A Modified OPA Algorithm on Image Steganographic Method for Optimum Hiding Capacity

[1]A. Antony Judice, [2]Lekshmi Sree. H. A., [3]Divya Sree. D. J
[1]Dept. of ECE, Arunachala College of Engineering for Women

Abstract
Steganography gained importance in the past few years due to the increasing need for providing secrecy in an open environment like the internet.Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet Steganography is used to conceal the information so that no one can sense its existence. In most algorithm used to secure information both steganography and cryptography are used together to secure a part of information.
Steganography has many technical challenges such as high hiding capacity and imperceptibility. In this paper,we try to optimize these two main requriments by proposing a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm.The coefficients used are selected according to a pseudorandom function generator to increase the security of the hidden data.The OPA algorithm is applied after embedding secret message to minimize the embedding error.The proposed system showed high hiding rates with reasonable imperceptibility compared to other steganographic system.

Keywords
Steganography, Adaptive Algorithm, Spatial Domain, Discretewavelet Transform, Optimum Pixel Adjustment Algorithm

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 world steganography is originally composed of two greek words steganos and graphia,which means "covered writing". The use of steganography dates back to ancient times where it was used by romans and ancient Egyptians.The interest in modern digital steganography started by simmons in 1983 [1].When he presented the problems of two prisoners wishing to escape and being watched by the warden that blocks any suspicious data communication between them and passes only normal looking one.Any digital file such as image,video,audio,text or IP packets can be used to hide secret message.Generally the file used to hide data is referred to as cover-objects,abd the term stego-object is used for the file containing secret message.
Nowadays data hiding is a challenging issue steganography is considered one of the branches in data hiding and it is the art of hiding secret data within the cover image. Internet users frequently need to store,send, or receive private information.The most common way to do this transform the data into a different form. The resulting data can be understood only by those who know how to return it to its orginal form.This method of protecting information is known as encryption.A major drawback to encryption is that the existence of data is not hidden .
Among all digital file formats available nowadays image files are the most popular cover objects because they are easy to find and have higher degree of distortion tolerance over other type of files with high hiding capacity due to redundancy of digital information representation of an image data.In steganography, the possible cover carriers are innocent looking carrier(image,audio,video,text,or some other digitally representative code) which will hold the hidden information.
For example ,when a secret message is hidden within a cver image, the resulting product is a stego-image. A possible formula of the process may be represented as:Cover image+embedded message+Stego key=Stego Image.
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.
The other type of hiding method is the transform domain technique which appeared to overcome the robustness and imperceptibility problems found in the LSB substitution techniques.There are many transform 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).Most recent researches are directed to the use of DWT since it is used in the new image compression format JPEG2000 and MPEG4.In[2] the secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients subband unaltered.While in an adaptive hiding capacity function is employed to determine how many bits of the secret message is to be embedded in each of the wavelet coefficients.The advantages of transform domain techniques over spatial domain techniques are their high ability to tolerate noises and some signal processing operation but on the other hand they are computationally complex and hence slower [2].In all proposed techniques for steganography whether spatial or transform the key problem is how to increase the size of the secret messages without causing noticeable distortions in the cover object.Some of these techniques try to achieve the high hiding capacity of the cover according to its local characteristics as in [2-5].
The steganography transform-based techniques have the following disadvantages;low hiding capacity and complex computations [6-7]. Thus,to get over these disadvantage,the present paper proposes an adaptive data hiding technique joined with the use of optimum pixel adjustment algorithm to hide data into the integer wavelet coefficients of the cover image in order to maximize the hiding capacity as much as possible.We also used a pseudorandom generator function to select the embedding location of the integer wavelet coefficients to increase the system security.
Recently,two benchmarks are adopted by steganographic techniques to evaluate the hiding performance.First one is the capacity of hiding data and another one is the imperceptibility of the stego-image,also called the quality of stego-image. The Pixel –Value Differencing (PVD) method proposed by Wu and Tsai [8] can successfully provide both high embedding capacity and

outstanding imperceptibility for the stego-image.Therefore,based on PVD method,various approaches have been proposed

II. The Steganography Method

The proposed method embed the message in Discrete Wavelet Transform coefficients based on GA and OPAP algorithm and then applied on the obtained ambedded image.This section describes this method,and embedding and extracting algorithms in details.

A. Haar Discrete Wavelet Transform

Wavelet transform has the capability to offer some information on frequency-time domain simultaneously. In this transform,time domain is passed through low and high frequencies respectively. This process is repeated for several times and each time a section of the signal is drawn out.

DWT analysis divides signal into two classes (i.e. Approximation and detail) by signal decomposition for various frequency bands and scales.DWT utilizes two function sets:scaling and wavelet which associate with low and high pass filters orderly.Such a decomposition manner bisects time separability.In other words,only half of the samples in a signal are sufficient to represent the whole signal,doubling the frequency separability.

Haar wavelet operates on data by calculating the sums and differences of adjacent elements.This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements.One nice features of the Haar wavelet transform is that the transform is equal to its inverse.Each transform computes the data energy in relocated to the top left hand corner.Figure 1 shows the image lena after one Haar wavelet transform.

Fig. 1: The Image Lena After One Haar wavelet Transform

After each transform is performed the size of the square which contain the most important information is reduced by a factor of 4.

B. Embedding Algorithm

The details of data hiding steps are described as follows.

1. Calculate four difference values d i,(x, y) for four pixel.
2. Using |di,(x, y)| (i = 0,…,3) to locate a suitable R K,I in the designed range table, that is to compute J= min($U_{K,j}$-|$d_{I,(x,y)}$|) where $U_{K,i} \geq |d_{i,(x,y)}|$ for all $1 \leq k \leq n$. Then the located range can be represented by $R_{i,j}$.
3. Compute the amount of secret data bits ti can be embedded in each pair by $R_{j,i}$. The value ti can be estimated from the width $W_{j,i}$, this can be defined by ,t = | $\log_2 w_{j,i}$ |.
4. If ti of P_i (i = 0,1,2) satisfies branch conditions, two pixel pairs of P0 and P3 are processed by the original PVD method. Otherwise, the proposed triway scheme is used to process P_i (i = 0,1,2).
5. Read t_i bits from the binary secret data and transform the bit sequence into a decimal value b_i.
6. Calculate the new difference value d'i,(x, y) .
7. Modify the values of P_n and P_{n+1} by the following formula:
(P'_n ,P'_{n+1}) = (Pn – [m /2] ,Pn+1 + [m /2])
where P_n and P_{n+1} represent two pixels in Pi and m = d' − d .
8. Using the selection rules to choose the optimal reference point $P'_{i(x,y)}$ with minimum MSE, then this selected point is used to offset the other two pixel pairs.
9. Now, the new block constructed from all pixel pairs and embedded with secret data is generated.

C. Image Steganography Model

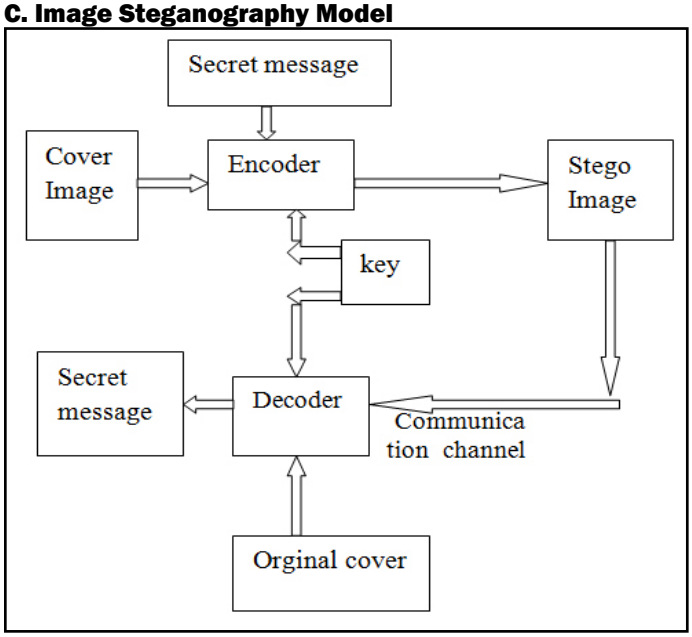

Fig. 2: Model of Steganography

The basic model of steganography is as shown in the above figure. The cover image act as a carrier for the secret data.The secret data is embedded into the cover image by means of a steganographic algorithm.The result obtained is the stego-image is transferred from the sender's end to the receiver's end over the communication channel.At the receivere's end, the same steganographic algorithm works to extract the orginal secret data from the cover image.The sender and receiver must agree upon a common key to embed and extract the secret data from the cover image.

III. Proposed System

The proposed system is an adaptive data hiding scheme, inMwhich randomly selected integer wavelet coefficients of the cover image

are modified with secret message bits. Each of these selected coefficients hide different number of message bits according to the hiding capacity function, the capacity function used is a modified version of the one in . After data insertion we apply optimum pixel adjustment algorithm in to reduce the error induced due to data insertion. The block diagram is shown in fig. 2. We can say that the proposed system is classified into three cases of operation according to different applications; Low hiding capacity with good visual quality (high value of peak signal to noise ratio "PSNR"), average hiding capacity with reasonable visual quality and high hiding capacity with low visual quality.

A. Embedding Algorithm

The blocks of the embedding algorithm is explained in the following steps:

Step 1: Read the cover image file into a two dimensional decimal array to handle the file data more easily.

Step 2: histogram modification it is used to prevent overflow/underflow that occurs when the changed values in integer wavelet coefficients produce stego-image pixel values to exceed 255 or to be smaller than O[5,9]. This problem was found to be caused by the values near 255 or 0 . The problem can be solved by mapping the lowest 15 grayscale levels to the value of 15 and the highest 15 grayscale levels to the value 240.

Step 3: divide the cover image into 8x8 non overlapping blocks. By this division each 8x8 block can be categorized as a smooth or complex block.

Step 4: (Integer wavelet Transform): transform each block to the transform domain using 2D Haar integer wavelet transform resulting LLI, LHI, HLI and HHI.

Step 5: Calculate hiding capacity (number of bits to be used in hiding message bits) of each coefficient, we used a modified version of the hiding capacity function in .The length of LSBs of wavelet coefficients (L) is determined according to [5]:

From experiments we found that as we lower the bits used to hide the secret message in the LL subband the resulted distortion in the stego-image becomes lower; so that we modified this hiding capacity function by using different ranges for k for the LH, HL and HH subbands where its values are form 1 to 4. For the LL subband the value of k is equal to 0 and in some cases the bits used is fixed to only bits to enhance the stego-image quality.

Form experiments of different values of k we divided the system into 3 cases of operation depending on the requirements of the user; these cases are:

Case 1: k 1 for LHl, HLI and HH 1 sub bands, while using 2 bits for embedding data in LL 1 sub band

This case provides low hiding capacity with high visual quality of the stego-image.

Case 2: k 3 for LHl, HLI and HHI subbands, while using 2 bits for embedding data in LL 1 subband

This case is for applications requiring average hiding capacity with reasonable visual quality.

Case 3: k 4 for LHl , HLI and HHI subbands, while k = 0 for LLI subband.

Case 3 is considered as the worst case of data embedding where it is used when the high visual quality of the stegoimage is not important and the user requires only high hiding capacity.

Note that we dropped the case of k=2 because it provided no significant improvement to the result obtained by k=1or k=3.

Step 6: Embed L bits of message into the corresponding randomly chosen coefficients. Random selection of coefficients provides more security where the sequence of the message is only known to both sender and receiver by using a previously agreed upon secret key.

Step 7: Apply optimal pixel adjustment algorithm, while taking into consideration that each modified coefficient stays in its hiding capacity range where each value of L is calculated according to the absolute value of the wavelet coefficients any significant change in this value will producedifferent value of L to be calculated at the receiver.

The main idea of using the Optimum Pixel Adjustment (OPA) algorithm is to minimize the error difference between the original coefficient value and the altered value For example, if a binary number 1000 (decimal number 8) is changed to 1111 (decimal number 15) because its three LSB's were replaced with embedded data; the difference from the original number is 7.

The algorithm we used in is the final step in the proposed scheme, where it can minimize the error by half. The main idea of OPA is to check the bit right next to the last changed LSBs is used to decrease the error

Step 8: Finally, calculate the inverse integer wavelet transform on each 8x8 block to restore the image to spatial domain.

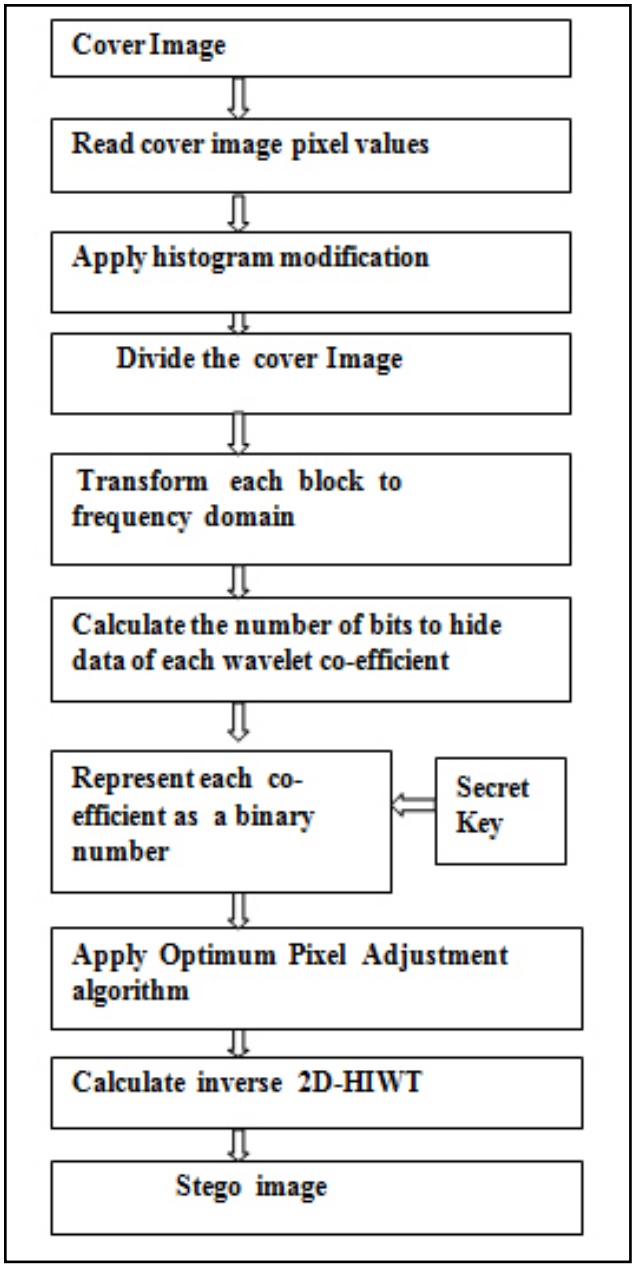

Fig. 3: The Blockdiagram of the Embedding

B. The Extraction Algorithm

At the receiver uses the extraction algorithm to obtain the secret message. The block diagram of the extraction algorithm is shown in fig. 4.

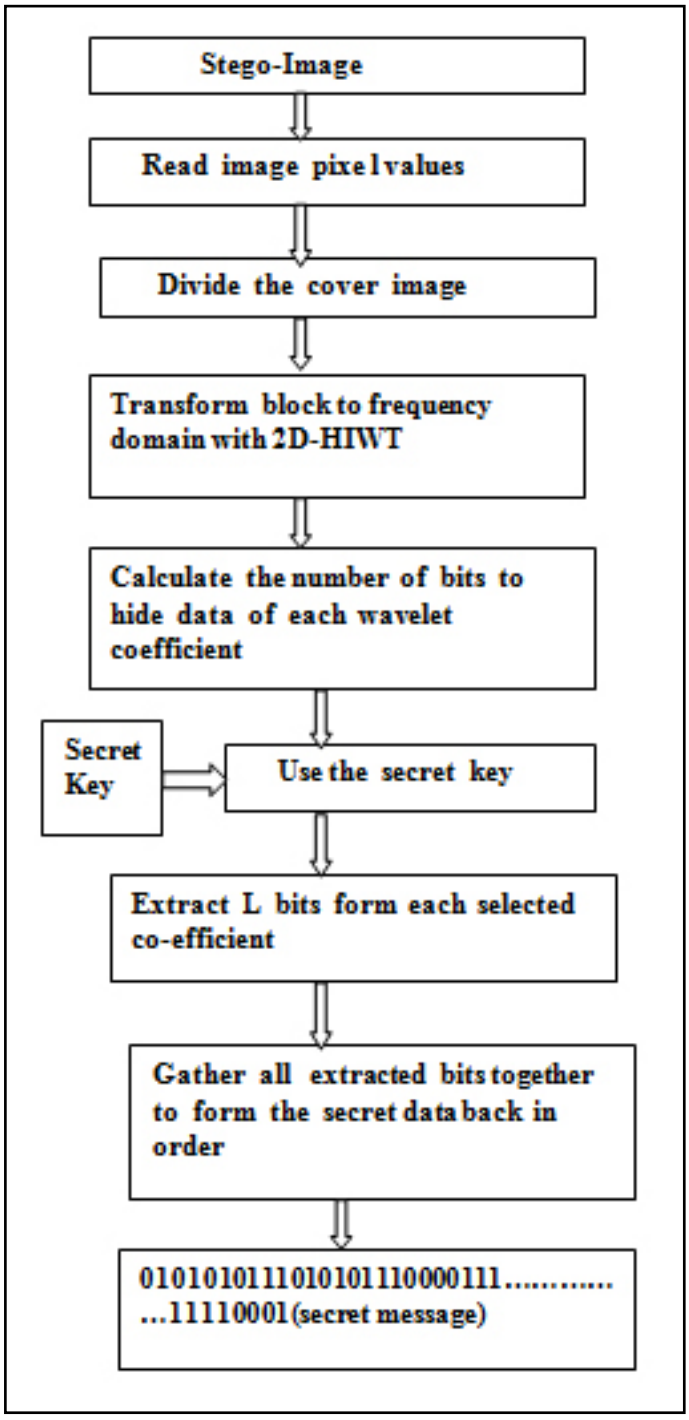

Fig. 4: The Block Diagram of the Extraction Algorithm

As we can see from fig. 4 the extraction procedure is a blind process since it requires only the secret key from the receiver.It is also simpler than the embedding procedure.

IV. Experimental Results

The program was implemented using Matlab 7.4.

The secret message to embed is a randomly generated binary stream with the same length as the calculated hiding capacity.

Fig. 5 shows the original cover images along with their histogram analysis which will be used later to compare it with the ones of the resulting stego-images to test for imperceptibility.

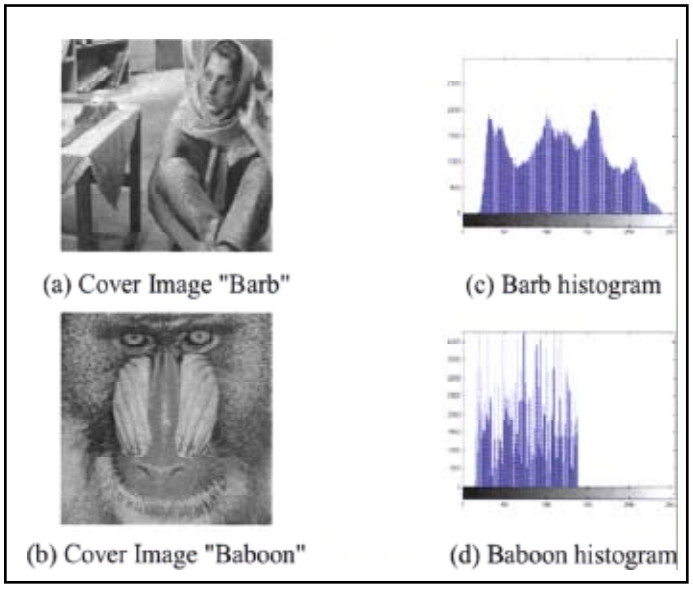

Fig. 5: Three Cover Images Used in System Simulation and Their Corresponding Histogram

A. ImperceptibilityIStego-Image Quality

This aspect measures how much difference distortion) was caused by data hiding in the original cover, where the higher the stego-image quality, the more invisible the hidden message. We can judge the stego-image quality by using Peak Signal to Noise Ratio (PSNR). The PSNR for an image of size MxN is calculated by

$PSNR=10\log_{10}\ [255^2/MSE]$

The MSE is the Mean Square Error, P(x, y) stands for the image pixel value in the cover image and P'(x, y) is for the pixel value at position (x, in the image after inserting secret message. A high value of PSNR means better image quality (less distortion), it is recorded that in grayscale images that the Human Visual System (HVS) can not detect any distortions in stego-images having PSNR that goes beyond 36 dB.

B. Payload /Hiding Capacity

The hiding capacity indicates of how muchdata can be hidden within a cover image without making obvious degradation in the cover image quality. Due to the importance where it has no meaning that an algorithm hides large amount of data and produce large distortion in image quality. So we can say that a steganographic technique is an addition if it proves increase in payload while maintaining an acceptable visual quality of stego-image or improve the stego-image quality at the same hiding capacity level or ifit can improve both [11] .

Fig. 6 shows the resulting stego-images along with their histogram when applying casel (k=1 for the three subbands LHI, HLl and HHI, while using two bits for embedding secret data in LLl subband) of embedding a randomly generated binary stream. The hiding capacity (H.C.) is calculated for each image as a percentage of the cover image size. The values ofH.C. ranges from (22% to 30%). Also the PSNR is calculated for each stego-image and it ranges form (37 dB to 40 dB); which are far above the threshold for the HVS of 36dB.

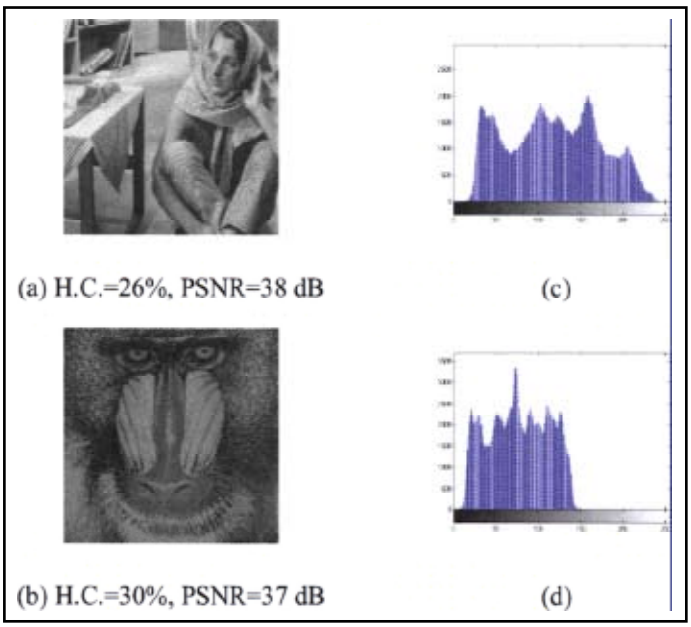

Fig. 6: Output Stego-Image of Case1 for Embedding Data and Their Corresponding Histograms

Comparing the resulting stego images and their histograms with the ones in fig. 4, we can see that there is no significant change in Barb histogram. Unlike barb image we can see that the Baboon histogram is changed significantly due to the large number of edges in the original image although it does not affect the visual quality of the resulting
stego-image.
Fig. 7 and fig. 8 show the corresponding results for case 2 (k 3 for LHI, HLl and HHI subbands, while using 2 bits for embedding data in LLl subband) and case 3 (k 4 for LHI, HLl and HHI subbands, while k=0 for LLl subband)respectively.

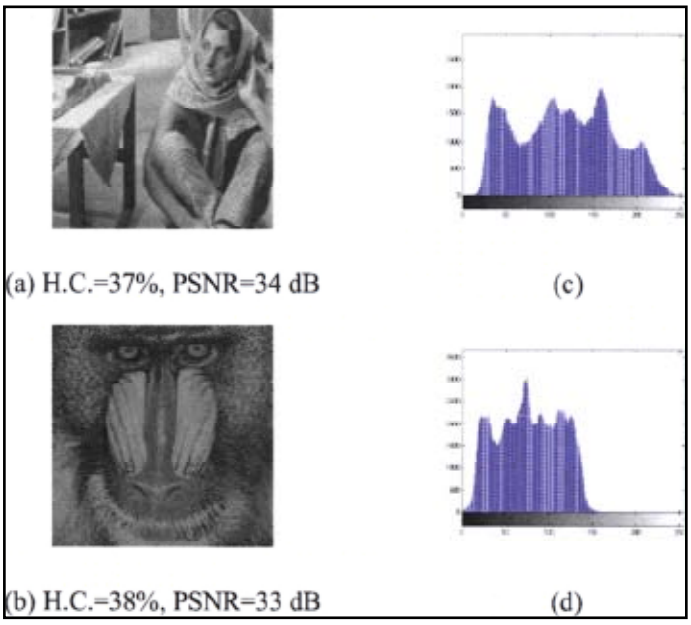

Fig. 8: Output Stego-Images of Case 2 for Embedding Data and their Corresponding Histograms

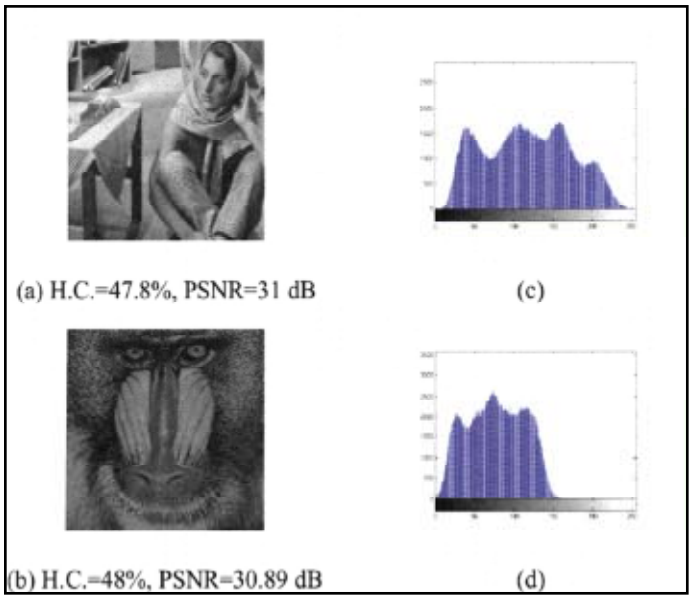

Fig. 9: Output Stego-Images of Case 3 for Embedding Data and Their Corresponding Histograms

Fig. 8 shows that the proposed system can give a high hiding capacity of 48% of the cover image size with a PSNR of about 31 dB which gives a reasonable visual quality of the stego-image. The histogram analysis for both stego-images shows that when the size of secret data increases, thehistogram tends to be smoother. This is clear when comparing the histograms in fig. 5, fig. 6 and fig. 7, with the corresponding ones of the original images in “Fig. 8”.

Fig. 10: Result of Our Proposed Method

Table 1: Comparison of Maximum Hiding Capacity Achieved and the PSNR Obtained Between Our System and the Proposed Systems

Cover image	Method	Max. H.C. (bits)	Max. H.C. (%)	PSNR (dB)
Lena	Proposed technique	986408	47%	31.8
	Adaptive technique using HDWT [10]	801842	38%	33.58
	Distorionless technique using IWT [14]	85507	4%	36.64
	Pixel Value Difference of IWT coefficients [15]	760958	36%	34.63
Baboon	Proposed technique	1008593	48%	30.89
	Adaptive technique using HDWT [10]	883220	42%	32.69
	Distorionless technique using IWT [14]	14916	0.7%	32.76

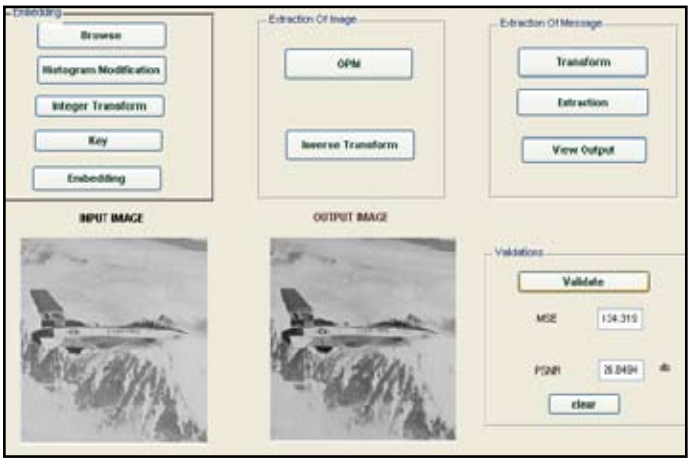

Fig. 11: Result of Our Proposed Method

To further investigate the imperceptibility of the proposed system we compared the hiding capacity of our system with other systems at the same PSNR value and it showed better results. For example, the system in [12] showed a maximum hiding capacity of 36% of the cover image at a PSNR value of 34.63 dB while our system showed a hiding capacity of 38% ofthe cover image at the same PSNR.

The proposed method is applied on 512x512 8-bit grayscale images “Jet”, “Boat”, “Baboon” and “Lena”. The messages are generated randomly with the same length as the maximum hiding capacity. Table I shows the stego image quality by PSNR by the formula. Human visual system is unable to distinguish the grayscale images with PSNR more than 36 dB [5].

V. Conclusion

In this paper, we proposed a novel data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines an adaptive data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. The proposed system embeds secret data in a random order using a secret key only known to both sender and receiver. It is anadaptive system which embeds different number of bits in each wavelet coefficicient according to a hiding capacity function in order to maximize the hiding capacity without sacrificing the visual quality of resulting stego image. The proposed system also minimizes the difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm. There was no error in the recovered message (perfect recovery) at any hiding rate. From the experiments and the obtained results the proposed system proved to achieve high hiding capacity up to 48% of the cover image size with reasonable image quality and high security

References

[1] G.J.Simmons,"Thebprisoner’s problem and the subliminal channel”, In proceedings of Crypto’83, pp. 51-67, 1984.

[2] P.Chen, H.Lin,"A DWT Approach For Image Steganography”, International Journal of Applied Science and Engineering 2006.

[3] H.H.ZAYED,"A High-Hiding Capacity Technique for hiding Data in Images Based on K-Bit LSB Substitution", The 30th International Conference on Artifical Intelligence.

[4] A.Westfeld,“F5a steganography algorithm:? High Capacity despite better steganalysis”, 4th International workshop on Information Hiding.

[5] B.Lai, L.Chang,"Adaptive Data Hiding forImages Based on Harr Discrete Wavelet transform”, Lecture Notes in Computer Science, Vol. 4319/2006.

[6] S.Lee ,C.D.Yoo, T.Kalker,"Reversible image watermarking based on integer-to-integer wavelet transform", IEEE Transactions on Information Forensics and security, Vol. 2, No. 3, Sep. 2007, pp. 321-330.

[7] M.K.Ramani, Dr.E.V.Prasad an Dr.S.Varadarajan, "Steganography Using BPCS to the Integer Wavelet Transformed Image”, UCSNS International Journal of Computer Science and Network Security, July 2007.

[8] D-C.Wu, W-H.Tsai,"A steganographic method for images by pixel value differencing”, Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003.

[9] G.Xuan, J.Zhu, Y.Q.Shi, Z.Ni, W.su,"Distortion data hiding based on integer wavelet transform", IEEE Electronic letters, Dec, 2002.

[10] C.K.Chan, L.M.Cheng,"Hiding data in images by simple LSB substitution", Mar. 2004.

[11] N.Wu, M.Hwang,"Data Hiding:Current Status and Key issues”, International Journalof Network Security, Jan 2007.

[12] J.Liu,M.Shih,"Generalization of Pixel-value Differencing Steganography for Data Hiding in Images”, 2008.

Antony Judice.A received his M.E degree in Applied Electronics from SSN college of Engineering, Chennai, India, in 2008, the B.E degree in ECE from Noorul Islam college of Engineering , Nagercoil, India in 2006, and he is pursuing the Part time Ph.D. degree from Anna University, Chennai. He has five years of Teaching Experience. His research interests include Digital Image processing, Computer network security, Digital signal processing. At present, He is Working as a Assistant Professor in Arunachala College of Engineering for women,Manavilai,Tamil Nadu.

Lekshmi Sree.H.A currently Doing B.E Final year in the Department of ECE at Arunachala college of Engineering for Women, Manavilai, Tamil Nadu. Her research interests include Digital Image processing, Computer network security.

Divya Sree.D.J currently Doing B.E Final year in the Department of ECE at Arunachala college of Engineering for Women, Manavilai, Tamil Nadu. Her research interests include Digital Image processing, Computer network security.