ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 12, December 2015

A Novel Approach for hiding data in Image Steganography by using Three Pixel Pair Differencing Method

Vidya S Shirguppi

Abstract— **A novel steganographic approach using Three pixel-Pair value differencing (TPVD) is proposed here which contains the Implementation of how to enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision. I am using TPVD to upgrade the hiding capacity of original PVD method which refers to only one direction, but in TPVD three different directional edges are considered and effectively adopted to design for Communication system. The main approach is to reduce the quality distortion of stego-image brought from setting larger embedding capacity, and optimal selection of the reference point for which adaptive rules are presented.**

I. INTRODUCTION TO STEGANOGRAPHY

In our day to day life we communicate with one another in the different place of the world by using the internet.[2] Internet users frequently receive, store, send their private information through internet while doing this the common way is to transform data into a different form of communication to keep the unauthorized users away and for that purpose one of the secure technique is steganography .

In this paper I have proposed a new method which hides the image, text inside an image without damaging the original image and this is done by using the Triway-Pixel value differencing method. Here I have designed an algorithm through which the data which is in the form of text is hidden behind the original image that is cover image and send by using the TPVD Method. Then after embedding process At the Receiver side the stego image is form which is approximately as same as original image and receiver can extract the message. I am using a three pixel pair value through which the I will get large hiding capacity and data will be secured from unauthorized users.

Department of Electronics & Telecommunication Engineering, D.Y. Patil College of Engineering & Technology, Kolhapur [2]vice-principal, H.O.D.(IT), D.Y. Patil College of Engineering & Technology, Kolhapur

Review of steganographic Techniques

There are six techniques of Steganography which are as follows:

[1] Substitution Techniques
[2] Transform Domain Techniques
[3] Spread Spectrum Technique
[4] Statistical Techniques cover block
[5]Distortion Techniques
[6] Cover Generation Techniques.[4]

Thus these are some of review methods for hiding data, for security purpose. The rest of paper is organized as follows. Section II Present Method, Section III discussion of result obtained , Section IV Conclusion, Section V References.

II. PRESENT METHOD

The present work is implemented by using the images which are BMP, GIF, BITMAP, and JPEG. Which are known as steganographic images .In this method two types of data base is used first is for Text and second for Image , as the Secret text is to be hide inside an image the first text is browsed from data base and then the image is browsed in which the text is to be hide and they are embedded together and send to the receiver side the data is extracted and it is in form of stego image which is similar to original image.

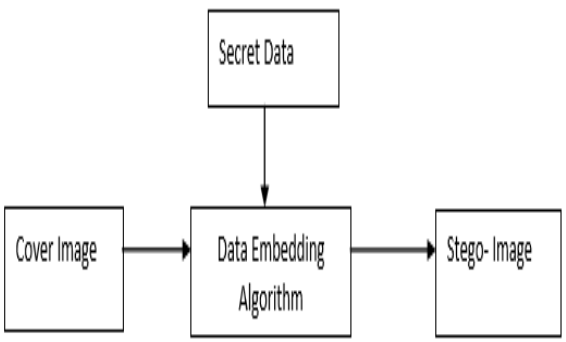


Figure 1. Block diagram of Present method.

A. *Embedding Process*

In Embedding Process data hiding steps are carried out as follows. An cover image is taken into which Secret data is to be hide. By using three pixel pair an data is embedded. The cover image is partition into 2*2 pixel pair without overlapping each other. After inputting data it is converted form binary to decimal form to find optimal selection and reference point.

B. *Stego Image*

The combination of original image or cover image and secret data is called as Stego Image.

C. *Extraction Process*

The Extraction Process is to retrieve the secret data from stego image. Here a new difference value is generated for each pixel pair and that value is subtracted from original difference value which separates out the stego image and secret data.

III. IMPLEMENTATION OF SYSTEM

A. *Embedding Algorithm*

1.Calculate four difference value for four pixel pair.
2.Locate the four pixel pair to designed the range table.
3.Compute the secret data into bit embedded in each pair from the width.
4.The original value satisfies the two condition for pixel section otherwise TPVD is selected.
5.Read the bit form and convert binary data to decimal form.
6. Calculate the new difference value obtained for four pair
7. Modify the value.
8. Select the MSE by optimal selection .

Figure 2. Algorithm for Embedding

B. *Extraction Algorithm*

1. Partition the stego image into 2*2 pixel block.
2. Calculate the difference value for each pixel block of stego image.
3. If branch condition are satisfied then two pixel are selected otherwise three pixel are selected.
4. The original value satisfies the two condition for pixel section otherwise TPVD is selected.
5. After range table is located difference bit is

Figure 3. Algorithm for Extraction.

D. *Flow chart for Present System*

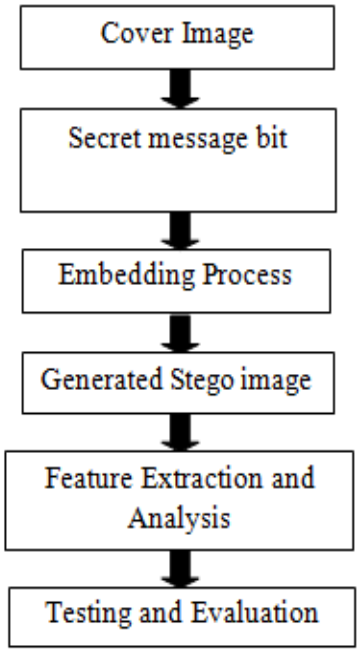


Figure 4. Flowchart of System

IV. RESULT ANALYSIS

Figure 5. GUI of PVD and TPVD Method.

A. Capacity and PSNR.

Capacity means the hiding capacity in bytes and the PSNR value is utilized to evaluate the invisibility of the stego images. It is calculated in db. The listed values are the results after embedding randomly generated bit sequence.

B. Histogram.

Histogram Refers to the graphical representation of pixel value differencing which is different for original and stego image.

C.COMPARATIVE ANALYSIS

Figure 6. Comparative analysis of Image

TABLE I

D.COMPARISON RESULT OF TWO METHODS FOR PROPOSED METHODS AND PVD METHOD

SR NO.	SAMPLE IMAGES	PVD METHOD		TPVD METHOD	
		PSNR (db)	CAPACITY (bytes)	PSNR (db)	CAPACITY (bytes)
1.	BRIDGE	81.6	48	76.7	48
2.	COUPLE	84.9	88	80	168
3.	EDGES	80.9	168	72.3	664
4.	GIRLFACE	76.8	576	61.3	8888
5.	HOUSE	61.8	8424	59.1	9752
6.	KEIL	59.3	28392	54.9	36960

Here Six Bmp Images are taken for comparison and the results are then compared using various BMP Images as shown in Experimental result had shown the strong point of this method as compare to PVD methods. For this method we embedded the secret image in cover image and get stego image. The PSNR(Peak Signal to Noise Ratio) & Capacity of stego-image is calculated and compared with previous work.

.

Above results can be graphically represented for both PSNR as below:

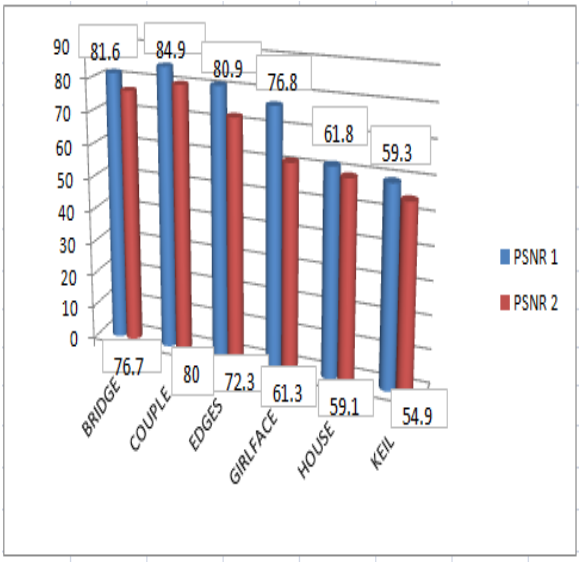


Figure 7.PSNR Values for PVD & TPVD Result.

Above results can be graphically represented for both Capacities as below:

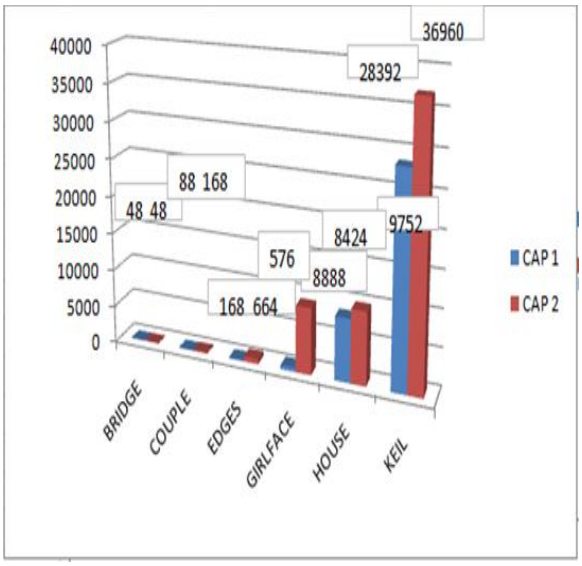
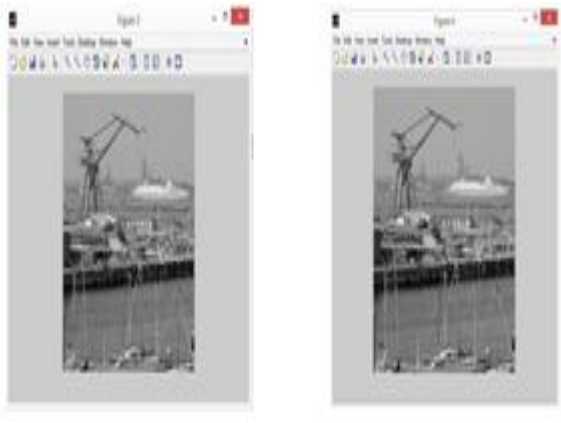
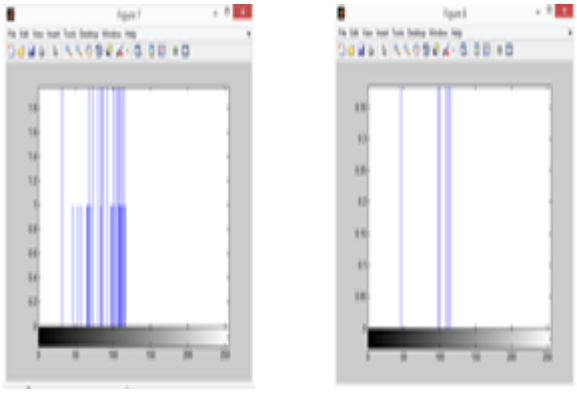


Figure 8.Capacity Values for PVD & TPVD Result.

E.FINAL STEGO IMAGE OBTAINED AND ORIGINAL IMAGE WITH THERE HISTOGRAM OUTPUTS.



HISTOGRAM OF ABOVE IMAGE.



V. CONCLUSION

As the steganography technique is one of the popular and used by everyone so to resolve the needs that is why a new method Triway Pixel Value Differencing which is based on steganography used which enlarge the capacity and decreasing PSNR Value so that there is imperceptible image for human vision.

REFERENCES

[1]] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "*Information Hiding - a Survey,"* Proceedings of the IEEE, Vol. 87, pp. 1062–1078, 1999.

[2] Ali Shariq Imran, M. Younus Javed, "A Robust Method for Encrypted Data Hiding Technique Based on Neighborhood Pixels Information," *World Academy of Science, World Academy of Science, Engineering and Technology 7 2007*

[3] 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 Proceedings on Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005.*

[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] Norishige Morimoto, "Digital Water Marking Technology with Practical Application" Information Science Special Issues on Multimedia Information Technologies-Part 1 Vol 2 No 4 1999.