International Journal of Electronics and Communication Engineering (IJECE)
ISSN(P): 2278-9901; ISSN(E): 2278-991X
Vol. 2, Issue 5, Nov 2013, 187-194

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

A DIGITAL IMAGE STEGANOGRAPHY: SOFTWARE & HARDWARE APPROACH

P. D. GADEKAR[1] & S. K. WAGHMARE[2]

[1]G.H.R.C.O.E.M Chas, Ahmednagar, Maharashtra, India

[2]Department of Electronics Engineering, GHRCEM, Wagholi, Pune, India

ABSTRACT

Information hiding is a technique that inserts secret messages into a cover file, so that the existence of the messages is not apparent. Research in information hiding has tremendous increased during the past decade with commercial interests. Information hiding techniques that are used today include watermarking and Steganography. The major concern of watermarking is to protect the ownership of a digital content, while Steganography is to embed secret messages into digital content so that the secret messages are not detectable. Although many Steganography techniques have been developed for digital images, most of them are irreversible. That is, the original image cannot be recovered to its original state after the extraction of secret data. A lossless or reversible Steganography is defined as an original image can be completely recovered from the stego-image after the embedded data has been extracted. This technique has been focused on spatial uncompressed domain recently which include Least Significant Bit algorithm (LSB), and is considered more challenging to carry out in the compressed domain. In this, we propose a lossless, compressed domain Steganography technique for compressed images based on the Discrete Wavelet Transform (DWT). The stego-image preserves the same image quality as the original compressed images. The results taken with the help of both approaches (i.e. software and hardware) are differing by some little values.

KEYWORDS: Discrete Wavelet Transform, Least Significant Bit (LSB) Algorithm, Spatial Domain, Steganography

INTRODUCTION

The word Steganography is originally composed of two Greek words steganos and graphia, means "covered writing". The use of Steganography dates back to ancient times where it was used by romans and ancient Egyptians. Steganography is the art and science of hiding secret data in plain sight without being noticed within an innocent cover data so that it can be securely transmitted over a network.[2] Any digital file such as image, video, audio, text or IP packets can be used to hide secret message. The file used to hide data is referred as ‘cover object’ and the term ‘stego-object’ is the file containing secret message. [1]

We are using image to hide secret data because among all digital file formats available nowadays image files are the most popular cover objects. [1] As they are easy to find and have higher degree of distortion tolerance and high hiding capacity due to the redundancy of digital information representation of an image data. [1] There are a number of Steganographic schemes that hide secret message in an image file; these schemes can be classified according to the format of the cover image or the method of hiding. We have two popular types of hiding methods; spatial domain embedding and transform domain embedding.

This technique has been focused on spatial uncompressed domain i.e. Least Significant Bit algorithm (LSB). The basic idea in LSB is the direct replacement of LSBs of noisy or unused bits of the cover image with the secret message bits. It is simple to implement offers high hiding capacity, and provides a very easy way to control stego-image quality [3]

There are many transforms that can be used in data hiding, such as the discrete cosine transform (DCT), the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). We propose a lossless, compressed domain Steganography technique for compressed images based on the Discrete Wavelet Transform (DWT). The secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients sub band unaltered [9].

DISCRETE WAVELATE TRANSFORM (DWT)

A fast computation of wavelet transforms which is easy to implement and reduces the computation time and resources required is DWT which based on sub-band coding. [6] DWT stores the information in an image and removes noise efficiently. Wavelets are nothing but localized waves. They have their energy concentrated in time or space for analysis of transient signals. [1]

We are having different types of wavelet families such as Haar, Daubechies4, Coiflet1, Symlet2, Meyer, Morlet, Mexican Hat etc Based on application one can use the type. We used Haar Wavelet transform in this case.

Haar Wavelet Transform

We are using Haar Wavelet type because it is the simple among all. In this the low frequency wavelet coefficients are generated by averaging the two pixel value.[10] High frequency coefficients are generated by taking half of the difference of the same two pixels.[1]

The four bands obtained are LL, LH, HL, and HH which is shown in Figure 1.

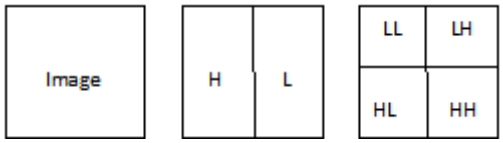


Figure 1: Image and its Transform Domain Bands

The LL band is known as approximation band, consists of low frequency wavelet coefficients, which consist of significant part of the spatial domain image. The other bands are called as detail bands which consist of high frequency coefficients and contain the edge details of the spatial domain image.[1]

Step 1: Column wise processing to get H and L[1]

$$H=(C_o-Ce) \quad (1)$$

$$L=(Ce-[H/2]) \quad (2)$$

Where Co: odd column , Ce: even column pixel values.

Step 2: Row wise processing to get LL, LH, HL and HH,

Separate odd and even rows of H and L,[1]

Namely, H_{odd}– odd row of H

L_{odd}– odd row of L

H_{even} – even row of H

L_{even} – even row of L

$$LH=L_{odd}–L_{even} \quad (3)$$

$$LL=L_{even}–LH/2 \quad (4)$$

$$HL=H_{odd}–H_{even} \quad (5)$$

$$HH=H_{even}-HL/2 \quad (6)$$

LEAST SIGNIFICANT BIT (LSB) ALGORITHM

LSB is the most preferred technique used to hide the data because it is simple to implement and have high hiding capacity. Also easily control stego-image quality. [3] In LSB we directly replace LSBs of noisy or unused bits of the cover image with the secret message bits.[1]

LSB technique has low robustness to modifications made to the stego-image such as low pass filtering and compression [5] and also low imperceptibility. To overcome the robustness and imperceptibility found in the LSB substitution techniques the transform domain technique DWT is used.[1]

In this paper, an image file with '.jpg','.bmp','png' extension has been selected as host file and the LSB of that file should be modified without degrading the image quality.

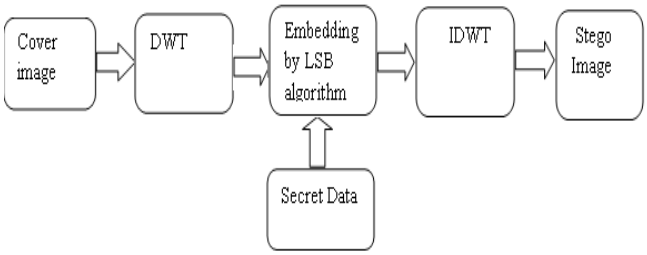
There are 3 types of this algorithm:

- 2 pixel per character
- 4 pixel per character
- 8 pixel per character

As move on from first type to last type the data hiding capacity decreases but quality of image increases. In this paper 4 pixel per character type is used.[1]

SOFTWARE APPROACH

Embedding



Extraction

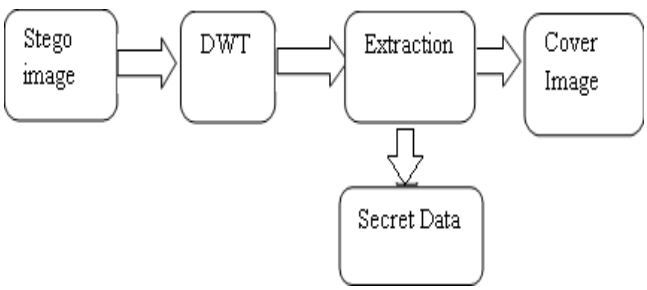


Figure 2: The Flow Diagram of Proposed System

Step 1: First we take input image as cover image in .jpg format as shown in Figure 3

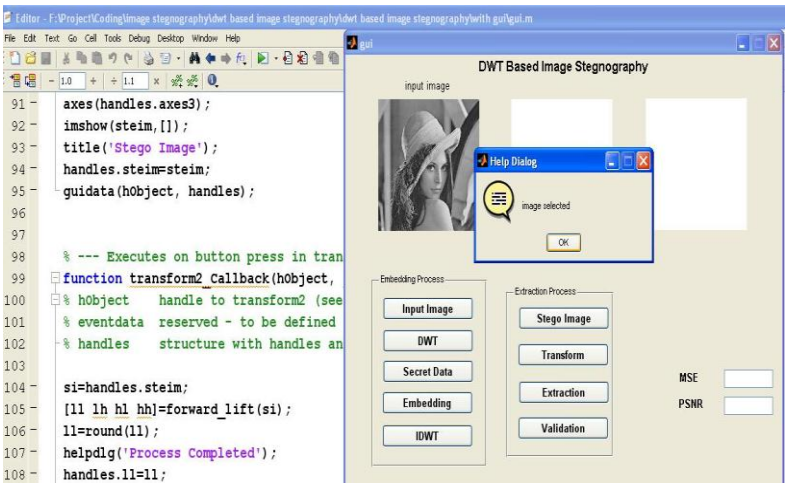


Figure 3

Step 2: Then apply discrete wavelet transform mechanism to compress the image as shown in Figure 4

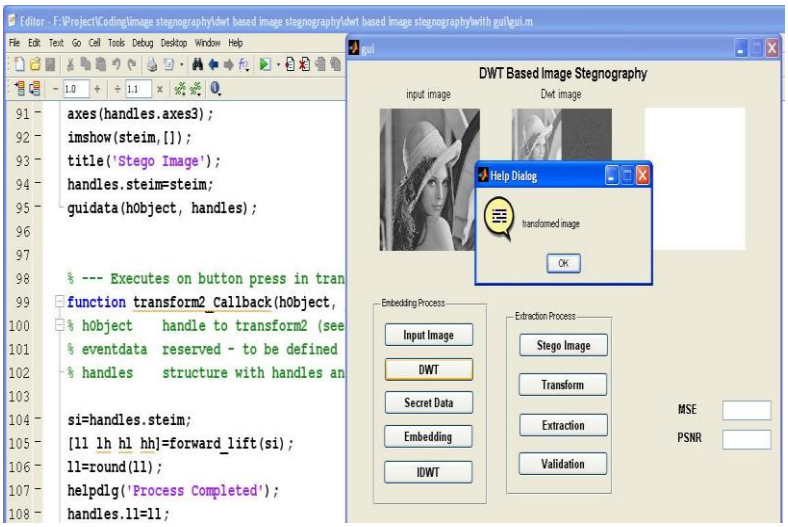


Figure 4

Step 3: With the help of LSB algorithm, embed the secret data and compress image which is shown in Figure 5

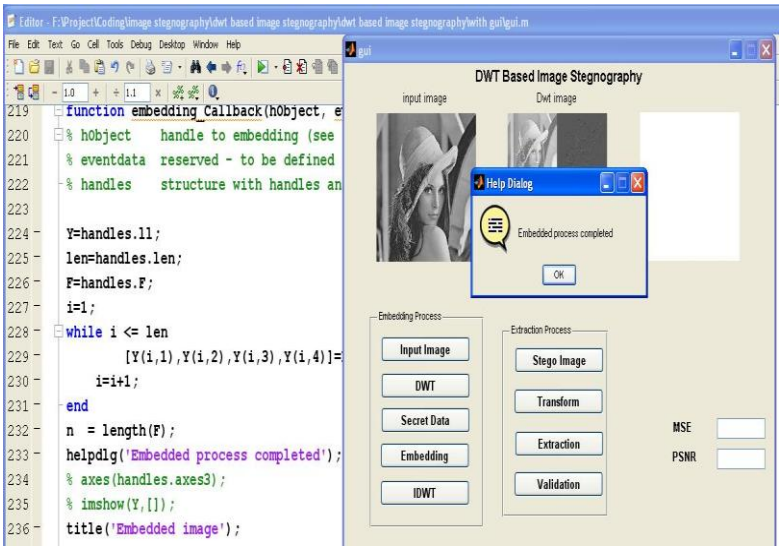


Figure 5

Step 4: After embedding apply IDWT to get stego image at transmitter side as shown in Figure 6

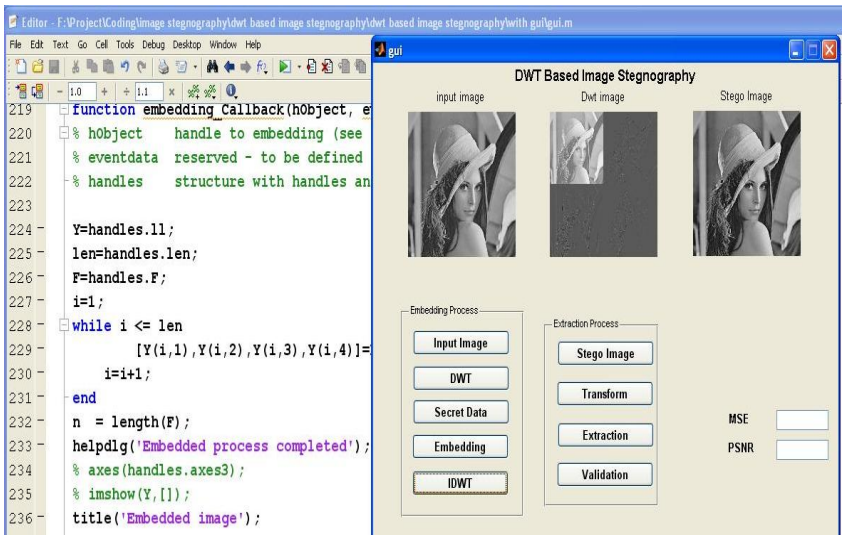


Figure 6

Step 5: Exactly reverse process is done at the receiver side. On stego image apply DWT.

Step 6: Then we are extracting secret data from stego image.

Step 7: In validations we are calculate the MSE and PSNR values as shown in Figure 7

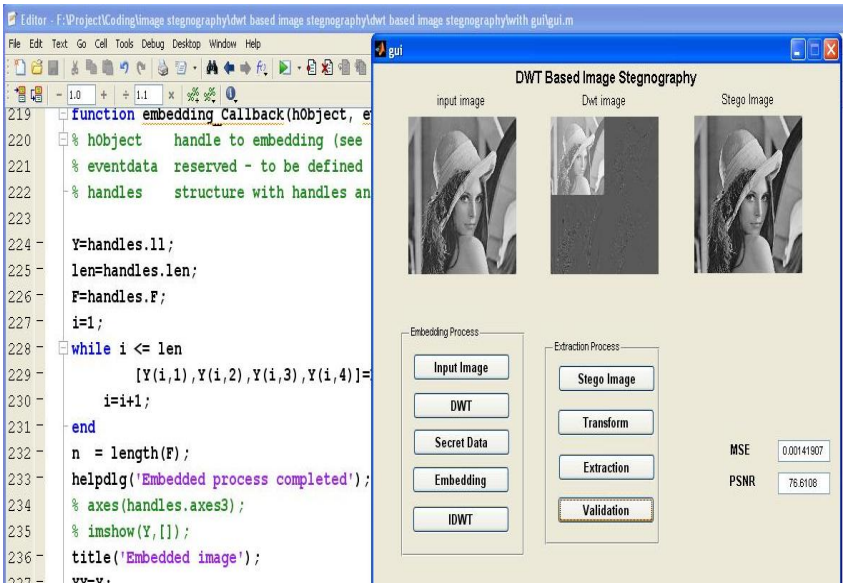


Figure 7

With software we are getting the MSE and PSNR values as 0.001419 and 76.61% respectively.

Now we are running same concept with the help of hardware that means using Advance DSP BF532 processor.

HARDWARE APPROACH

Figure 8 shows the hardware interface of the system. We are using BF532 processor. There are two parts of the process first part is embedding and other is extraction.[1]

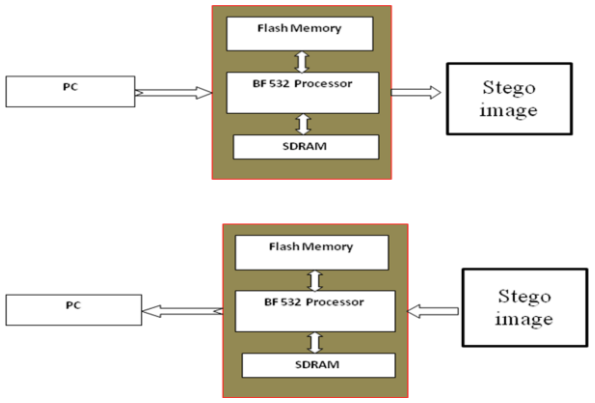


Figure 8: The Hardware Interface Diagram

Embedding

From personal computer we are getting input image as cover image then giving that to processor It process that image. In that firstly it compress the image with the help of Discrete Wavelet transform (DWT).Then in that compressed image embed the secret data which we have to passed to get stego image. This embedding process is done with the help of Least Significant Bit (LSB) algorithm. Then apply Inverse Discrete Wavelet Transform (IDWT) to get Stego image. [1]

Extraction

After getting stego image at transmitter, at receiver exactly reverse process is done. On stego image apply DWT then extract secret data. Finally we get our original image.[1] We have taken some snapshots of project demo (hardware approach) also calculate the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) values as shown in Figure 9,10,11.[1]

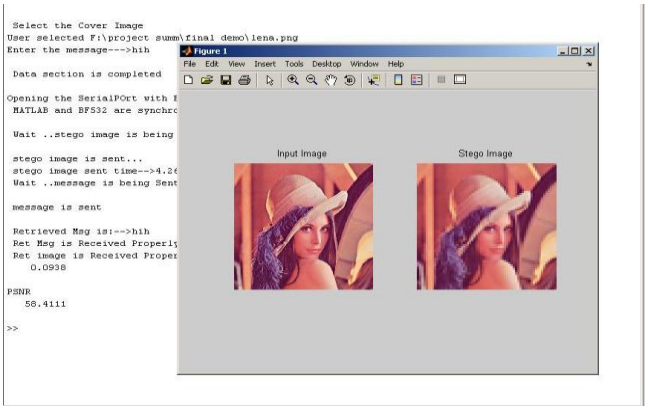


Figure 9: Snapshot of Lena Image

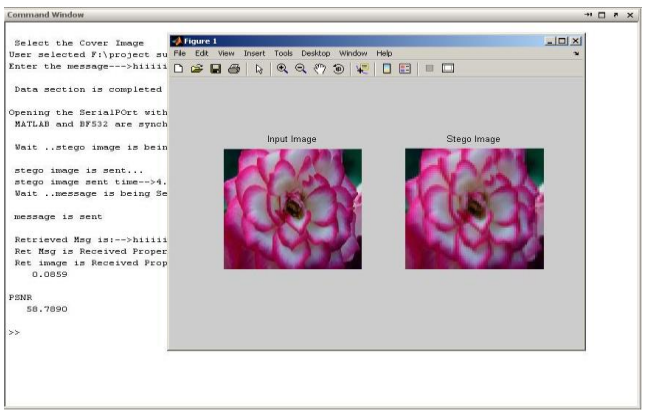


Figure 10: Snapshot of Flower Image

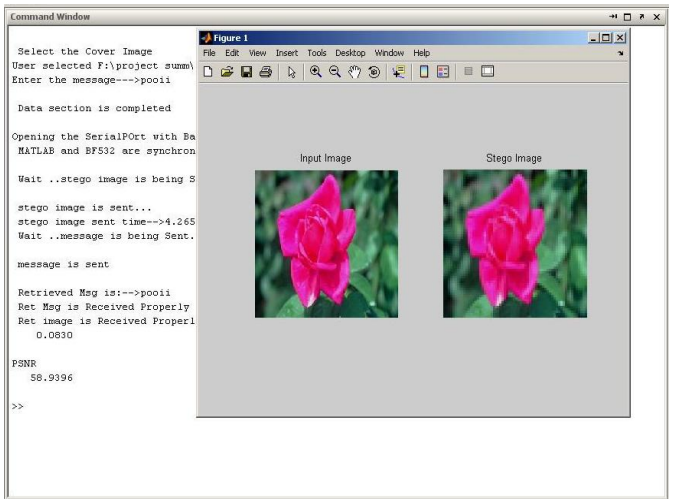


Figure 11: Snapshot of Rose

VALIDATIONS

The performance of stego image is measured with two parameters namely, 1.Mean Square Error (MSE) and 2.Peak Signal to Noise Ratio (PSNR).

- The MSE is calculated by using the equation,

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \tag{7}$$

Where *M* : number of rows and N : number of columns in the input image.[1]

- The PSNR calculated using the following equation:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \tag{8}$$

Where R is the maximum fluctuation in the input image data type.[1]

As we know ideally MSE value should be small and PSNR value should be very high, we get results for MSE and PSNR values near to ideal values in software approach compared to hardware approach.

Table shows MSE and PSNR values 3 different images.

Table 1: Some Experimental Results for Software Approach

Sr. No.	Image	MSE	PSNR
1	Lena	0.001419	76.61%
2	Flower	0.0139771	66.6766
3	Rose	0.0230713	64.5001

Table 2: Some Experimental Results for Hardware Appraoch

Sr.No.	Image	MSE	PSNR
1	Lena	0.0938	58.411
2	Flower	0.0859	58.7890
3	Rose	0.0830	58.9396

CONCLUSIONS

In this paper we consider both software as well as hardware approaches. We get results for MSE and PSNR values near to ideal values in software approach compared to hardware approach. The results taken with the help of both approaches (i.e. software and hardware) are differing by some little values that mean we get near about same results by both ways.

REFERENCES

1. P. D. Gadekar, S. K. Waghmare, ”Implementation of Digital Image Steganography Using ADSP BF532 Processor” International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 9- September 2013
2. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, ”Digital image Steganography: Survey and analysis of current methods Signal Processing”, 90 (2010),727–752.
3. C.K. Chan, L.M. Chen, “Hiding data in images by simple LSB substitution”, Pattern recognition, 37 (3) (2004), 469–474.
4. R.O. EI Safy, H. H. Zayed, A. EI Dessouki, “An Adaptive Steganography Technique Based on Integer Wavelet Transform”, International conference on Networking and media convergence ICNM-(2009),111 - 117.
5. Guorong Xuan; Jidong Chen; Jiang Zhu; Shi, Y.Q.; Zhicheng March, 2011 Ni; Wei Su,” Lossless data hiding based on integer wavelet transform” , IEEE Workshop on Multimedia Signal Processing,Vol.2,(2002), 29-32.
6. Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 4,(2006), 275-290.
7. Saeed Sarreshtedari and Shahrokh Ghaemmaghami, “High Capacity Image Steganography in Wavelet Domain”, IEEE CCNC 2010 proceedings,(2010),1-5.
8. Cheng jiang Lin, Bo Zhang, Yuan F. Zheng,” Packed Integer Wavelet Transform Constructed by Lifting Scheme”, IEEE Transactions on Circuits and Systems for Video Technology, (Dec 2000), 1496 – 1501
9. P. Chen, and H.Lin, "A DWT Approach for Image Steganography," International Journal of Applied Science and Engineering 2006. 4, 3: 275:290.
10. B. Lai and L. Chang, "Adaptive Data Hiding for bnages Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume 4319/2006