

Steganography Based on Integer Wavelet Transform and Bicubic Interpolation

N. Ajeeshvali

M.Tech student, Department of Electronics and communication engineering,
Gudlavalleru Engineering College, Gudlavalleru
Jawaharlal Nehru Technological University Kakinada, Kakinada
E-mail: ajeeshvali@gmail.com

B.Rajasekhar

Associate Professor, Department of Electronics and Communication Engineering,
Gudlavalleru Engineering College, Gudlavalleru
Jawaharlal Nehru Technological University Kakinada, Kakinada
E-mail: surajb2000@gmail.com

Abstract— Steganography is the art and science of hiding information in unremarkable cover media so as not to observe any suspicion. It is an application under information security field, being classified under information security, Steganography will be characterized by having set of measures that rely on strengths and counter attacks that are caused by weaknesses and vulnerabilities. The aim of this paper is to propose a modified high capacity image steganography technique that depends on integer wavelet transform with acceptable levels of imperceptibility and distortion in the cover image as a medium file and high levels of security. Bicubic interpolation causes overshoot, which increases acutance (apparent sharpness). The Bicubic algorithm is frequently used for scaling images and video for display. The algorithm preserves fine details of the image better than the common bilinear algorithm.

Index Terms— Steganography, Integer Wavelet Transform (IWT), Optimal Pixel Adjustment Process (OPAP), Bicubic interpolation

I. INTRODUCTION

The information communicated comes in numerous forms and is used in peer to peer communication networks and digital communications. Steganography is a type of hiding the communication data that means “covered writing” obtained from the Greek words stegano or “covered” and graphos or “to write”. The goal of Steganography is to hide an information message inside harmless cover medium in such a way that it is impossible even to detect that there is a secret message [1, 2]. The information data-hiding process in a Steganographic system starts by identifying a cover medium’s redundant bits (those that can be modified without destroying that medium’s integrity). The embedding process produces a stego medium by

replacing these redundant bits with data from the hidden message. Such secret communication ranges from the cases of bank transfers, corporate communications, and credit card purchases, a large percentage of everyday mail. Mainly Steganography aim is to keep its presence undetectable, but steganographic systems, because of their nature, leaves detectable traces in the cover medium file. Modifying its statistical properties, anyone can detect the distortions in the resulting stego medium’s statistical properties. The process called statistical steganalysis is used to find the distortions occurred.

II. STEGANOGRAPHY SYSTEM

A steganographic system’s security is dependent on the encoding system’s secrecy. Although such a system might work for a time, it is simple to expose the entire received media like images are passing by to check for hidden messages; such a steganographic system may be fails. Modern steganographic system, as shown in Figure 1 attempts to be detectable only if secret information is known namely, a secret key [1]. In this process, cryptography should be used, which holds that a cryptographic system’s security should dependant solely on the key material. Steganography to remain undetected, the unmodified cover medium by keeping secret, if it is exposed, a comparison between the cover and stego media immediately describes the changes [4, 6].

The basic types of stego systems are available under three models:

- Pure stego systems - no key is used for the system.
- Secret-key stego systems – here a private key is used.
- Public-key stego systems – in this public key is used.

The technique that is followed in this paper will use secret key to encrypt the hidden message that will be encapsulated inside a cover media

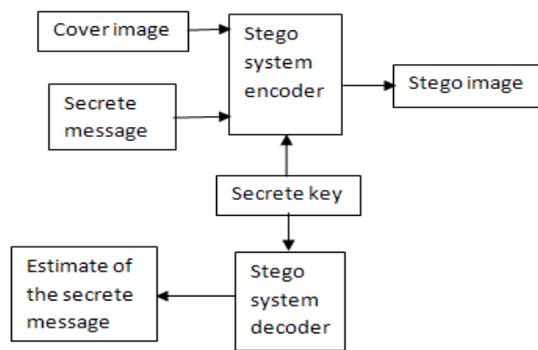


Figure 1. Steganography system

A. Information-hiding system features

An information-hiding system is characterized by having three different aspects that contend with each other: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [6].

B. Data hiding techniques

The most popular hiding techniques are spatial domain and transform domain based techniques. The first group is based on embedding message in the Least Significant Bits (LSB) of image pixels. It has low robustness versus some attacks such as low-pass filtering and compression [5]. Spatial domain based steganography includes the Least Significant Bit (LSB) technique [3]; Pixel value differencing and later includes DCT, DWT and IWT. Several steganography techniques for data hiding in JPEG have been proposed; such as J-Steg [7], JP Hide& Seek [7] and Out-Guess [8]. Most recent researches utilize Discrete Wavelet Transform (DWT) because of its wide application in the new image compression standard, JPEG2000. An example is the employment of an adaptive data embedding technique with the use of OPAP to hide data in Integer Wavelet coefficients of the cover image [9].

III. THE STEGANOGRAPHY METHOD RELATED WORKS

In the proposed method, the message is embedded on Integer Wavelet Transform coefficients based LSB embedding. Then, OPAP algorithm is applied on the obtained embedded image. After that we apply Bicubic interpolation, and then we get the stego image.

A. Wavelet decomposition and histogram modification

We propose to use the integer wavelet transform, for image lossless data hiding to obtain the wavelet coefficients. Because of what is called frequency mask, the data embedded into the high frequency sub bands, HL, LH and HH, will have less visible to human eyes. After data are embedded into some high frequency IWT

coefficients, it is possible that after inverse integer wavelet transform, the grayscale values of some pixels in the marked image may exceed the upper bound (255 for an eight-bit grayscale image) and/or the lower bound (0 for an eight-bit grayscale image). This phenomenon is called overflow/underflow. In order to prevent the overflow and underflow, histogram modification [10] is applied to narrow down the histogram from both sides.

In order to illustrate the histogram narrow down process, we use the following simplified example, where the size of an original image is 6×6 with $8=2^3$ grayscales ($6 \times 6 \times 3$). We can see that the range of the modified histogram now is from 1-6 instead of 0-7, i.e., no pixel assumes gray scales 0 and 7. After modification, grayscale 1 is merged into gray scale 2. Grayscale 0 becomes grayscale 1. In the same way, grayscale 6 is merged into grayscale 5. Grayscale 7 becomes grayscale 6.

Though this example is simple, the histogram modification algorithm illustrated here can be applied to image of large size efficiently in terms of less computation. This efficient histogram modification algorithm has been automatically and successfully applied to all of the 1096 images to our lossless data hiding algorithms.

IV. THE USE OF WAVELET TRANSFORM IN STEGANOGRAPHY

The Wavelet domain is growing up very quickly. Wavelets have been utilized as a powerful tool in many diverse fields, including approximation theory; signal processing, physics, astronomy, and image processing [1]. A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficient and functions. A two-parameter system is constructed such that one has a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal. In Wavelet transform, the original signal (1-D, 2-D, 3-D) is transformed using predefined wavelets. The wavelets are orthogonal, ortho-normal, or biorthogonal, scalar or multi wavelets.

A. One dimensional wavelet decomposition

A single-level one-dimensional Wavelet decomposition with respect to either a particular Wavelet or particular Wavelet decomposition filters is illustrated in Figure 3. Starting from a signal s , two sets of coefficients are computed: approximation coefficients $cA1$, and detail coefficients $cD1$. These vectors are obtained by convolving s with the low-pass filter Lo_D for approximation coefficients and with the high-pass filter Hi_D for detail coefficients, followed by dyadic decimation. The length of each filter is equal to $2N$. If n is the length of s , the signals F and G are of length $n + 2N - 1$, and then the coefficients $cA1$ and $cD1$ are of

length $[(n-1)/2] + N$. The one dimensional decomposition is as shown in figure 2.

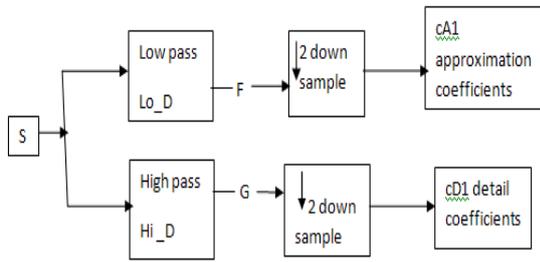


Figure 2. One dimensional wavelet decomposition filters.

B. Multilevel 2-dimensional wavelet decomposition

For images, an algorithm similar to the one dimensional case is possible for two-dimensional Wavelets and scaling functions obtained from one dimensional ones by tensor product [1]. This kind of two- dimensional DWT leads to a decomposition of approximation coefficients at level j in four components: the approximation at level $j+1$, and the details in three orientations (horizontal, vertical, and diagonal), as depicted in Figure 3.

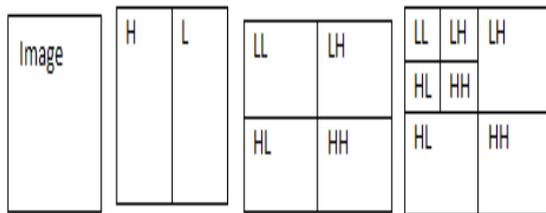


Figure 3. Two dimensional wavelet transformation of an image

Figure 3 describes the basic decomposition step for images using the 2D Wavelet transform. Increasing the levels will add complexity and computational overhead, but the robustness of the steganography method will be enhanced [9]. We can do the same decomposition on the LL quadrant up to $\log 2(\min(\text{height}, \text{width}))$.

C. Integer Wavelet Transform (IWT)

The use of wavelet transform will mainly address the capacity and robustness of information of the information. The Haar wavelet transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients that are generated by taking half of the difference of the same two pixels. The LL sub band is called as approximation band, consists of low frequency wavelet coefficients and contains significant part of the spatial domain image. The other bands LH, HL, HH are called as detail bands, consist of high frequency coefficients and contain the edge details of the spatial domain image. Integer wavelet transform can be obtained by using a lifting scheme. The lifting scheme is a technique used for the conversion of DWT coefficients into integer coefficients without losing information. The problems occurred with floating point precision of the

wavelet filters, we use IWT to avoid. The LL sub band in the case of IWT appears to be a similar copy with smaller scale of the original image but in the case of DWT the resulting LL sub band is distorted [9] as shown in "Figure 4 a, b, c below.



Figure 4.a) Original image

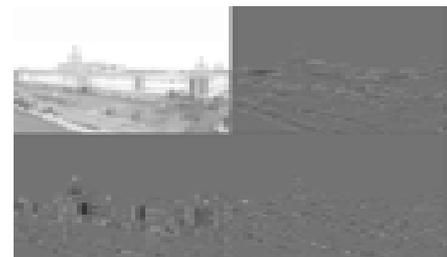


Figure 4.b) IWT image

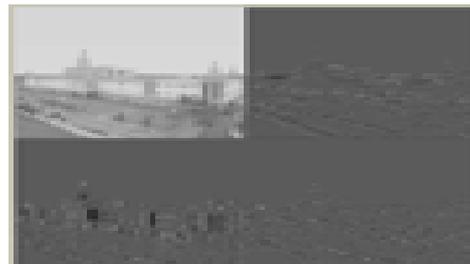


Figure 4.c) DWT image

D. Forward lifting scheme in IWT

Lifting Scheme is one of the techniques on integer wavelet transform. The decomposing filter in integer wavelet transform can be calculated according to [13]:

Step1: Column wise processing to get high (H) and low (L) elements

$$H = (C_o - C_e)$$

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

Where c_o and C_e is the odd and even column wise pixel values

Step2: Row wise processing to get LL, LH, HL, and HH, separate odd and even rows of H and L,

Namely,

$$H_{\text{odd}} - \text{odd row of H}$$

$$L_{\text{odd}} - \text{odd row of L}$$

$$H_{\text{even}} - \text{even row of H}$$

$$L_{\text{even}} - \text{even row of L}$$

$$LH = L_{\text{odd}} - L_{\text{even}}$$

$$LL = L_{\text{even}} - \lfloor (LH/2) \rfloor$$

$$HL = H_{\text{odd}} - H_{\text{even}}$$

$$HH = H_{\text{even}} - \lfloor (HL/2) \rfloor$$

Inverse integer wavelet transform is formed by reverse lifting scheme. Lifting phenomenon is same as forward lifting scheme.

E. Genetic Algorithm

This paper embeds the message inside the cover with the least distortion therefore we have to use mapping function to LSBs of the cover image according to the content of the message. We use Genetic Algorithm to find a mapping function for all the image blocks. Block based strategy can preserve local image property and reduce the algorithm complexity compared to single pixel substitution. In our GA method, a chromosome is encoded as an array of 64 genes containing permutations 1 to 64 that point to pixel numbers in each block. Mating and mutation functions are applied on each chromosome. The mutation process causes the inversion of some bits and produces some new chromosomes, then, we select one which means the best chromosome will survive and be passed to the next generation.

Selecting the fitness function is one of the most important steps in designing a GA-based method. Whereas our GA aims to improve the image quality, Peak Signal to Noise Ratio (PSNR) can be an appropriate evaluation test. Thus the definition of fitness function will be:

The Peak Signal to Noise Ratio is expressed as

$$\text{PSNR} = 10 \log_{10} \left(\frac{I^2}{\text{MSE}} \right) \text{ dB} \quad ; \text{ Where } I=255$$

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

F. OPAP Process

The proposed optimal pixel adjustment process (OPAP) reduces the error caused by the LSB substitution method. In OPAP method the pixel value is adjusted after the secret data is hidden. It is done to improve the quality of the stego image without disturbing the data hidden. The adjustment process is done as follows:

- Let 'n' be the substituted in each pixel.
- Let d= decimal value of the pixel after substitution.
- d1=decimal value of last n bits of the pixel.
- d2=decimal value of n bits hidden in that pixel.
- If $(d1-d2) \leq (2^n)/2$ 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.

G. Bicubic Interpolation

In mathematics, Bicubic interpolation is an extension of cubic interpolation for interpolating data points on a two dimensional regular grid. The interpolated surface is smoother than corresponding surfaces obtained by bilinear interpolation or nearest-neighbor interpolation. Bicubic interpolation can be accomplished using Lagrange polynomials, cubic splines, or cubic convolution algorithm.

In image processing, Bicubic interpolation is often chosen over bilinear interpolation or nearest neighbor in image re-sampling, when speed is not an issue. In contrast to bilinear interpolation, which only takes 4 pixels (2x2) into account, Bicubic interpolation considers 16 pixels (4x4). Images re-sampled with Bicubic interpolation are smoother and have fewer interpolation artifacts. Bicubic interpolation causes overshoot, which increases acutance. The Bicubic algorithm is frequently used for scaling images and video for display. It preserves fine detail better than the common bilinear algorithm. However, due to the negative lobes on the kernel, it causes overshoot. This can cause clipping, but it increases acutance (apparent sharpness), and can be desirable.

V. PROPOSED METHODOLOGY

The proposed system is a high capacity steganography system. Preprocessing includes image resizing and histogram modification. The integer wavelet transform is applied to the cover image to get wavelet coefficients. Wavelet coefficients are randomly selected by using a key for embedding the secret data. Key is an 8x8 binary matrix in which '1' represents the data embedded in the corresponding wavelet coefficients and '0' represents no data present in the wavelet coefficients. The genetic algorithm and optimal pixel algorithm are used to obtain a optimal mapping function and to reduce the error difference between the stego image and cover image.

A. Embedding algorithm

Step 1: Read the cover image as a 2D file with size of any pixels. Do the plane separation of the image into R, G and B.

Step 2: Consider a secret data as a text file. Here each character will take 8 bits.

Step 3: Histogram modification 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 less than 0. All pixel values will be ranged from 15 to 240.

Step 4: Each plane is divided into 8x8 blocks

Step 5: Find the frequency domain representation of blocks by 2D Integer Wavelet Transform and get four sub bands LL1, HL1, LH1, and HH1.

Step 6: Using key calculate the bit length (BL) for corresponding wavelet coefficients. Select the position and coefficients for embedding the 'BL' length data using LSB substitution.

Step 7: The data is embedded only in LH, HL and HH sub bands. Data is not embedded in LL sub band because they are highly sensitive and to maintain good quality after embedding data.

Step 8: Apply optimal pixel adjustment procedure reduces the error caused by the LSB substitution method.

Step 9: Take inverse integer wavelet transform to each 8x8 blocks and combine R, G & B plane to produce stego image.

Step 10: Apply bicubic interpolation in order to smoothen the surface of the image. The bicubic algorithm is frequently used for scaling images and video for display. It preserves fine detail better than the common bilinear algorithm, but it increases acutance (apparent sharpness), and can be desirable.

B. Extraction algorithm

The following steps explain the process of extracting the secret data is as follows:

Step1: Read the stego image as a 2D file

Step 2: Do the plane separations of image and each plane is divided into 8x8 blocks.

Step 3: Apply Haar integer wavelet transform to all planes and get LL, LH, HL, and HH sub bands.

Step 4: Using key calculate the bit length (BL) for corresponding wavelet coefficients and select position and coefficients for extracting the 'BL' length data.

Step 5: Combine all the bits and divide it into 8 bits to get the text message.

C. Performance Metrics

A performance measure in the stego image is measured 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,

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

Where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image $X_{i,j}$ represents the pixels in the original image and $Y_{i,j}$ represents the pixels in the stego-image. The Peak Signal to Noise Ratio is expressed as

$$PSNR = 10 \log_{10} \left(\frac{I^2}{MSE} \right) \text{ dB, Where } I=255$$

VI. EXPERIMENTAL RESULTS

In this present implementation, blue hills and sunset color digital images have taken as cover images. The effectiveness of the stego process proposed has been studied by calculating MSE and PSNR for the two digital images. The messages are generated as with the same length as the maxim hiding capacity. Table2. Show the stego-image quality by PSNR as described. Usually Human visual system (HVS) is unable to distinguish the grayscale images with PSNR more than 35dB. This paper embedded the messages in the 4-LSBs and received a reasonable PSNR.



Figure 5.a) Input image blue hills

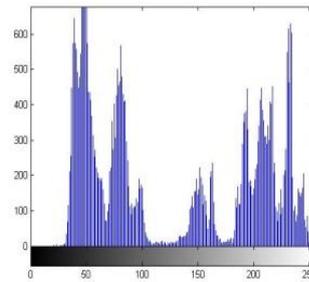


Figure 5.b) Blue hills input histogram

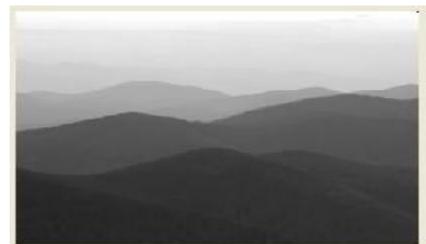


Figure 5.c) Output after embedding 4-LSB

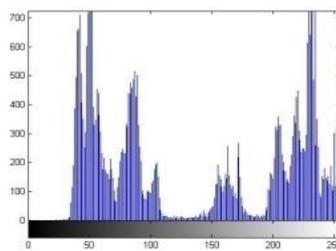


Figure 5.d) Blue hills output histogram



Figure 5.e) Input image sunset

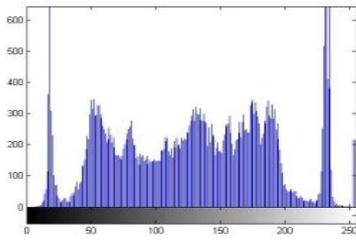


Figure 5.f) Sunset input histogram



Figure 5.g) Output after embedding 4-LSBs

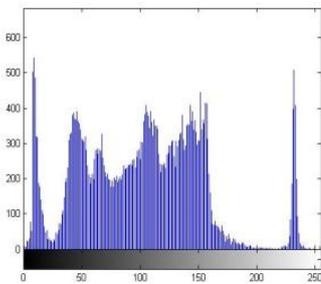


Figure 5.h) Sunset output histogram

The proposed method is applied on the two images namely sunset and blue hills. Figure 5.a shows the input

image of blue hills and its histogram is in figure 5.b as shown. The secret message is embedded in the cover image and the required stego image output is as shown in figure 5.c and its histogram with reference to stego image is in figure 5.d as shown. By observing the two histograms we can find a very small differences between images. The stego image is not susceptible to the observer in order to compare with the input image. As a quality factor for the image is PSNR for the stego-image is observed as approximated to 45dB with very little error performed. The figure 5.e shows the input image sunset used as a cover image for our proposed system. The figure 5.f shows the histogram of cover image in which our secret message is embedded. After embedding message we get the output image as a stego-image and this image is in figure 5.g as shown. The histogram for stego-image is as shown in figure 5.h, after data embedding. By observing two figures the input and output images have approximately same quality. As a result for quality the sunset stego-image obtained a PSNR value of 41dB. The difference between input and output is very little distortion occurred.

The table.1 shows the different images with acceptable PSNR values and less embedding error. The histograms for the images are as shown below for sunset, blue hills figures. The proposed method is applied on 256x256 8-bit gray scale images “sunset” and “blue hills”. The bicubic interpolation takes execution time is more. So in order to reduce the time taken we use median filter in pace of bicubic interpolation to process the images and it smoothens the image. It preserves the edge details of the image with good visibility.

TABLE I. PSNR AND MSE FOR DIFFERENT IMAGES AFTER EMBEDDING THE DATA

NAME OF THE FIGURE	USING GENETIC ALGORITHM		USING BICUBIC INTERPOLATION		USING MEDIAN FILTER	
	PSNR dB	MSE	PSNR dB	MSE	PSNR dB	MSE
COLLEGE	35.02	20.4	35.37	18.8	35.80	17.0
WATER LILIES	35.49	18.3	35.66	17.6	37.24	12.2
WINTER	36.98	13.0	36.81	13.5	38.15	9.9
ROSE	36.89	13.2	36.82	13.4	38.82	8.5
LENA	37.14	12.5	35.38	18.8	39.30	7.6
HILLS	37.39	11.8	35.74	17.3	39.18	7.8
WATER	38.14	8.8	35.90	17.1	39.93	6.5
LEAVES	39.17	7.8	35.93	16.5	41.4	4.8
SUNSET	40.24	6.1	36.68	13.4	41.9	4.1
BLUE HILLS	41.15	1.9	36.24	15.4	44.6	2.2

TABLE II. COMPARISON OF PSNR AND HIDING CAPACITY

Cover image	Method	Max.H.C (bits)	H.C (%)	PSNR (dB)
Blue hills	Proposed method	32768	50%	44.6
Blue hills	Adaptive method	30800	47%	31.82
Sunset	Proposed method	32768	50%	41.9
Sunset	Adaptive method	30800	48%	30.89
Leaves	Proposed method	32768	50%	41.4
Leaves	Adaptive method	30800	47%	30.5

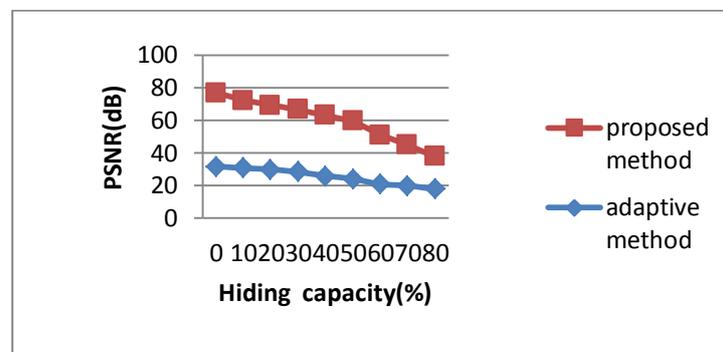


Figure 6. Comparison performance analysis of two methods

The median filter is a nonlinear digital filtering technique, often used to remove noise and is used in digital image processing because; it preserves edges while removing noise. The main idea of the median filter is to run through the signal entry by entry, replacing each entry with the median of neighboring entries. Median filtering is one kind of smoothing technique. While reducing the noise in a signal, it is important to preserve the edges. Edges are of critical importance to the visual appearance of images. The results obtained by using median filter are in table.1 as shown. The table.2 shows the different images with acceptable PSNR values and hiding capacity. The figure.6 shows the comparison performance analysis of two methods. The results show our proposed system yields less embedding error with acceptable PSNR values.

VII. CONCLUSION

We designed a lossless steganography system, to increase the capacity and the imperceptibility of the image after embedding. To avoid problems with floating point precision of the wavelet filters and to decompose the cover image, we used Integer Wavelet Transform. Wavelets transform and key provides high security. Bicubic interpolation is used to increase apparent sharpness. The bicubic algorithm is frequently used for

scaling images and video for display. It preserves fine detail better than the common bilinear algorithm. It was found that the proposed method gives high payload capacity in the cover image with very little error. The drawback of this method is the execution time and the hiding capacity that can be subject of our future studies.

REFERENCES

- [1] Ali Al-Ataby and Fawzi Al-Naima "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" in the International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010
- [2] G M. K. Ramani, E. V. Prasad, S. Varadarajan, "Steganography using BPCS to the integer wavelet transformed image " IJCSNS, Vol. 7, No. 7, pp. 293-302, July 2007.
- [3] C. K. Chan and L. M. Chang, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469- 474, Mar. 2004.
- [4] Lee K. and Chen H., "A High Capacity Image Steganographic Model," in IEEE Proceedings on Vision Image and Signal Processing, China, pp. 288-294, 2000.

- [5] Lin T. and Delp J., "A Review of Data Hiding in Digital Images," in Proceedings of the Image processing.
- [6] N. Provos, "Defending against statistical steganalysis," In Proc. OfiOth Usenix Security Symp, Usenix Assoc, pp. 323-335,2001.
- [7] El Safy, R.O, Zayed. H. H, EI Dessoki. A, "An adaptive steganography technique based on integer wavelet transform," ICNM International Conference on Networking and Media Convergence, pp 111-117,2009.
- [8] Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique Guorong Xuan¹, Yun Q. Shi², Chengyun Yang¹, Yizhan Zheng¹, Dekun Zou², Peiqi Chai
- [9] A.M. Fard, M.R Akbarzadeh and A. F Varasteh. "A new genetic algorithm approach for secure JPEG steganography," International Conference on Engineering of intelligence Systems, pp 1-6,2006.
- [10] Ji. Rongrong, Yao. Hongxun, L. Shaohui and W. Liang, "Genetic algorithm based optimal block mapping method for LSB substitution," International Conference on Information Hiding and Multimedia Signal Processing, pp, 215-218, Dec 2006.
- [11] A.R. Calderbank, I. Daubechies, W. Sweldens and B. Yeo., "Wavelet transforms that map integers to integers," Applied and Computational Harmonic Analysis, vol. 5, no. 3, pp. 332-369, July 1998.
- [12] S. Sarreshtedari, S.Ghaemmaghmi, "High capacity image steganography in wavelet domain", IEEE CCNC 2010 proceedings.



B.Rajasekhar received the B.E degree in Electronics from the Dr.Babasaheb Ambedkar Marthwada University Aurangabad, Maharashtra, India and M.Tech in Digital Systems & Computer Electronics from the JNTU Anantapur, Andhra Pradesh, India. Currently he is

working as Associate Professor at Gudlavalleru Engineering College, Gudlavalleru, and Andhra Pradesh. He is having a total of 12 Years experience in teaching various subjects in Electronics & Communication Engineering branch. His research interests include Wireless Communication and Signal Processing.



N.Ajeeshvali received the B.Tech degree in Electronics and Communications Engineering from the JNTU Kakinada, India and currently doing M.Tech in the specialisation of Digital Electronics & Communication Systems in JNTU

Kakinada, Andhra Pradesh, India.