Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

A NEW ALGORITHM FOR DATA HIDING USING OPAP AND MULTIPLE KEYS

V.Eswari[1], G.Arumugam[2]
[1]*P.G. Student Dept. of ECE, Seshachala Institute of Technology*
[2]*Assistant Professor, Dept. of ECE, Seshachala Institute of Technology*

***Abstract*—**Steganography gained significance in the past few years due to the increasing need for providing secrecy in an open environment like the internet. With almost anyone can observe the communicated data all around, steganography attempts to hide the very existence of the message and make communication undetectable. In this paper we propose a modern technique with Integer Wavelet transform (IWT) and double key to accomplish high hiding capability, high security and good visual quality. Here cover image is transformed in to wavelet transform co-efficients and the coefficients are selected randomly by using Key-2 for embedding the data. Key-1 is used to calculate the number of bits to be embedded in the randomly selected coefficients. Finally the Optimum Pixel Adjustment Process(OPAP) is applied to the stego image to reduce the data embedding error.

Keywords- *Steganography, Integer wavelet transform (IWT), Optimum Pixel Adjustment Process(OPAP).*

I. INTRODUCTION

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. The word steganography is originally composed of two Greek words steganos and graphia, which means "covered writing". Modern steganography is generally understood to deal with electronic media rather than physical objects. Image steganography, of all has gained much impetus and reputation in the recent past [1-18]. It comes under the general assumption that if the feature is visible, the point of attack is evident. Thus the goal here is to always conceal the coherence of the embedded data. The basic model of secret key steganography consists of cover, secret data, stego image and key. Any digital file such as image , video, audio, etc can be used as cover. Cover is also known as cover-object or cover image, is the plain digital image with no secret data deposited in it. After the embedment it is called the stego image or stego object [1, 2, 3, 10]. In image steganography [1] the critical data is camouflaged in a cover image with immense dexterity.

The most popular hiding techniques are spatial domain based steganographic techniques and transform domain based steganographic techniques. A useful, practical steganographic method should be robust and should retain the hidden data even after many pixel values have been modified. The other type of hiding method is the transform domain techniques which appeared to overcome the robustness andimperceptibility problems found in the LSB substitution techniques. There are many transforms that can be used in data hiding, the most widely used transforms are; the discrete cosine transform (DCT) which is used in the common image compression format JPEG and MPEG, the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT).One approach to this problem is to transform the

image and embed the data in the transformed pixels[4-6,8,9]. We say that the original image exists in the spatial domain and the transformed image in the transformed domain. The data is then embedded in the transformed pixels and the image is transformed back to the spatial domain. The idea is that the image may now be exposed to various operations that will change the pixels, but when this modified image is transformed again, the hidden data will still be embedded in the transformed pixels. The disadvantage of the DCT based steganographic technique [9, 13], is the hiding capacity. Wavelet transform based stego technique provides high capacity as much as possible. In [4] the secret message is embedded into the high frequency and low frequency coefficients of the wavelet transform to high hiding capacity, but it provides less PSNR at high hiding rate. In this paper we propose a new modified version of the methodology in [4], which can embed a larger amount of data in integer wavelet transform (IWT) domain with high PSNR.

II. RELATED WORKS

A. Integer Wavelet Transforms

Generally wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands (HL, LH and HH), Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information which may lead to the failure of the data hiding system.

To avoid problems of floating point precision of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which doesn't allow perfect reconstruction of the input image [12] and in this case there will be no loss of information through forward and inverse transform [11].

The Haar Wavelet Transform is the simplest of all wavelet transform. The four bands obtained are LL, LH, HL, and HH which is shown in Fig 1. The LL band is called as approximation band, which consists of low frequency wavelet coefficients, and contains 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. Integer wavelet transform can be obtained through lifting scheme. Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information. [5, 8].

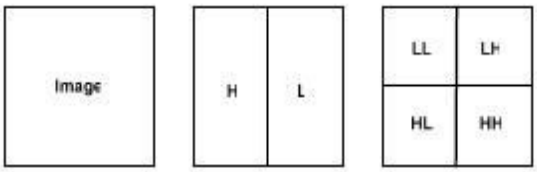

Figure 1 Image and its transform domain bands

B. Forward Lifting scheme in IWT.

Step1: Column wise processing to get H and L

$$H = (Co\text{-}Ce) \quad (1)$$

$$L = (Ce- \lfloor H/2 \rfloor) \quad (2)$$

Where Co and Ce is the odd column and even column wise pixel values.

Step 2: Row wise processing to get LL,LH,HL and HH,
Separate odd and even rows of H and L,
Namely, Hodd – odd row of H
Lodd- odd row of L
Heven- even row of H
Leven- even row of L

$$LH = Lodd - Leven \quad (3)$$
$$LL = Leven - \lfloor LH / 2 \rfloor \quad (4)$$
$$HL = Hodd – Heven \quad (5)$$
$$HH = Heven - \lfloor HL / 2 \rfloor \quad (6)$$

C. Reverse Lifting scheme in IWT

Inverse Integer wavelet transform is formed by Reverse lifting scheme. Procedure is similar to the forward lifting scheme.

D. LSB Embedding

Simple LSB embedding [2]is detailed in this section. Consider a 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the stego-image is not visually perceptible.

This can be further extended, and any number of LSB's can be modified in a pixel. The quality of the image, however degrades with the increase in number of LSB's. Usually up to 4 LSB's can be modified without significant degradation in the message. Mathematically, the pixel value 'P' of the chosen pixel for storing the k-bit message Mk is modified to form the stego-pixel 'Ps' as follows:

$$Ps=P-mod(P,2k)+Mk \quad (7)$$

The embedded message bits can be recovered by

$$Mk=mod(Ps,2k) \quad (8)$$

One method to recover the quality of the LSB substitution is Optimal Pixel adjustment Process (OPAP)[2].

E. Optimal Pixel adjustment Process

The projected Optimal Pixel adjustment Procedure (OPAP) reduce the error caused by the LSB substitution method. In OPAP method the pixel value is adjusted after the secret data is concealed. It is done to improve the quality of the stego image without disturbing the data hidden.

F. Adjustment Process

Let 'n' LSBs be substitute in each pixel.
Let d= decimal value of the pixel after the substitution.

d1 = decimal value of last n bits of the pixel.
d2 = decimal value of n bits concealed in that pixel.
If(d1~d2)<=(2^n)/2
then no adjustment is made in that pixel.
Else
If(d1<d2)
d = d – 2^n .
If(d1>d2)
d = d + 2^n .
This d is converted to binary and written back to pixel.

III. PROPOSED METHODOLOGY

Fig. 2 shows the proposed system is a high capacity steganography system. Preprocessing includes R, G and B plane separation and Histogram modification. Then Integer wavelet transform is applied to the cover image to get wavelet coefficients. Wavelet coefficients are randomly selected by using key-2 for embedding the secret data. Key -2 is 8x8 binary matrix in which '1' represents data embedded in the corresponding wavelet coefficients and '0' represents no data present in the wavelet coefficients.

Key-1(K1) is a decimal number varying from 1 to 4 and it will decide the number of bits to be embedded in the cover object.

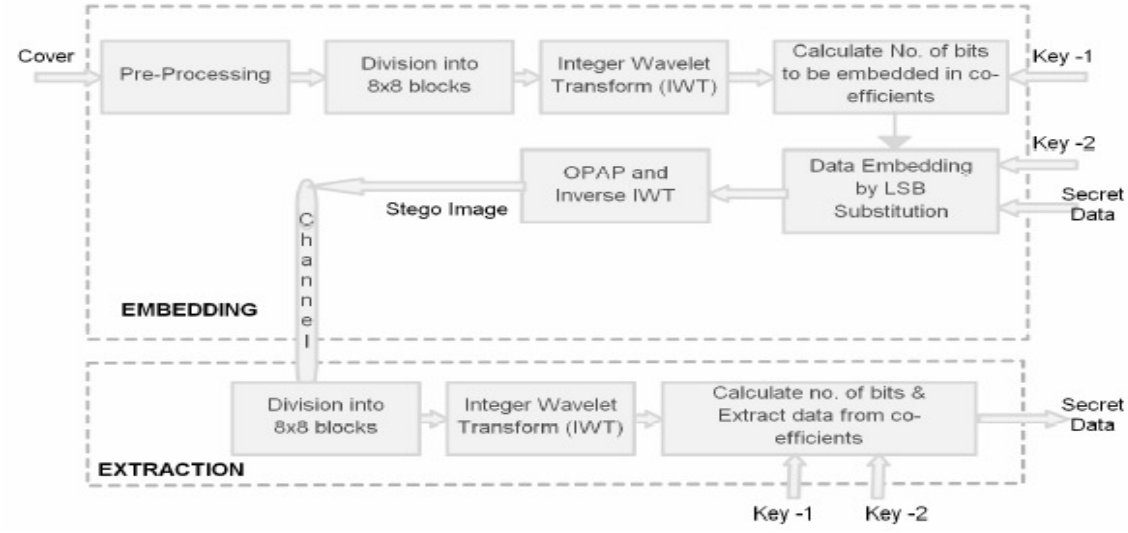

Figure 2 The Block Diagram of the Proposed Methodology

A. Algorithm (For Embedding of Data):

Step 1: Read the cover image as a 2D file with size of 256×256 pixels.

Step 2: R, G and B planes are separated.

Step 3: Consider a secret data as text file. Here each character will take 8 bits.

Step 4: Histogram adjustment[16] is done in all planes, Because, the secret data is to be embedded in all the planes, while embedding integer wavelet coefficients produce stego-image pixel values greater than 255 or lesser than 0. So all the pixel values will be ranged from 15 to 240.

Step 5: Each plane is divided into 8×8 blocks.

Step 6: Apply Haar Integer wavelet transform to 8 × 8 blocks of all the planes, This process results in LL1, LH1, HL1 and HH1 sub bands.

Step 7: Using Key-1(K1) calculate the Bit length(BL) for corresponding wavelet co-efficients (WC), Here we used modified version of Bit length calculation used in [4]. Using the following equation, we get the high capacity steganography.

$$BL = \begin{cases} K1 + 3 & if \quad WC \geq 2^{K1+2} \\ K1 + 1 & if \quad WC < 2^{K1+2} \end{cases} \quad (9)$$

Step 8: Using key-2 select the position and coefficients for embedding the 'BL' length data using LSB substitution[2]. Here data is embedded only in LH1,HL1and HH1 subbands. Data is not embedded in LL1 because they are highly sensitive and also to maintain good visual quality after embedding data. An example of key-2 is shown below.

$$\text{Key} - 2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \quad (10)$$

Step 9: Applying Optimal Pixel adjustment Procedure (OPAP) reduces the error caused by the LSB substitution method.

Step 10: Take inverse wavelet transform to each 8×8 block and combine R,G&B plane to produce stego image.

B. Algorithm (For Extracting of Data):

Step 1: Read the Stego image as a 2D file with size of 256 × 256 pixels.

Step 2: R, G and B planes are separated.

Step 3: Each plane is divided into 8×8 blocks.

Step 4: Apply Haar Integer wavelet transform to 8×8 blocks of all the planes, This process results LL1,LH1,HL1 and HH1 subbands.

Step 5: Using Key-1 calculate the Bit length(BL) for corresponding wavelet co-efficients(WC), using the 'BL' equation used in Embedding procedure.

Step 6: Using key-2 select the position and coefficients for extracting the 'BL' length data.

Step 7: Combine all the bits and divide it in to 8 bits to get the text message.

IV. ERROR METRICS

A performance estimate in the stego image is calculated by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The MSE is calculated by using the equation,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{i,j} - Y_{i,j}\right)2 \qquad (11)$$

key - 1(K1) = 1								
Various key -2	Cover Image	Total No. of bits embedded	Channel - I Red		Channel - II Green		Channel - III Blue	
			MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)
Key - A	Flower	59168	1.31219	53.9016	1.86553	50.8456	1.05667	55.7828
	Elephant	80512	3.34099	45.7841	3.10357	46.4244	2.80991	47.2878
Key - B	Flower	78696	1.32099	53.8436	1.86851	50.8317	1.06836	55.6872
	Elephant	92968	3.31004	45.8649	3.10463	46.4214	2.79836	47.3235
Key - C	Flower	104944	1.32786	53.7986	1.86316	50.8566	1.07731	55.6148
	Elephant	196480	3.37844	45.6873	3.14449	46.3106	2.82475	2.82475
Key - D	Flower	110320	1.29164	54.0388	1.84346	50.949	1.04401	55.8875
	Elephant	252784	3.36729	45.716	3.14812	46.3006	2.81612	47.2686
Key - E	Flower	240840	1.33505	53.7517	1.88163	50.7709	1.0914	55.5019
	Elephant	335560	3.40763	45.6126	3.18555	46.1979	2.8945	47.0301

where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image Xi, j represents the pixels in the original image and Yi,j represents the pixels of the stego-image.

The Peak Signal to Noise Ratio (PSNR) is expressed as

$$PSNR = 10\log_{10}\left(\frac{I_{max}^2}{MSE}\right) db \qquad (12)$$

V. RESULT AND DISCUSSION

In this present implementation, Flower and Elephant 256 × 256 × 3 color digital images have been taken as cover images, as shown in Figure 3&4- a,b, c & d, tested with key-2(key-

E) and various key-1s. The effectiveness of the stego process proposed has been studied by calculating MSE and PSNR for the two digital images in RGB planes and tabulated.

First analysis is used to select the Key-2 for random selection of coefficients for embedding data (in this analysis Key-1 has been set as K1=1) and the results are tabulated in Table-I for various Key-2 using the proposed method. From table –I we will understand that Key-E provides high capacity and Key – A provides low capacity.

In the second analysis, Key-E will be taken with various 'K1' values and the results are tabulated in Table-II. Combining Key-E with K1=4 will yield high hiding capacity with high PSNR.

Table – II MSE, PSNR for fixed Key-2(Key-E) with varying Key-1 in all the three planes

Key-1	Cover Image	Total No. of bits embedded	Channel - I Red		Channel - II Green		Channel - III Blue	
			MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)
K1=1	Flower	240840	1.33505	53.7517	1.88163	50.7709	1.0914	55.5019
K1=2	Flower	299256	1.35302	53.6355	1.88619	50.7499	1.0997	55.4357
K1=3	Flower	307280	1.34458	53.6899	1.87415	50.8055	1.0992	55.4397
K1=4	Flower	348192	1.35817	53.6025	1.87792	50.7881	1.0911	55.504
K1=1	Elephant	335560	3.40763	45.6126	3.18555	46.1979	2.8945	47.0301
K1=2	Elephant	348192	3.39305	45.6498	3.16413	46.2565	2.8627	47.126
K1=3	Elephant	370288	3.38845	45.6616	3.16842	46.2447	2.8782	47.0791
K1=4	Elephant	435304	3.38991	45.6578	3.18234	3.18234	2.8663	47.1151

Figure 3. K1=1,2,3 & 4 respecively

Figure 4. K1=1,2,3 & 4 respecively

VI. CONCLUSION

Data hiding with steganography has two primary objectives firstly that steganography should grant the maximum possible payload, and the second, embedded data must be undetectable to the observer. It should be stressed on the fact that steganography is not meant to be robust. It was found that the proposed method gives high payload (capacity) in the cover image with very little error. This is of course on the expense of reducing PSNR and increasing the MSE. By modifying the equation (9) to get high capacity for the various applications using wavelet transform, Key-1 and Key-2 provides high protection. The drawback of the proposed method is the computational overhead. This can be reduced by high speed computers.

REFERENCES

[1]Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc kevitt Digital image steganography: Survey and analysis of current methods Signal Processing", 90 (2010),727–752.
[2]C.K. Chan, L.M. Chen, "Hiding data images by simple LSB substitution", Pattern recognition, 37 (3) (2004), 469–474.
[3]R.O. EI Safy, H. H. Zayed, A. EI Dessouki, " An Adaptive Steganographic Technique Based on Integer Wavelet Transform", International conference on Networking and media convergence ICNM-(2009), 111 - 117.
[4]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
[5]R.Amirtharajan, Adarsh D, Vignesh V and R. John Bosco Balaguru, "PVD Blend with Pixel Indicator - OPAP Composite for High Fidelity Steganography", International Journal of Computer Applications 7(9),(October 2010),31–37.
[6]Guorong Xuan; Jidong Chen; Jiang Zhu; Shi, Y.Q.; Zhicheng Ni; Wei Su," Lossless data hiding based on integer wavelet transform" , IEEE Workshop on Multimedia Signal Processing,vol 2,(2002).
[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 IntegerWavelet Transform Constructed by Lifting Scheme", IEEE Transactions on Circuits and Systems forVideo Technology, (Dec 2000), 1496 –1501.
[9]H. W. Tseng and C. C. Chnag, "High capacitydata hiding in jpeg compressed images," Informatica, vol. 15, no. I,2004.
[10]H. H. Zayed, "A High-Hiding Capacity Technique Hiding data in hnages Based on K-Bit LSB Substitution," The 30th International Conference on Artificial IntelligenceApplications (ICAIA - 2005) Cairo, Feb. 2005.
[11]A. R. Calderbank, 1. Daubechies, W. Sweldens and B. Yeo.,"Wavelet transforms that map integers

to integers". Appied and Computational Harmonic Analysis, vol.5,.332-369,1998.
[12]G. J. Simmons, "The prisoners' problern and the subliminal channel," in Proceedings of Crypto' 83, pp. 51-67, 1984.
[13]W. Bender, N. Morimoto, A. Lu, Techniques for data hiding,IBM Syst. J. 35 (3/4) (1996) 313–336.
[14]K.L. Chung, C.H. Shen, L.C. Chang, A novel SVD- and VQ-based image hiding scheme, Pattern Recognition Lett. 22 (9)(2001) 1051–1058.
[15]Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, pattern Recognition 34 (3) (2001) 671–683.
[16]Yildiray Yalman, Ismail Erturk, "A New Histogram Modification Based Robust Image Data Hiding Technique", 24th Interational Symposium on Computer and Information Sciences, ISCIS 2009, 39-43 .
[17]Rengarajan Amirtharajan and John Bosco Balaguru Rayappan,"Tri- Layer Stego for Enhanced Security – A Keyless Random Approach" - IEEE Xplore, DOI, 10.1109/IMSAA.2009.
[18]J. Lillo M. Shih, "Generalizations of Pixel-Value Differencing Steganography for Data Hiding in bnages", Fundamentaaticae, vol. 83, noJ, pp. 319-335, 2008

