# Hiding of Data in Images using Spread Spectrum Technique

T. Sai Sampath
Dept. of Electronics and Communication Engineering
Gudlavalleru Engineering College
Gudlavalleru, India

T.S.R. Krishna Prasad, Associate Professor
Dept. of Electronics and Communication Engineering
Gudlavalleru Engineering College
Gudlavalleru, India

***Abstract*— Steganography is an art of hiding some secret information in other image without letting anyone know about presence of secret information except the intended receiver. In the DWT technique the hiding capacity is less and peak signal to noise (PSNR) ratio is less. So, in order to hide large amount of data in digital images using Spread Spectrum technique is used. The Spread Spectrum method improves the Peak Signal to Noise (PSNR) value compared to the DWT technique. The performance of the system is analyzed by varying the gain factor value on the cover image. As the gain factor increases the data present in the stego image will be visible to the human beings.**

***Keywords- DWT, PSNR, Stego Image and Steganography.***

## I. INTRODUCTION

In early days of computer(1940),data security was not an important matter Computers weren't connected as a network, and in order to steal data from computer, it was necessary to inter to the computer room itself, and the security was on the building rather than data or computer. In 1980, a new type of criminals (Hackers) arises, this phrase was used for all computer users and then for information robbers. Many of hackers steal data for challenge only, but some of them for other purposes (financial, competition, etc.).Data threats are existent even in minicomputer systems, and they increase whenever the financial processes increase. Steganography is an art of hiding some secret message in another message without letting anyone know about presence of secret message except the intended receiver. The message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In other words, stego message is combination of host message and secret message. Steganography is often mixed-up with cryptography. Cryptography [4] changes representation of secret message being transmitted while Steganography hides presence [7] of secret message. Steganography can be applied to different media including image, text, audio, video files also [3].

## II. OVERVIEW OF DWT TECHNIQUE IN WAVELET DOMAIN

In LSB technique the message should be [1] extracted easily so DWT technique is used. The Fourier transform is applicable for stable signals only. In order to apply for unstable signals also wavelet transform is used. The Multi Resolution analysis on the images will be done by using the wavelets. The wavelet transform applied on the image then that will divide the image into 4 levels they are approximation [5] coefficients (LL), horizontal coefficients (HL), vertical coefficients (LH), detailed coefficients (HH). The data should be embedded only in the middle band frequency range in HL, LH bands only. Any change in the coefficient values of DWT in LL band there will be degradation in the image quality. Any change in the DWT coefficient in HH band is not detectable to human eyes and it is vulnerable to attacks. Embedding must be done in such a way that minimizes distortion between the host signal and composite signal. In DWT technique the embedding capacity will be less and PSNR value is also less. In order to increase [6] the embedding capacity and Peak Signal to Noise Ratio Spreading is required.

## III. PROPOSED ALGORITHM

In spread spectrum technique the data is spread by using the pseudo random noise sequence. The spreading will be done on the DWT coefficients of image in such a way that Image coefficients Multiplied with the pseudo random noise sequence based on the message bit [2]. In Spread Spectrum Technique the data is spread over many frequency bins so that the energy at those bins will be very small and certainly undetectable. Spreading of the data throughout the spectrum of an image ensures large amount of security.

The proposed algorithm embedded data in the cover image by dyadic sub band decomposition is performed on the cover image using Haar Wavelet transform. For each message bit two Pseudo Noise (PN) sequence of size identical to the size of the DWT coefficients. Based on the message bit the embedding rule will be as follows

$W = V + K X$ If bit = 0
$W = V - K X$ If bit = 1

Where $V$ is wavelet coefficient, $K$ is gain factor, $X$ is PN sequence for the message bit, $W$ is the wavelet coefficient after embedding. Following steps are applied in the data embedding process:

### *A. Data Embedding*

(1). Read the cover image $I_c$ (M, N) of size M x N.
(2). Read the hidden image and convert it into binary form.

(3). Apply "Haar" wavelet transform on the cover image in order and get second level DWT coefficients A2, H2, V2, D2.
(4). Generate n different PN sequence pairs (PN1, PN2) of size (M/4) x (N/4).
(5). If message = 0

H2 = H2 + *K* x PN1
V2 = V2 + *K* x PN2
Else message = 1
H2 = H2 - *K* x PN1
V2 = V2 - *K* x PN2
End

(6). Apply inverse "Haar" transform to get the final Stego image $I_w$ (M, N).

### *B. Extraction of Hidden Data*

The extraction of data from the stego image, the threshold value should be selected in such a way that one third of all the largest coefficients in the LH, HL bands. The value D chooses in such a way that average of the middle band frequencies coefficients. The following steps are applied on the stego image:

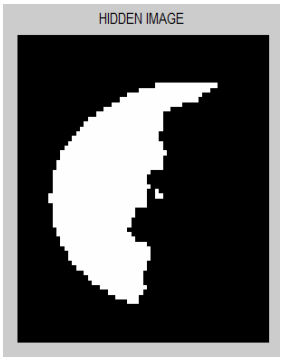
(1). Read the Stego image.
(2). Apply DWT on the Stego image.
(3). If H2 (i, j), V2 (i, j) both < Threshold (TH)
B (i,j) = (H2 (i, j) / S mod 2 + V2 (i, j) / S mod 2) / 2
Else
Maxcoef = max (H2 (i, j), V2 (i, j))
Step = Maxcoef / D;
If Maxcoef = abs (H2 (i, j))
B (i, j) = (V2 (i, j) / Step mod 2)
Else
B (i, j) = (H2 (i, j) / Step mod 2)
End
End

In order to extract the secret image the gain factor value should be chosen properly. The proper value of the gain factor will be useful to extract the message, so, choose proper value for the gain factor.

## IV. PERFORMANCE ANALASIS

First read the cover image of size 256 * 256 image. Calculate DWT on the cover image that will gives 4 coefficients, they are approximation coefficients, horizontal, vertical, detailed coefficients. Apply DWT on the approximation coefficients again it will give 4 coefficients. DWT applied on the approximation coefficients only. Take the pseudo random noise sequence generator same size as that of horizontal and vertical coefficients. Read the message to be hide, convert it into black and white image same as the size of the pseudo random noise sequence. When the message bit is '1' subtract wavelet coefficient of cover image with the product of gain factor and pseudo random noise sequence. When the message bit is '0' add wavelet coefficient of cover image with the product of gain factor and pseudo random noise sequence.

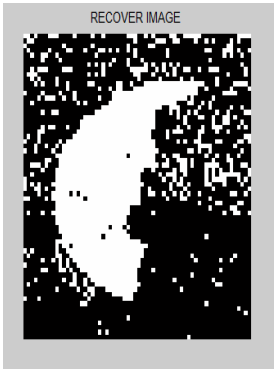
For different values of the gain factor the variation in the stego image will be observed. As the gain factor (*K*) value increases the message that should be hide in the stego image will be clearly visible to the human beings. The proposed method will improves the PSNR value; the comparison will be shown in the Table 1. When *K* = 0.5




*a ) Hidden Image*


*b) Cover Image*


*c) Stego Image*




*d) Recovered Image*

Variation in the stego image when gain factor value increases degradation in the stego image as shown in below figures, and the content that will be present in the stego image will be visible. So the gain factor value should be taken in such a way that the changes in the stego image will not be identified by others. As the gain factor value is increased the signal reconstruction will not possible so gain factor value choose in such a way that nobody can recognize the presence of data in the Stego image. As gain factor increases the PSNR will be decreased (from Table II) so its value should be in between 0 and 1.

*e) For K = 32*

*f) For K = 64*

*g) For K = 128*

*h) For K = 256*

Fig. 1: (a) Hidden image, (b) Cover image, Stego image for different gain factor (*K*) (c) 0.5, (e) 32, (f) 64, (g) 128, (h) 256, (d) Recovered message.

TABLE I

COMPARISON OF PSNR VALUES FOR DIFFERENT HIDDEN IMAGES

| SECRET IMAGE | DWT TECHNIQUE | | SPREAD SPECTRUM TECHNIQUE | |
|---|---|---|---|---|
| | PSNR | MSE | PSNR | MSE |
| MOON.TIF | 39.1712 | 7.8697 | 63.3093 | 0.0243 |
| CIRCUIT.TIF | 39.1696 | 7.8726 | 63.4739 | 0.0248 |
| RICE.PNG | 39.1666 | 7.8781 | 63.2142 | 0.0249 |
| BAG.PNG | 39.1689 | 7.8742 | 63.2918 | 0.0201 |

From the table 1 we can say that for the same size of the message the PSNR value increases and the MSE value decreases for the spread spectrum technique. The variation in the PSNR values of the stego image when gain factor value is increasing shown in the table 2.

TABLE II

COMPARISON OF PSNR VALUES FOR DIFFERENT GAIN FACTOR VALUES ( K )

| SECRET IMAGE | SPREAD SPECTRUM TECHNIQUE FOR DIFFERENT GAIN FACTOR ( K ) VALUES | | | | |
|---|---|---|---|---|---|
| | K=0.5 | K=4 | K=16 | K=32 | K=64 |
| MOON.TIF | 63.3093 | 52.5641 | 43.0619 | 37.5240 | 31.7318 |
| CIRCUIT.TIF | 63.4739 | 52.5333 | 43.1359 | 37.4757 | 31.7875 |
| RICE.PNG | 63.2142 | 52.5351 | 43.1144 | 37.4300 | 31.7322 |
| BAG.PNG | 63.2918 | 52.6225 | 43.0973 | 37.5333 | 31.7408 |

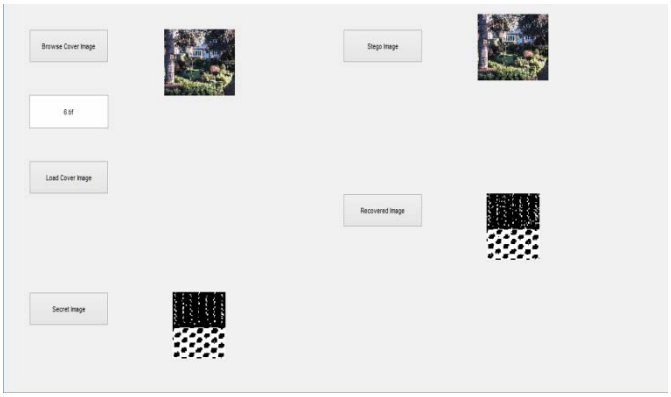



*Fig. 2: Simulation Results When the Cover Image is Color using GUI.*

When the cover image is taken as color image and the embedded message is black and white then the simulation results will be displayed in the GUI. When the cover image is same and the hidden message is different the simulation results will be displayed in the GUI in figure 3.

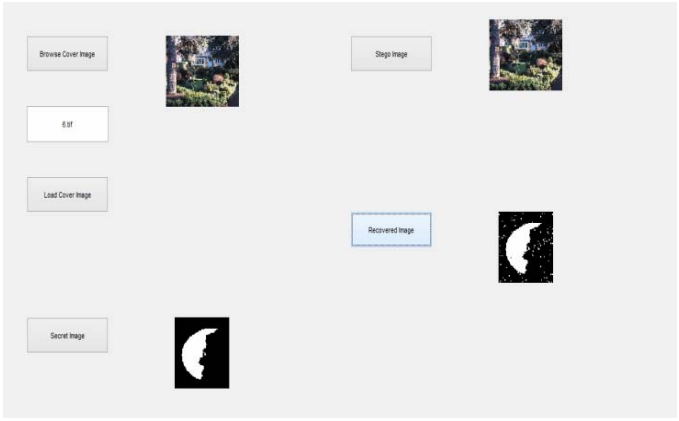



*Fig. 3: Simulation Results using GUI.*

The gain factor value increases the content present in the stego image is visible to others. So, choose proper value for

the gain factor so that the image present in the stego image will not be visible. As gain factor value increases PSNR value decreases and data reconstruction also not possible, so selection of gain factor is an important task in the spread spectrum technique.

## V. CONCLUSION

The gain factor value will be chosen in such a way that the data present in the Stego image will not be visible. As the gain factor value increases, degradation in the Stego image, the PSNR value also decreases, and data reconstruction is not possible. So, selection of gain factor is an important task and the value lies in between 0 to 1. The embedding capacity also increased. So, large amount of data is embedded by using Spread Spectrum technique compared to DWT technique.

## ACKNOWLEDGMENT

We would like to thank our Professor & HOD Dr. M. Kamaraju, in department of Electronics and Communication Engineering in Gudlavalleru Engineering College for his great encouragement and facilities provided for this project.

## REFERENCES

[1] Manu Devi, Nidhi Sharma, “Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images”, Proceedings of RAECS UIET Panjab University Chandigarh, 06 – 08 March, 2014.

[2] Basant Kumar , Harsh Vikram Singh , Surya Pal Singh , Anand Mohan, “ Secure Spread-Spectrum Watermarking for Telemedicine Applications”, Journal of Information Security, vol. 2, pp.no: 91-98, April , 2011.

[3] Arooj Nissar, A.H. Mir, “Classification of Steganalysis techniques: A study”, Digital Signal Processing 20, Elsevier Inc., pp.no:1758–1770, February 13, 2010.

[4] Geetha C R, Dr. Puttamadappa C, “Enhanced Stego-Crypto Techniques of Data Hiding through Geometrical Figures in an Image”, IEEE sponsored 2nd international conference on electronics and communication system (ICECS), pp.no: 116-122, 2015.

[5] Saravanan Chandran, Ph.D, MIEEE, Koushik Bhattacharyya, “Performance Analysis of LSB, DCT, and DWT for Digital Watermarking Application using Steganography”, International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) , 2015.

[6] Krupi Patel, Dr. Leena Ragha, “ Binary Image Steganography in Wavelet Domain ”, International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune, India, pp no: 1635-1640,May 28-30, 2015.

[7]. Rina Mishra, Praveen Bhanodiya, “A Review on Steganography and Cryptography”, International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India, pp.no: 119-122, 2015.

## AUTHOR’S PROFILE

**T. Sai Sampath** is M.Tech student in Gudlavalleru Engineering College, Andhra Pradesh. He has complete B.Tech from Chalapathi Institute of Engineering and technology. His main insteresting areas are Signal Processing, Vlsi design.

**Sri T.S.R Krishna Prasad** is Associate Professor in E.C.E department of Gudlavalleru Engineering College. He has about 13 years of teaching experience and presented papers in several international and national conferences and published papers in international journals. His main insteresting areas are Biomedical, Signal Processing, Security and Cryptography, Steganography.