IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Special Issue-1 E-ISSN: 2347-2693

A novel technique to hide information using Daubechies Transformation

Jyotsna Kumar Mandal
Dept. of Computer Sc. &Engg
University of Kalyani
jkm.cse@gmail.com

Sujit Das
Dept. of Computer Sc. &Engg.,
University of Kalyani
sujit4uwbslg@gmail.com,

Madhumita Sengupta*
IIIT, Kalyani
madhumita.sngpt@gmail.com

Abstract— **Steganography is an ancient approach of fusing data into innocence medium to hide data secretly in such a way no one can have knowledge of it. This paper presents a technique of Image steganography on frequency domain through Daubechies Transformation. This transformation converts image from spatial domain to frequency domain and allowed embedding with a payload of 2.0 bpb without visual degradation. A gray level image considered as innocent medium of size NxN, where $N = 2^p$, p is an positive integer & is divided into 4x4 non-overlapping blocks in a row major order and a 2D Daubechies Transformation is applied to each of (NxN)/16 blocks to generate frequency components. Three layer of adjustment in terms of security enhancement are applied to improve the quality of stego image. The number of bits embedded per pixel or block is a variable and based on hash function which is used to find the position of each bit. After embedding 4 bits from LSB are grouped into two pairs and XORed, bitwise results are shuffled and stored on last four bits from LSB**

Keywords: *Daubechies Transform,Cover Image,Stego Image*

I. INTRODUCTION

Security is inherent part of information technology where information transfer over the open network is a major concern. Wide range of authentication technique are available for different type of documents.

For all the steganographic operations, an innocent cover medium is selected to hide secret information. This process is embedding. After embedding the resultant image is called stego image.The art of embedding is to manipulate the bits of pixel values,the spatial information of an image, at the Least Signifi- cant Bits(LSB) ,which is very popular Steganography technique. Such embedded information aretransferred over unsecured medium.

Steganography provides us a mechanism to hide secret information for various problem domains such as information authentication, copy right protection, ownership verification etc. All the Steganographic techniques- based on images - are widely categorized into techniques related to spatial domain and techniques related to frequency domain. In spatial domain the bits of the secret image is embedded directly at LSB of the cover image.

In case of frequency domain the entire image is converted from spatial to frequency components before embedding. Numerous transformation functions available in literature to transfer an image from spatial domain to its corresponding frequency domain. Discreet Fourier Transform(DFT) [1], Discrete Cosine Transform(DCT) [2] etc are the examples of such transformations in continuous and discrete forms. There is another type transformation procedure available in literature, named Wavelet transformation [4], which has got high attention of researchers of this field. Like other transformation, Wavelet has its discrete and continuous form. There are number of wavelet transformations available like Haar, Daubechies,

Z transform etc. Discrete frequency transformations are used for image staganography.

The discrete wavelet transform is characterized by equation 1 and equation 2.

$$Y_{low}[k] = \sum_{n} x[n]h[2k-n] \quad (1)$$

$$Y_{high}[k] = \sum_{n} x[n]g[2k-n] \quad (2)$$

Where x[n] is original signal, g[n] is half band high pass filter and h[n] is half band low pass filter.
Yhigh[k] is output of high pass filter after sub sampling by 2.
Ylow[k]is output of low pass filter after sub sampling by 2.
After transformation the image can be regenerated by equation 3

$$x[n] = \sum_{-\infty}^{\infty}(Y_{low}[k]h[2k-n]) + (Y_{high}[k]g[2k-n]) \quad (3)$$

In Daubechies transform of an image the first requirement is the image dimension should be 2^p by2^p where p=1,2,....N.Then the image is scanned by non overlapping 4 by 4 window in row major fashion.This subimage is then multiplied by a 4x4 mask.The result is then multiplied by transpose of the mask.The order of the operands in the multiplication is shown in equations 4 and 5:

$$R1 = S \times M \quad \text{.....(4)}$$
$$R2 = M' \times R1 \quad \text{..... (5)}$$

where S is the 4 × 4 sub-image matrix,M is the mask ,M' is the transpose of the mask M and R1,R2 result of the multiplication result.

The final result is the copied to transformed image matrix in row major fashion as Figure 1.The four colors of the 4 ×4 matrix represents the four 2 ×2 sub-matrix which are to be copied into the four bands.

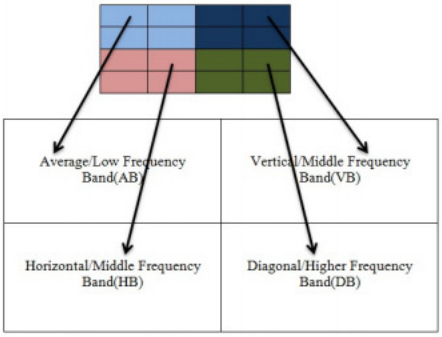

Figure 1: Representation of Image in frequency domain

The structure and values of mask is given in figure 2 ,where values of H are used for half band low pass filtering and values of G are used for half band high pass filtering.

H_0	H_2	G_0	G_2
H_1	H_3	G_1	G_3
H_2	H_0	G_2	G_0
H_3	H_1	G_3	G_1

Mask

H_0	H_1	H_2	H_3
H_2	H_3	H_0	H_1
G_0	G_1	G_2	G_3
G_2	G_3	G_0	G_1

Transpose of Mask

Figure 2: Structure of Mask and its Transpose

The values of H's and G's are: H0 = 0.482963,H1 = 0.836516,H2 = 0.224144, H3 = –0.129410 G0 = –0.129410,G1 = –0.224144,G2 = 0.836516, G3 = –0.482963.

The original image is reconstructed as-first,the values from four bands are copied into a 4 × 4 matrix in row major fashion as shown in the figure 3 ,the meaning of colors as same as before mentioned.

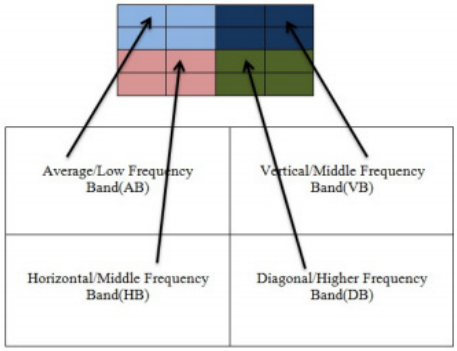

Figure 3: Inverse Daubechies Transform

Then the sub-image matrix is multiplied by mask and transpose of the mask as shown in equation 6 and 7:

$$R1 = M' \times S \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (6)$$

$$R2 = R1 \times M \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (7)$$

where symbols bears the same meaning as defined before.Then the result is copied to image matrix in row major fashion,when all operation is completed, we get the original image matrix.

Daubechies Transformation technique is used in this paper to convert spatial image into its corresponding frequency coefficients in a group of four bands such as– average, vertical,horizontal and diagonal.The proposed method is elaborated in section 2,the result is elaborated in section 3 and conclusion in section 4 followed by references

III. PROPOSED METHOD

The main idea of method is first convert the cover image using Daubechies discrete wavelet transform.After the transformation we get four bands namely average,vertical,horizontal and diagonal.The next step is to multiply these coefficient values with the value of π the bits of the secret image are embedded at LSB of the integer portion of the coefficient values. The 8-bit of an secret image pixel is divided three sets of bit-3-bit,3-bit,2-bit.One group of bits is embedded into a coefficient value at a time at LSB.But embedding sequence is not always 3,3,2 i.e. the sequence is permuted as (3,3,2),(3,2,3) and (2,3,3)-only one out of these three options is selected for embedding. The selection is done as follows- 1.Fisrt constructa 3x3 matrix as-

$$\begin{pmatrix} 3 & 3 & 2 \\ 3 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix}$$

2.Then a particular sequence selection is equal to selection a particular row,so the row is selected as equation 8—

$$row = k \bmod 3 + 1 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (8)$$

because base of the matrix is started from (1, 1),here k is position of a pixel in cover image. After embedding the last 4-bits are grouped into two pair as

Figure 4: Grouping 4 LSB Bits

3. Then the two pair.lets say A & B are XORed.The result is stored at the position of A and the group A is placed at the position of B

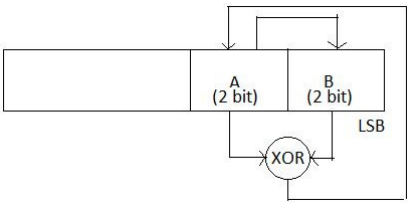

Figure 5: XORing the two groups

The embedding process used in proposed method is shown in flowchart as in the Figure 6

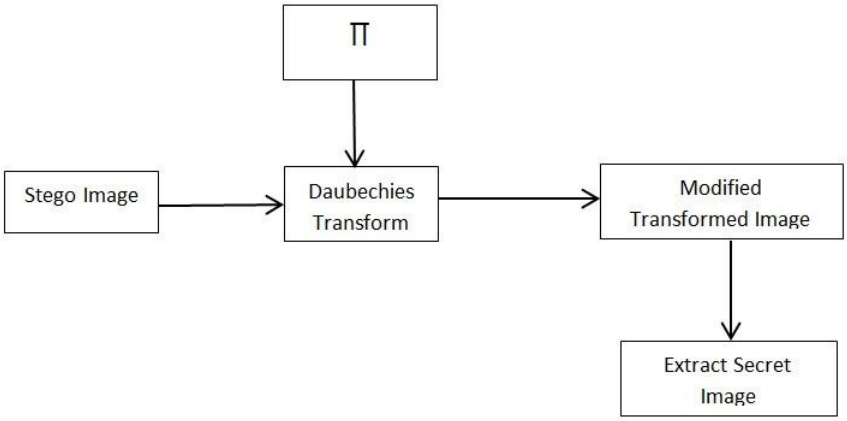

Figure 6: Embedding Flow Chart

The Extraction Method used in proposed method is shown in flowchart as in the Figure 7

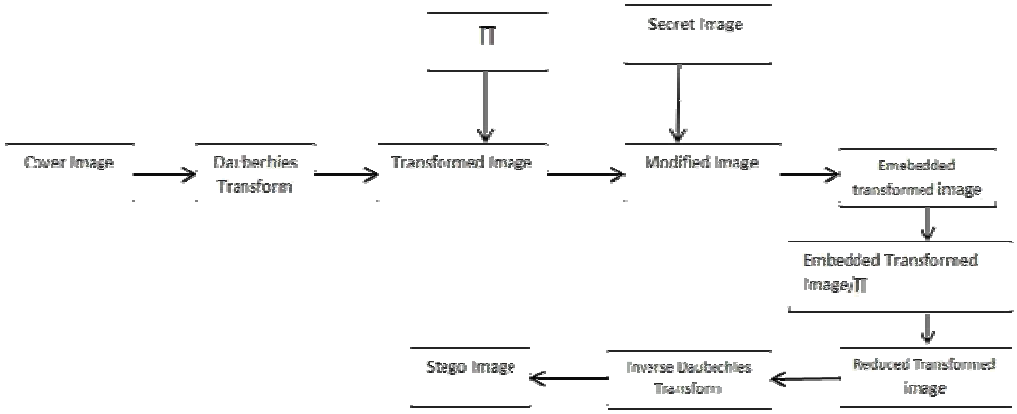

Figure 7: Secret Data Extraction Flow Chart

The algorithm of embedding the secret image into the cover image is described bellow:

Algorithm 1 Embedding Algorithm

1: let A is input image matrix and B is transformed image matrix and A' is the stego image matrix of dimention N×N such that N = 2pwhere p ∈ Set of Natural number
2: let B is dived into four sub-matrices having dimension N/2×N/2

3: let PERMUTE is 3 × 3 matrix whose content is ((3,3,2),(3,2,3),(2,3,3))
4: for i is 1 to N do
5: for j is 1 to N do
6: Read a 4×4 sub-image into matrix S of dimention 4×4
7: let R1=S×M
8: let R2=M'×R1
9: let R2=R2×π
10: Read a sub-matrix of dimension 2×2 from R2 in row major fashion
11: Store each of these 2×2 sub-matrices into B's sub-matrices in row major fashion i.efirt 2×2 sub-matrix into first N/2×N/2 sub-matrix second into into next sub-matrx in this order.
12: end for
13: end for
14: for each N/2×N/2 sub-matrix except the first do
15: Read a byte from secret image matrix until it exhaust
16: let row = k mod 3 + 1,where k is position of values in B
17: Each byte divided into 3 group of bits according to values of PERMUTE(row) vector
18: embed each group of bits into the integer portion of sub-matrix of B at LSB according to the following hash function.The position p1,p2,p3 are used for 3-bits embedding and p1,p2 used for 2-bits embedding p1 = k mod 4 + 1 p2 = p1 mod 4 + 1 p3 = p2 mod 4 + 1
19: After embeding the the last 4 bits at LSB are dived into 2 group of bits and XORed and the result is copied at position 4 & 3 at LSB and the old values at postion 4 & 3 at LSB are coped to the position 3 & 2 at LSB.
20: end for
21: Read 2 × 2 matrix from each of sub-matrix of B in row major fashion and construct a 4 × 4 matrix S'
22: let R1 = M´ × S´
23: let R2 = R1 × M
24: let R2 = R2/π
25: copy values of R2 into a matrix A' of same dimention of A in row major fashion.
26: Repeat the steps from 21 to 25 until the matrix B exhaust.
27: End

The algorithm for extraction of secret image from the cover image is described bellow:

Algorithm 2 Extarction Algorithm

1: let A' represents the stego image matrix
2: let B' represents the transformed matrix of A'
3: for i is 1 to N do
4: for j is 1 to N do
5: Read a 4×4 sub-image into matrix S of dimention 4×4
6: let R1=S×M
7: let R2=M'×R1
8: let R2=R2×π
9: Read a sub-matrix of dimension 2×2 from R2 in row major fashion
10: Store each of these 2×2 sub-matrices into B's sub-matrices in row major fashion i.efirt 2×2 sub-matrix into first N/2×N/2 sub-matrix second into into next sub-matrx in this order.
11: end for
12: end for
13: for each N/2×N/2 sub-matrix except the first do
14: Read the integer portion of B's values until we reach the size of the secret image
15: let row = k mod 3 + 1,where k is position of values in B
16: Read the LSB bits according to values of PERMUTE(row) vector and use the following hash function as it was embedded into LSB and construct a 8-bit word and copied to a matrix SI of size of the secret image
p1 = k mod 4 + 1
p2 = p1 mod 4 + 1
p3 = p2 mod 4 + 1
17: end for

IV. RESULT

The the proposed method is tested on following pictures which are shown in the Figure 8 The each image in the image set is of dimention 512 × 512 dimention.

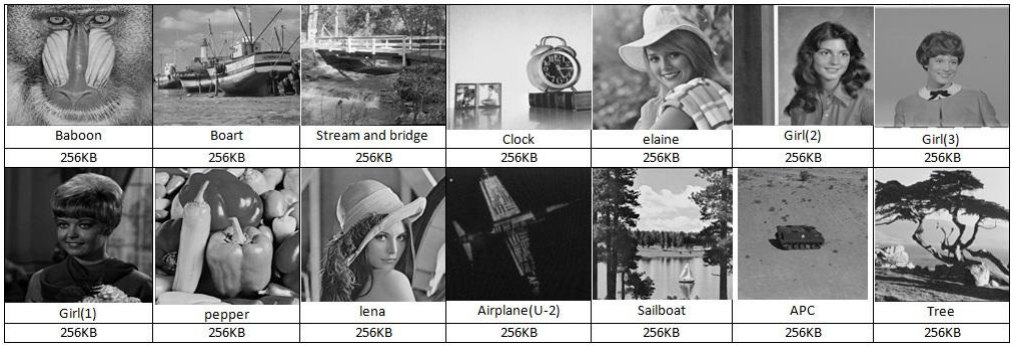

Figure 8: Image Set

And the secret image is used is shown in the Figure 9.

Figure 9: Secret Image

All the above images are experimented with our proposed algorithm and the result of the experiments are cataloged in the Table 1.The table the three attribute of the result psnr(dB),IF(Image Fidelity) and SSIM which represents the retention of the visual clarity after generating the Stego Image .

Table 1: Test Data

Image	Size(KBytes)	Capacity(bits)	PSNR	IF	SSIM
Baboon	256	589824	31.2067	0.9978	0.9787
Elaine	256	589824	39.9098	0.9997	0.9783
lena	256	589824	37.9821	0.9994	0.9718
boat	256	589824	35.5057	0.9990	0.9752
Stream and bridge	256	589824	34.6525	0.9986	0.9836
APC	256	589824	40.6083	0.9998	0.9722
Airplane(U-2)	256	589824	40.2893	0.9980	0.9673

Girl(1)	256	589824	40.6415	0.9996	0.9494
Girl(2)	256	589824	39.9461	0.9997	0.9328
Girl(3)	256	589824	40.2541	0.9989	0.9512
sailboat	256	589824	31.8949	0.9981	0.9721
tree	256	589824	37.9067	0.9996	0.9645
pepper	256	589824	32.0109	0.9981	0.9698
clock	256	589824	39.1825	0.9998	0.9392

It can be seen that the psnr on average is 37.2851(dB) with great many capacity of 589824 bits-the maximum number of bits that can be embedded into cover image.This shows the efficiency of our proposed algorithm that with such a high capacity and manipulating the bits of the images with high range, we can achieve good psnr value.

The psnrvalues of the experimented result isploted in graph shown in the figure 10:

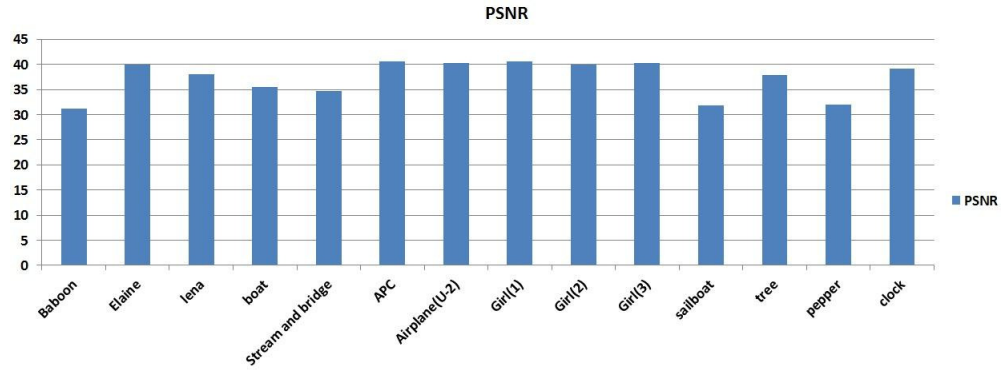

Figure 10: PSNR of Tested Data

Also the IF and SSIM values of the experimented result isploted in graph shown in the figure 11:

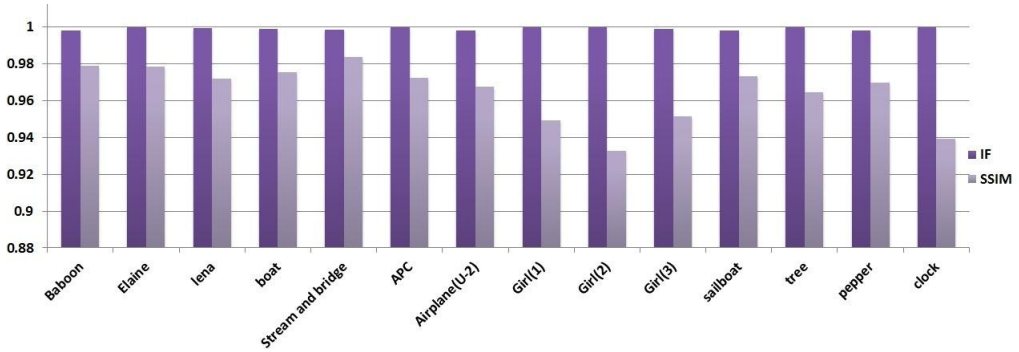

Figure 11: IF And SSIM of Tested Data

Our tested result is compared with other methods and we can see that our proposed method performs better for the same payload value.The table 2 shows psnr value for payload 2.0 of various methods along with our proposed method.

Table 2: Comparison

Technique	Payload	PSNR
WTSIC	2.0	32.78
ATFDWT	2.0	32.84
TISAWFD	2.0	34.62
ATGT-D4	2.0	34.64
AHSG-D4(2013)	2.0	33.53
PROPOSED METHOD	2.0	37.29

The method WTSIC [3] gives PSNR 32.78dB with payload 2.0bpb which is much less than the proposed method.The method ATFDWT [5] which better than WTSIC also less has PSNR musch less than proposed method.Likewise the methods TISAWFD [6],ATGT-D4,AHSG-D4 [7] has less PSNR value than proposed value as well. The comparison is also shown in graphical representation in the Figure 12.The graph also depicts the superiority of the proposed method over above mentioned methods.

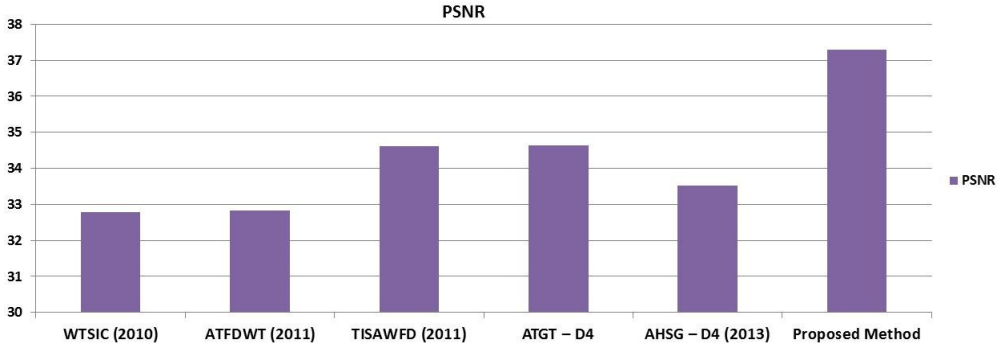

Figure 12: Comparison of Proposed Method

V. CONCLUSION

In our approach we can see that with great many manipulation of bits and with such a high capacity we can still a good psnrvalue.With such a platform we can go further to achieve good result with higher payload.

REFERENCES

[1] Alturki F.; Russell, Mersereau. (2001, October 7-10). Secure blind image steganographic technique using discrete Fourier transformation. International Conference on Image Processing. Proceedings., vol.2,. 542 545. doi: 10.1109/ICIP.2001.958548

[2] Hashad, A.I.; Madani, A.S.; Wahdan, A.E.M.A. (2005, December 5th 6th). A robust steganography technique using discrete cosine transform insertion. 3rd International Conference on Information and Communications Technology. Enabling Technologies for the New Knowledge Society: ITICT. 255 264, doi: 10.1109/ITICT.2005.1609628.

[3] J.K. Mandal,MadhumitaSengupta, ”Authentication/Secret Message Transformation through Wavelet Transform Based Subband Image Coding (WTSIC)”,2010

[4] Hsieh, Ming-Shing; Tseng, Din-Chang; Huang. Yong-Huai. (2001, October). Hiding digital watermarks using multiresolution wavelet transform. Industrial Electronics, IEEE Transactions on, 48(5). 875 882. doi: 10.1109/41.954550.

[5] MadhumitaSengupta,J. K. Mandal, N. Ghoshal ,”An Authentication Technique in Frequency Domain through Wavelet Transform (ATFDWT)”,2012

[6] Sengupta, Madhumita; Mandal, J. K.,”Transformed IRIS Signature fabricated Authentication in Wavelet based Frequency Domain (TISAWFD)”,2011

[7] MadhumitaSengupta,J.K. Mandal,”Authentication Through Hough Transformation Generated Signature on G-Let D3 Domain (AHSG)”,2013