7] Method	PSNR (dB)values of Proposed Method
Lena	41.70	42.26	45.01
Baboon	36.86	38.44	43.65
Pepper	40.55	42.28	44.32

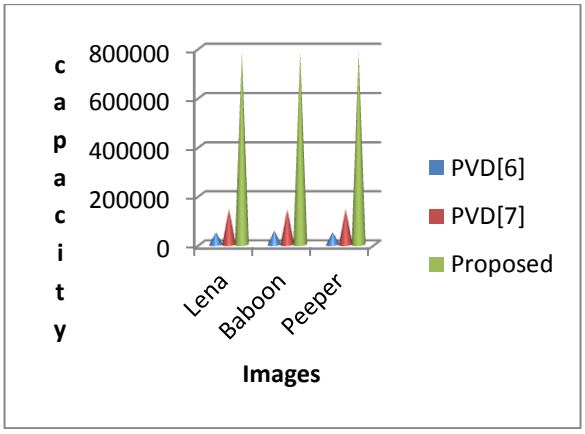


Figure 24. Capacity comparison of proposed method with PVD [6] and PVD [7]

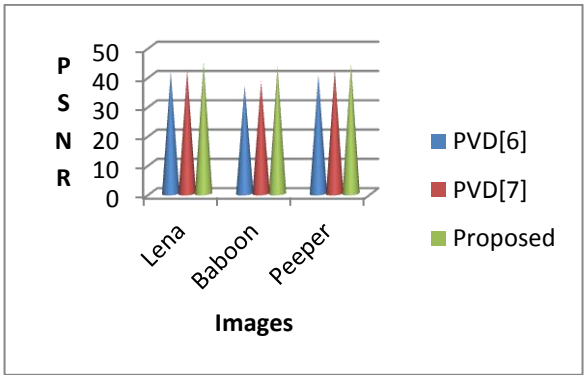


Figure 25. PSNR comparison of proposed method with PVD [6] and PVD [7]

V. CONCLUSIONS

This paper proposes one new pixel selection using a suitable hash function. From experimental analysis it is clear that proposed method achieved high PSNR along with good capacity for various images. In future the PSNR and capacity of images may be further increased by improvement of our proposed method. Our proposed method can be applied on document associated with e-governance, e-commerce, e-learning etc where valuable information is transacted through internet.

REFERENCES

[1] Behrouz A. Forouzan , "Data Communication and Networking ",MacGraw Hill Education (India) Private Limited.

[2] N. Provos, P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy, Vol. 1, No. 3, pp. 32–44,2003 .

[3] A. Kumar ,K. M. Pooja , "Steganography a Data Hiding Technique" , International Journal of Computer Applications, Vol-9,No-7,Nov 2010.

[4] W. bender, D. Gruhl, N. Morimoto, A.Lu, "Techniques for data hiding", IBM Systems Journal Vol. 35(3-4),pp. 313-336, 1996.

[5] A. Sarkar, S.Karforma, " A new pixel selection Technique of LSB based steganography for data hiding",IJRCS, Vol-5,Issue-3,pp.12-125,March 2018.

[6] D.C. Wu, and W.H. Tsai, "A Steganographic method for images by pixel-value differencing", Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003.

[7] J. K. Mandal ,D. 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.

[8] H.C. Wu, N.I. Wu, C.S. Tsai , M.S. Hwang, "Image Steganographic Scheme Based on Pixel Value Differencing and LSB Replacement Method", IEEE Proceedings on Vision, Image and Signal processing, Vol. 152, No. 5,pp. 611-615, 2005.

[9] G.R. Manjula ,A. Danti "A novel hash based LSB (2-3-3) image steganography in spatial domain", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol. 4, No 1, February 2015 .

[10] P. Bharti ,R. Soni, " A new approach of data hiding in images using cryptography and Steganography",IJOCA,vol. 58,no. 8,Nov 2012.

[11] Ali Akbar Nikoukar, "An Image Steganography Method with High Hiding Capacity Based on RGB Image", International Journal of Signal and Image Processing, Vol. 1,Issue.4, pp. 238-241,2010.

[12] Ran Zan Wang, Chi Fang Lib, Ja Chen Lin, "Image hiding by optimal LSB substitution and Genetic algorithm", Pattern Recognition Society. Published by Elsevier Science Ltd., pp.671-683, 2001.

[13] N. Kaur, A .Garg, "Steganography Using PSO Based Hybrid Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering,Vol-4,Issue.1,Nov 2014.

Author's Profile

A. Sarkar is a research scholar under University of Burdwan, Burdwan, India. He has completed M.C.A from university of Burdwan. His fields of research work are Cryptography and Steganography

S. Karforma has completed B.E and M.E in Computer Sc. And Engineering from Jadavpur University and completed his PhD in Computer Science from The university of Burdwan. He is currently serving as Professor and Head of the Department of the Computer Science in The University of Burdwan. His research area includes Cryptography and Bio-informatics. He has published more than 100 research papers in many reputed national and international journal and conferences including 2 books and 2 book chapters in reputed publishing agencies. He has successfully supervised 4 PhD dissertations.

