



STEGANOGRAPHY TO HIDE INFORMATION WITHIN IMAGE FILE

Shital Shirish Aherkar

Department of Electronics and Telecommunication, S.E.S.Polytechnic, Solapur-413002, India.

(Email: shtlaherkar@gmail.com)

ABSTRACT

Digital steganography exploits the use of a host data to hide a piece of information in such a way it is imperceptible to a human observer. In this paper we propose an image steganography system, in which the data hiding (embedding) is realized in bit planes of subband wavelets coefficients obtained by using the Integer Wavelet Transform (IWT). To increase data hiding capacity while keeping the imperceptibility of the hidden data, the replaceable IWT coefficient areas are defined by a complexity measure used in the Bit-Plane Complexity Segmentation Steganography (BPCS). The proposed system shows a high data hiding capacity.

KEY WORDS: Bit plane complexity segmentation, Integer wavelet transform, steganography, stegoimage.

INTRODUCTION

The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication to be done should be kept secret. Cryptography is a technique to scramble a confidential message to make it unreadable for a third party. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. It is commonly used in the Internet communications today. Cryptography can hide the content of the message but it cannot hide the location of the secret message. It is the reason why an encrypted message can be targeted by the attackers.

Watermarking is another information hiding technique which is used for hiding actually embedding some digital evidences, symbol data or in the valuable digital data such as a photo picture, musical sound, digital movie, etc. The purpose of the watermarking is to protect copyright and/or ownership of the data. In this technique the robustness of the embedded evidence that can be very small is treated as most important. In watermarking the valuable information is the external information that is visible/audible. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Steganography is the ancient art of embedding a secret message into a seemingly harmless message. Most of the newer applications use steganography like a watermark to protect a copy right on information. The forms of steganography vary but unsurprisingly innocuous spam messages are turning up more often containing embedded text. A new transform domain technique for embedding the secret information in the integer wavelet transformed cover image is implemented here. Many different carrier file formats can be used in steganography, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden.

WORK DESIGN

Enhanced Steganography is a method of hiding the message in image files, in which the IWT and BPCS are used to get high data hiding capacity and low perceptibility. IWT is used to decompose the cover image. BPCS takes the advantage of human visual system which cannot recognize changes in complex positions of the image. The experimental results show different hiding capacities based on the cover image chosen. The data extracted from the cover image also depends on the pixel values of the image. The system can be further developed to hide secret image in cover image.

In the dissertation the researcher has proposed a lossless data hiding method using IWT and BPCS, in which image data are decomposed by IWT and each bit plane of the sub-bands segmented in 8x8 blocks. All blocks are analyzed by complexity measures to determine which blocks will be replaced by secret message. The complexity measurement used

in the proposed system is same one in the BPCS method. The proposed system can recover the hidden message in lossless manner if the communication channel is ideal. A wavelet transform that maps integers to integers is the S-transform.. In it large amounts of data can be compressed as smaller one by using IWT method, without data loss.

The system is used to produce same quality of image while compressing and embedding the image, there will be no change in the quality of image and can be retained the same as the first. By using BPCS (Bit Plane Complexity Segmentation) the embedding process has been done here, so the security is very high for the embedded image. BPCS-Steganography is a new steganographic technique which can embed confidential information in vessel data that is typically a true color image (24-bit BMP format) and sometimes in an 8-bit indexed color image. Embedding (actually, replacing) is made on the bit-planes of the image. The most important feature of the steganography is that its embedding capacity is very large.

Hiding Process

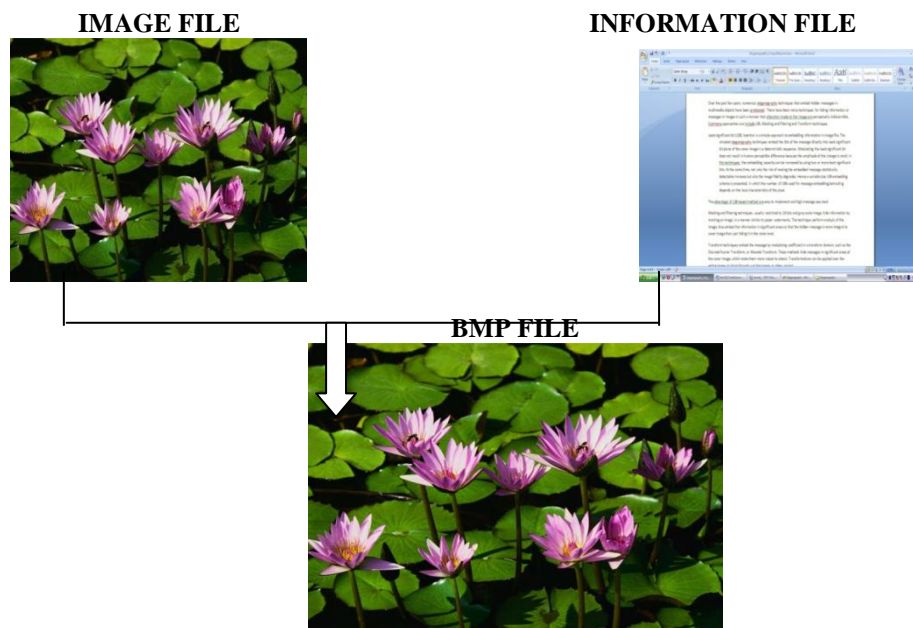
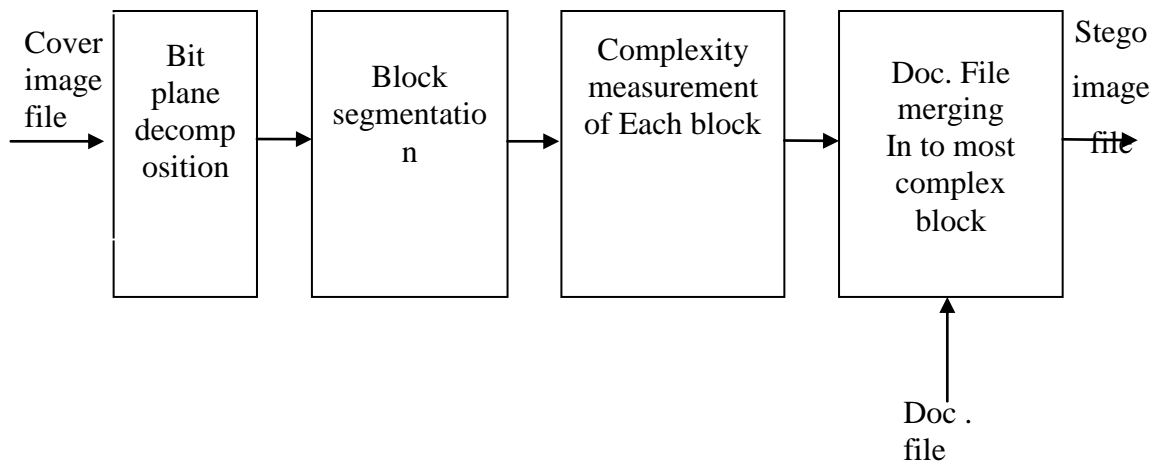


Figure 2.1.Embedding document



Extracting Process

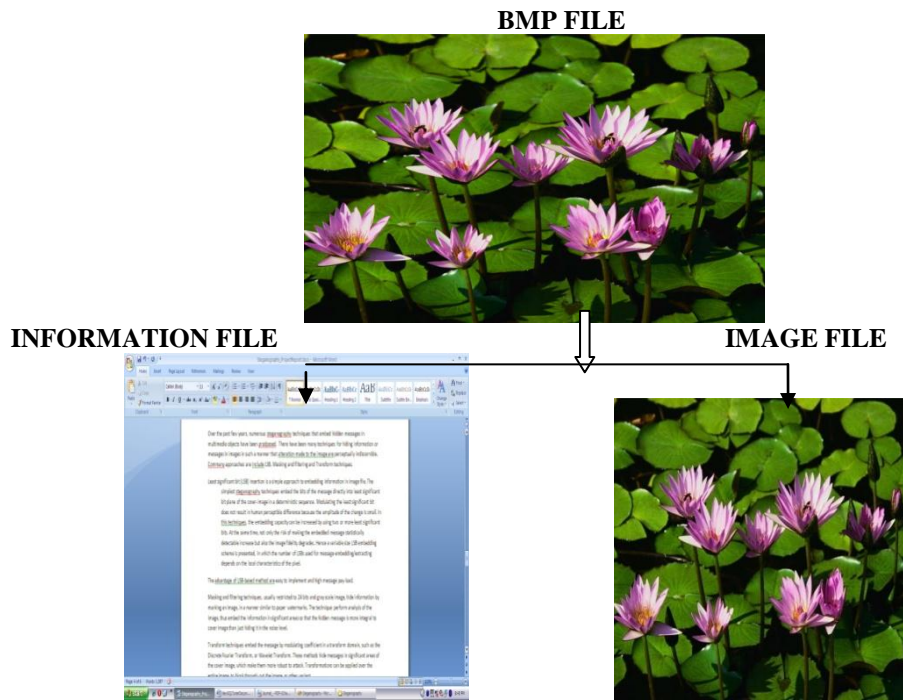


Figure 2.3 Extracting document

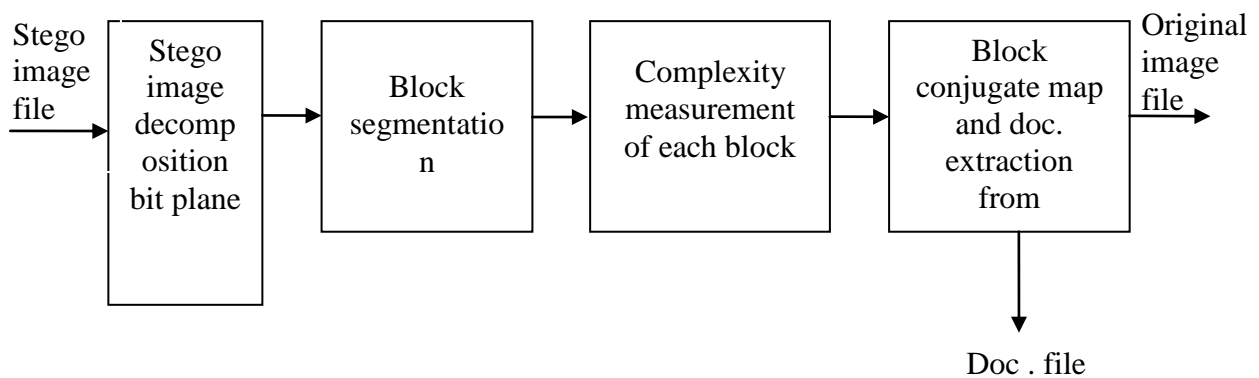


Figure 2.4 : Output side block diagram to Extracting document from image file Embedding Method

- a). Transformed image is decomposed into bitplanes.
- b). Each plane is segmented into 8X8 blocks and complexity is measured for each block.
- c). Threshold value is chosen to determine whether the block is complex or non-complex.
- d). Each 8 letters form a block of message, and complexity is measured for each message block.
 - If a message block is determined as no-complex block, the message block is conjugated.
 - i. Conjugation map is constructed from conjugated blocks.
 - ii. Complex image blocks are replaced by message blocks.

Extracting method 1

- Transformed image is decomposed into biplanes.
- Each plane is segmented into 8X8 blocks and complexity is measured for each block.
- Threshold value is chosen to determine whether the block is complex or non-complex.
- Secret message is extracted from the complex blocks, blocks are conjugated if necessary based on conjugation map information



Extracting method 2

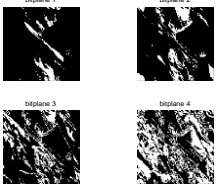
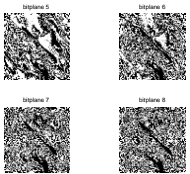


- Transformed image is decomposed into biplanes.
- Each plane is segmented into 8X8 blocks and.
- Each element of original image is compared with stegoimage if it is not equal then it is treated as a element of secret message and it is extracted.

RESULTS



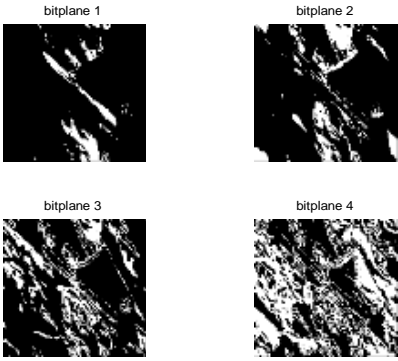
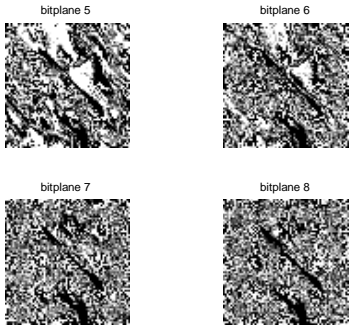
3.1) BABY IMAGE

3.1.1) Image Photographs of Embedding

Sr. No.	Output at different steps	Description
1.		Original Image Size-256x256x3
	The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication to be done in secrete.	Original document
2		IWT Image Size-128x128x3 Formula used- $A_{i,j} = (I_{2i,2j} + I_{2i+1,2j}) / 2$ $H_{i,j} = I_{2i,2j+1} - I_{2i,2j}$ $V_{i,j} = I_{2i+1,2j} - I_{2i,2j}$ $D_{i,j} = I_{2i+1,2j+1} - I_{2i,2j}$

3		<p>Bit plane segmentation of Red Component of IWT image Into 8 bit plane Each plane size-128x128x1 (Plane-1,2,3,4)</p>
Sr. No.	Output at different steps	Description
4		<p>Bit plane segmentation of Red Component of IWT image Into 8 bit plane continued Each plane size-128x128x1 (Plane-5,6,7,8)</p>
5		<p>Image after embedding text document Size-128x128x3</p>
6		<p>Restore Stego Image after taking IIWT,Size-256x256x3 Formula used- $I_{2i, 2j} = A_{i,j} - [H_{i,j} / 2]$ $I_{2i, 2j+1} = A_{i,j} + [H_{i,(j+1)/2}]$ $I_{2i+1,2j} = I_{2i, 2j+1} + V_{i,j} - H_{i,j}$ $I_{2i+1, 2j+1} = I_{2i+1,2j} + D_{i,j} - V_{i,j}$ PSNR- 40.0042db</p>

3.1.2) Image Photographs of Extracting

Sr. No.	Output at different steps	Description
1.		<p align="center">Stego Image Size-256x256x3</p>
2		<p align="center">IWT of stego Image Size-128x128x3 Formula used- $A_{i,j} = (I_{2i,2j} + I_{2i+1,2j}) / 2$ $H_{i,j} = I_{2i,2j+1} - I_{2i,2j}$ $V_{i,j} = I_{2i+1,2j} - I_{2i,2j}$ $D_{i,j} = I_{2i+1,2j+1} - I_{2i,2j}$</p>
3		<p align="center"><i>Bit plane segmentation of Red component of IWT image</i> Into 8 bit plane Each plane size-128x128x1 (Plane-1,2,3,4)</p>
4		<p align="center">Bit plane segmentation of Red Component of IWT image Into 8 bit plane continued Each plane size-128x128x1 (Plane-5,6,7,8)</p>
5	<p>The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication to be done in secrete..</p>	<p align="center">Extracting document</p> <p align="center">BER-0% BPP - 0.1260</p>

The following two methods have been used for extracting secret document

Method1-By comparing complexity of blocks of original image and stegoimage

Method2-By comparing each elements of original image and stegoimage

Table 3.1: Comparison between original and extracted document by method1 and method2 for Baby image

Original Document	Extracted Document by Method1	Extracted Document by Method2
Steganography today is a computer technique to make confidential information imperceptible to human eyes by embedding it in some innocent looking "vessel" data (aka "carrier", "cover" or "dummy" data) such as a digital image or a speech sound	Steganography today is a computer technique to make confidential information imperceptible to human eyes by embedding it in some innocent looking "vessel" data (aka "carrier", "cover" or "dummy" data) such as a digital image or a speech sound. No.of Errored bits-774/2800 Ratio- 0.2764	Steganography today is a computer technique to make confidential information imperceptible to human eyes by embedding it in some innocent looking "vessel" data (aka "carrier", "cover" or "dummy" data) such as a digital image or a speech sound. No.of Errored bits-0 Ratio- 0

Method1-By comparing complexity of blocks of original image and stegoimage

Method2-By comparing each elements of original image and stegoimage .

In above table there is no error in extracted document by method 2

Table 3.2: Comparative values of different parameter experimented on image 'Baby'

Sr. No.	Length of doc.in terms of No. of char.	PSNR for both Methods	BER Method1	BER Method2	CAP
1	50	40.0006	0.0022	0	194619
2	100	40.0053	0.0345	0	194187
3	200	40.005	0.1849	0	193259
4	400	40.00444	0.2535	0	191683
5	500	40.004	0.2813	0	190851
6	1000	40.0006	0.3238	0	186635
7	1500	39.9999	0.3294	0	182395
8	2000	39.9974	0.3321	0	178283
9	2500	39.9917	0.3324	0	174115

Method 1-By comparing complexity of blocks of original image and stegoimage

Method 2-By comparing each elements of original image and stegoimage

The above table reveals that as the Length of document increases, PSNR, CAP reduces. BER increases by Method 1, BER reduces to '0' by Method 2.

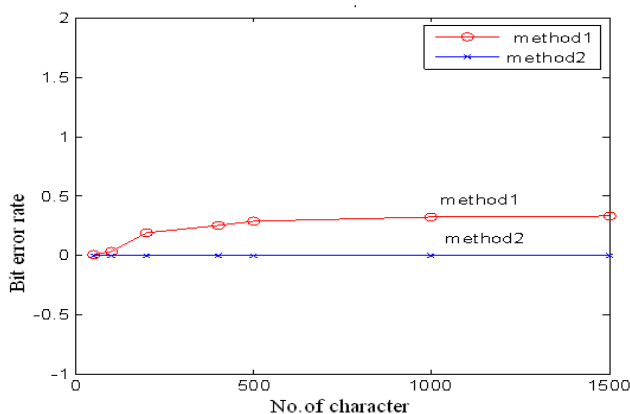


Figure: 3.1 Graphical representation of no. of character hide vs bit error rate experimented on baby image

Above graph shows that as length of character increases then bit error rate is almost reduces to zero by method 2.

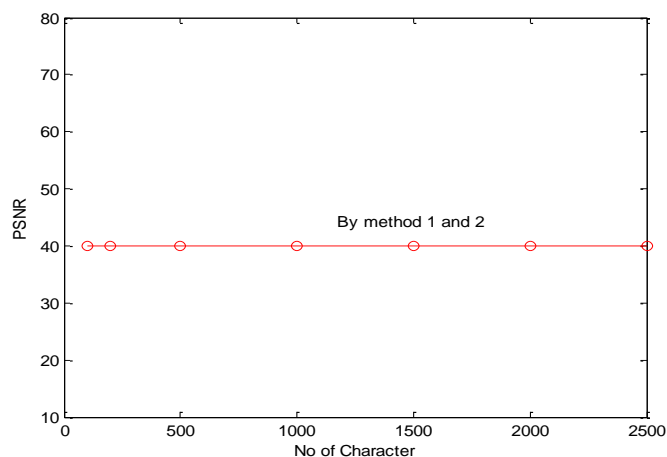


Figure: 3.2: graphical representation of no. Of character hide vs psnr experimented on baby image

Above graph shows that as length of characters increases PSNR of image slightly change.

CONCLUSIONS

A lossless steganography system is designed in which the IWT and BPCS are used to get high data hiding capacity and low perceptibility. IWT is used to decompose the cover image. BPCS takes the advantage of human visual system which cannot recognize changes in complex positions of the image. The data extracted from the cover image also depends on the pixel values of the image.

In above technique PSNR of different images for same document are observed which shows a quality measurement between the original and reconstructed image. The higher the PSNR, the better is the quality of the reconstructed image. The first picture of 'Baby' has PSNR more than 40db i.e. without much deterioration reconstructed image is observed. It is also observed that bit error rate for different length of hiding document is almost zero. Also there is no greater change in PSNR in spite of change in the length of hiding document. It shows that using above technique high quality reconstructed image can be retrieved with high data hiding capacity and low perceptibility.

Future Scope

This experiment has been carried on bitmap images. one can now experiment on other types of image like jpeg, tiff etc. and check the results. In this experiment, complexity technique is used based on length of black & white border. In future work, one can experiment using different complexity techniques and compare them based on the results obtained. This steganography is a very strong information security technique, especially when combined with encrypted embedded data. Furthermore, it can be applied to areas other than secret communication. Future research will include the application to vessels other than 24-bit images, identifying and formalizing the customization parameters, and developing new applications.

REFERENCES

- Silman J. (2001).** Steganography and Steganalysis: An Overview. *SANS Institute*.
- Jamil T. (1999).** Steganography: The art of hiding information is plain sight. *IEEE J.* **18**:1. 1999.
- Wang H. and Wang S (2004).** Cyber warfare: Steganography vs. Steganalysis. *Commun.* **47**:10.
- Anderson R.J. and Petitcolas F.A.P. (1998).** On the limits of steganography. *IEEE J. Selected Areas Commun.* **2**: 78-82.
- Marvel L.M., Boncelet Jr C.G. and Retter C. (1999).** Spread Spectrum Steganography. *IEEE Transactionson Image Process.* **8**:8.
- Dunbar B. (2002).** Steganographic techniques and their use in an Open-Systems environment. *SANS Institute.* 5:67.
- Artz D. (2001).** Digital Steganography: Hiding Data within Data. *IEEE Internet Computing J.* **23**:45.
- Simmons G. (1983).** The prisoners problem and the subliminal channel. *CRYPTO*.
- Chandramouli R., Kharrazi M. and Memon N. (2003).** Image steganography and steganalysis: Concepts and Practice”, Proc. 2nd Int. Workshop Digital Watermarking. 15thOctober 2003.



- Ramani K., Prasad E. V. and Varadarajan S. (2007).** Steganography Using BPCS to the Integer Wavelet Transformed Image in IJCSNS. *Int. J. Computer Sci. Network Security*. **7(7)**.
- Eijji Kawagauch and Richard O. Eason (1998).** Principle and Application of BPCS-Steganography. *Proc. SPIE*. **3529**:464-473.
- R. Schyndel A. Tirkel and C. Os born (1994).** A digital watermark. *Proc. IEEE Int. Conf. Image Processing*. **2**:86-90.
- R. Wolfgang and E. Delp,** "A watermark for digital image", in Proc. IEEE Int. Conf. Image Processing, , vol. 3, pp. 219-222, 1996.
- M. Ramkumar and A. Akansu (1999).** Some Design Issues for Robust Data Hiding Systems. *Proc. The 33 Asilomar Conf. on Signal, System and Comp.* **2**:1528-1532.
- Alturki F. and R. Mersereau (2001).** Secure Blind Image Steganographic Technique Using iscrete Fourier Transformation. *Proc. IEEE Int. Conf. on Image Processing*. **2**:542-545.
- W. Swedens (1996).** The lifting scheme: A Custom-design construction of biorthogonal wavelets. *Appl. Comput. Harmon. Anal.* **3**:186-200.