Image Steganography: Hiding Audio Signal in Image Using Discrete Wavelet Transform

Ms. Asawari S. Shinde, Dr. Archana B. Patankar
Ms. Asawari S. Shinde, Master of Engineering student, Thadomal Shahani College of Engineering, Mumbai-50 (Mob: +91-8097460069; *e-mail: ashu.shinde30@yahoo.com).*
Dr. Archana B. Patankar, Assistant Professor, Thadomal Shahani Engineering College, Mumbai-50 (Mob: +91-9226977842, *E-mail: athawalearchana@gmail.com)*

Abstract— Digital communication allows its users to transfer digital data from one place to another over the network. The digital data is formed of stream of bits, represents a meaningful communication between communicating parties. When this data is sent from one place to another it can be intercepted by the intruders. Therefore in this digital world of communication it has become necessary to provide some protection to the data before it leaves from sender's place. The techniques like Cryptography & Steganography provide such protection to the data travelling through communication channels. Cryptography uses mathematical key on secret data to encrypt the data which generates the encoded version of secret data in the same form as original data and thereby Cryptography provides security but cannot hide the existence of secret data. Whereas Steganography hides the existence of secret data by hiding it in other form of data. This encapsulates the secret of "secret communication". There are many ways in which Steganography can be applied on secret data. This paper is focusing on Image Steganography where the audio is hidden in image using discrete wavelet transform. The difference in Original image and Stegoed image is evaluated by Peak Signal to Noise Ratio and the difference between Original audio i.e secret data and extracted audio is evaluated by Signal to Noise Ratio.

Keywords— Discrete Wavelet Transform, Image Steganography, PSNR, Secret Communication, SNR, SPCC.

*****

I. INTRODUCTION

The word '*Steganography'* is the combination of two Greek words 'Stegano' & 'Graphine'. The meaning of word 'Stegano' is "covered, concealed, or protected" and 'Graphine' means "writing" and therefore together it means "concealed writing"[1]. In short using Steganography we can hide secret information in other communicating medium. The medium used for concealing is called 'cover object'. Cover objects can be in any form. It can be an image, audio, video and which can hide secret audio, image, video, text inside it using Steganography. The Steganography technique which uses image as cover object is called 'Image Steganography'. Generally while developing a technique for Steganography the care is taken about the appearance of the cover object after hiding secret message inside it[1]. For successful Steganography the cover object should not show the changes made to it after hiding secret information. The paper presents Image Steganography technique which hides secret audio in image. Here the cover object is RGB color image and secret object is audio file and Steganography is achieved in transform domain. There are two major domains in which image Steganography can be achieved: Spatial domain and Transform domain. In Spatial domain, the intensity value of a pixel is directly manipulated to store or hide values of secret information whereas in transform domain the cover object is converted into different domain such as frequency domain, to get the transformed coefficients. These transformed coefficients are then manipulated to hide the secret information. Then the inverse transformation is applied on the coefficients to get Stego [2]signals. The transform domain techniques are more immune to attacks than temporal domain techniques because there actual sample values are not modified.

In this paper, the proposed method of Steganography provides extra layer of security by adding a coat of Cryptography before actually performing Steganography. The purpose of this is to tighten the protection provided to the secret information.

A. Features Of Steganography:

1. *Imperceptibility*: The method of Steganography should be such that no intruder should smell the existence of secret information.
2. *Capacity*: The Steganography method should provide as much capacity as it can.
3. *Security*: This feature of Steganography method depicts the quality of Stego signal.
4. *Robustness:* It is the ability of the Steganography method to keep the embedded data intact in cover object[2].

This paper presents Discrete Wavelet transform based Steganography where cover object is image and the secret object is audio signal. The image used is of JPEG type and audio signal used is of wav type.

II. Literature Review

A. Discrete wavelet Transform

Wavelets are small waveforms. Wavelet transform is to change the form of signal to visualize it in some different format. Discrete wavelet transform separates the data into various frequency components. This transformation of signal allows us to separate the frequency component at specific time from the other components[2]. This feature of DWT gives power of separating low frequency components and high frequency components. In wavelet transformation, a base wavelet is selected, a function that is nonzero in some small interval, and it is used to explore the properties of the function in that interval. The wavelet funcion is then translated to another interval of time and used in the same way[6]. So with wavelet transforms, signals with sharp discontinuities can be approximated and also they provide a time-frequency representation of the signal. This image Steganography technique is using DWT to separate high frequency components from the low frequency components of image. By applying DWT on image, the frequency of the image is divided four frequency sub-bands LL, HL, LH, HH. From these four sub-bands LL is the sub-band that carries approximation coefficients which are nothing but significant characteristics of image, whereas other frequency sub-bands carry less important features as they include high frequency components[7]. There are many wavelet transforms in which Haar wavelet transform is simplest one.

B. Haar Wavelet Transform

Alfred Haar introduced first wavelet system in the year of 1910 which is called Haar wavelet. This wavelet is famous for its simplicity and speed of computation. Application of Haar wavelet transform produces two types coefficients coarse approximation and fine details. The coarse coefficients are calculated by averaging two adjacent samples and fine details are calculated by subtracting two adjacent samples. This wavelet transform involves forward and reverse transformation[8]. Forward transformation involves computation of scaling coefficients by adding two adjacent samples and diving them by 2 and computation of wavelet coefficients by subtracting two adjacent samples and diving by 2. Reverse transformation is obtained by simply addition and subtraction of adjacent samples[3].

C. Color formats

The technique introduced in this paper makes use of color format of image to enhance the security measures. Most popular cover object in Steganography is color image. Images can be gray scaled or color images. Color images are more capable than gray scaled images in terms of storage space. RGB (Red Green Blue), HSV (Hue, Saturation, Value), YUV, YIQ, YCbCr (Luminance, Chrominance) etc are different formats of color images. RGB color image represents each of its pixel using three values for each of these colors (Red, Green, Blue). In this proposed work YCbCr color format of image is used by converting RGB color format to YCbCr. YCbCr color format represent image by chrominance and luminance value of each pixel[4]. According to human visual system(HVS), human eyes are more sensitive to small changes in luminance and not to chrominance. That is the HVS is sensitive to brightness of the color rather than color itself. Hence changes made in chrominance component dose not harm the appearance of the image[9]. Using this color conversion increases security level of the technique.

III. Proposed Method

There are two inputs to the method that are cover image and secrete audio. Cover image can be in any form of image file formats i.e it can be .jpeg, .jpg, .bmp etc. Audio file can be in .wav, .mp3 formats. The output file which is nothing but Stego image file is in jpg format.

A. Algorithm for Embedding Secret Audio in Cover image :

Input : Cover Image(CI), Audio Signal(AS).
Output: Stego Image(SI)

i. Read cover image file(CI) and audio signal(AS) from user.

CI=imread('CI.jpg')
AS=audioread('AS.wav')

ii. Convert image from RGB color format to YCbCr color format using,

y=rgb2ycbcr(CI)

iii. Select one of the chrominance components (cb or cr) from YCbCr format using,

cb=y(:,:,2) or cr=y(:,:,3)

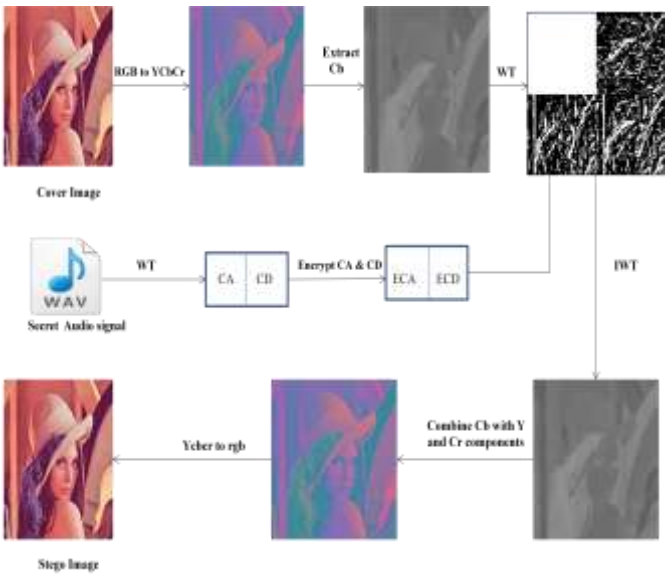

Fig. 1 Embedding secret audio in image

iv. Apply Haar wavelet transform on cb or cr (here assume cb is used) to get low frequency and low frequency sub-bands (LL, HL, LH, HH) by lifting wavelet using LS=liftwave('haar','int2int') and then apply wavelet transform on cb using lwt as,

[LL, HL, LH, HH]=lwt2(double(cb),LS)

v. Obtain wavelet transform of secret audio to get approximation coefficients(CA) and detailed coefficients(CD) using,

[CA,CD]=lwt(double(AS),LS).

vi. Hide approximation coefficients of audio (CA) in high frequency (HH) sub-band of image and detailed

coefficients (CD) in another sub-band(HL) after encrypting them using following method:

Hiding approximation coefficient (CA) of audio in high frequency components (HH) of image:

ESb(i)=bitxor(CA(i),HH(i,4))

HH(i,5)=ESb(i)

Here, ESb(i) is ith Encrypted Secrete bit which is obtained from EX-OR of ith bit of CA and 4th bit of each pixel value of HH from image. And this ESb(i) replaces 5th bit of each pixel value of HH.

vii. Hiding detail coefficients (CD) of audio in high frequency components (HL) of image:

ESb(i)'=bitxor(CD(i),HL(i,4))

HL(i,5)=ESb(i)'

Here, ESb(i)' is ith Encrypted Secrete bit which is obtained from EX-OR of ith bit of CD and 4th bit of each pixel value of HL from image. And this ESb(i)' replaces 5th bit of each pixel value of HL.

vii. Obtain inverse wavelet transform to get stego Cb. Then convert to RGB format.

SCb = ilwt2(LL, HL, LH, HH, LS)

SI=ycbcr2rgb(YSCbCr)

SI =imwrite(SI, 'stego.jpg')

viii. End Embedding.

B. Algorithm for Extracting Secret Audio from Cover image :

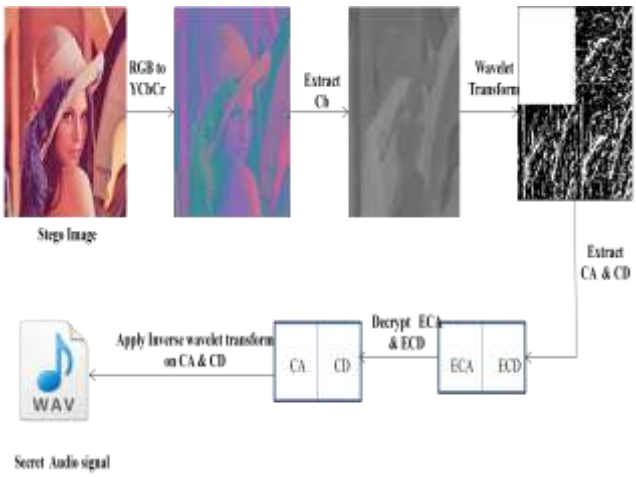

Fig. 2 Extracting secret audio from image

Input : Stego Image (SI),

Output: Extracted Secret Audio (ESA)

i. Read Stego Image (SI) and convert it from RGB to YCbCr format.

SI =imread('SI.jpg')

Ey=rgb2ycbcr(SI)

ii. Extract cb component from Ey and apply haar wavelet transform to get four sub bands (ELL, EHL, ELH, EHH)

Ecb=Ey(:,:,2)

ELS = liftwave ('haar', 'Int2Int')

[ELL, EHL, ELH, EHH] = lwt2(double(Ecb),LS)

iii. Extract the encrypted secret audio bits from the second and third bit planes of EHL and EHH.

iv. Then decrypt bits from EHH and EHL and extract secret audio bits as follows:

To extract approximation coefficients (ECAbin- one dimensional array of bits) from EHH:

ECAbin(i)=bitxor(EHH(i,5),EHH(i,4))

Here, 5th bit from each pixel value in EHH is encrypted secret bit of audio and 4th bit of each pixel value from EHH is the bit used for encryption. Thus EX-ORing these two bits from each pixel value gives original secret bit.

To extract detail coefficients (ECDbin- one dimensional array of bits) from EHL:

ECDbin(i)=bitxor(EHL(i,5),EHL(i,4))

Here, 5th bit from each pixel value in EHL is encrypted secret bit of audio and 4th bit of each pixel value from EHL is the bit used for encryption. Thus EX-ORing these two bits from each pixel value give original secret bit.

v. Arrange bits of ECAbin in length of (secret audio*8) bytes & convert to decimal to get approximation coefficients of secret audio & apply same for ECDbin.

ECA=bin2dec(ECAbin)

ECD=bin2dec(ECDbin)

vi. Obtain inverse wavelet transform for approximation coefficients & detailed coefficients obtained in step v to get the secret audio.

ESA=ilwt(ECA,ECB,LS)

vii. End Extracting.

IV. Results & Analysis

The performance of the algorithm is evaluated based on three parameters: imperceptibility, security and capacity. In any Steganography technique these three performance evaluators play vital role. The imperceptibility is ability of Steganography technique to bring the difference between cover image and stego image which should be near to zero. Here, imperceptibility is achieved by having unnoticeable difference between cover image and stego image.

A. Peak Signal to Noise Ratio (PSNR)

Highest imperceptibility is indicated by high Peak Signal to Noise Ratio(PSNR) value. PSNR value is the ratio of original signal and noise. The lesser the noise value the greater the PSNR value which attains goal of imperceptabily[5]. PSNR value is evaluated using,

$$PSNR = 10 + log10(\mathrm{MAX}^2/MSE)$$

MAX is the maximum value of pixels (255 for grey scale images).The mean square error(MSE) between the original and stego images is given by equation,

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}||\mathrm{O(i,j)} - \mathrm{D(i,j)}||^2$$

Where, pixel from original image is O(i,j) and pixel from stego signal id D(i,j). It is expressed in decibels (dB).

B. Signal to Noise Ratio (SNR)

The method is also evaluated based on similarity between secret audio(original) and extracted secret audio. This correspondence between original and extracted secret audio is measured using SNR(Signal to Noise Ratio). Highest value of SNR indicates that there is lesser difference in original and extracted audio.

$$SNR = 10 \times \log_{10}\left(\frac{\frac{1}{N}\sum_{i=0}^{N} xi^2}{MSE}\right)$$

Where, $MSE = \frac{1}{N}\sum_{i=1}^{N}(xi - yi)^2$ xi is original sample and yi is stego sample.

C. Squared Pearson Correlation Coefficient (SPCC):

Squared Pearson Correlation Coefficient (SPCC) is also used to measures the similarity level between these two signals. The higher the SPCC level, the better is the similarity level. The value of SPCC should be in range of 0 to 1.

D. Response Time

The response time of this method is evaluated using elapsed time in seconds calculated using 'tic toc' function in MATLAB.

Table I shows evaluated values for above parameters when this Steganography method implemented on lena.jpg and ten sample secret audios:

Sr. No.	Input		Results			
			Stego	Extracted		
	Cover image(512X512)	Secret audio samples	PSNR in dB	SNR in dB	SPCC	Elapsed Time in seconds
1	lena.jpg	84143	41.35	Inf	1	68.39
2	lena.jpg	97967	41.18	Inf	1	66.23
3	lena.jpg	93359	41.03	Inf	1	66.2
4	lena.jpg	8094	49.35	Inf	1	55.24
5	lena.jpg	84143	41.85	Inf	1	66.59
6	lena.jpg	57388	43.77	Inf	1	65.11
7	lena.jpg	106354	43.5	Inf	1	70.85
8	lena.jpg	74613	41.79	Inf	1	60.37
9	lena.jpg	65566	44.49	Inf	1	70.09
10	lena.jpg	85334	42.68	Inf	1	69.27

Table I Performance metrics for the stego and extracted secret signals

V. CONCLUSION

The main goal of this paper is to turn up with a technique to conceal any format of secret audio file in cover image in such a way that there are no intelligible changes in the image file after concealing secret audio. The techniques also adds extra security layer by encrypting secret audio before actually covering up audio by an image. The satisfactory results are measured based on three goals of Steganography named as imperceptibility, security and capability. The technique ensures imperceptibility by calculating PSNR between Cover and Stego image. The greater values of PSNR achieves the goal of lesser noise in Stego image and thus indicates that there is invisible difference in over and stego image which is not recognizable by Human Visual System. The proposed scheme also makes sure exact retrieval of secret audio after hiding it in cover image which is indicated by SNR=inf and SPCC=1.

ACKNOWLEDGMENT

The work on this paper is done by Ms. Asawari Shinde Student of Master of Engineering, Department of Computer Engineering Under the guidance of Dr.Archana B. Patankar Assistant Professor in Computer Engineering, in Thadomal College of Engineering, Mumbai.

REFERENCES

[1] Sushil Kumar, S.K.Mutto, "a comparative study of image steganography in wavelet domain", Department of Mathematics, Rajdhani College, University of Delhi, Delhi India IJCSMC, Vol. 2, Issue. 2, February 2013, pg.91 – 101.

[2] Hemalatha Sa, U. Dinesh Acharyaa, Renuka A," Wavelet transform based steganography technique to hide audio signals in image", Manipal Universuty, Manipal 576104, India, ScienceDirect Procedia Computer Science 47 (2015) 272 – 281.

[3] Amol Bhujade, Prof. Sonu Lal," Advanced Steganography: Embedding High Capacity Audio in Colour Image", Dept. of CE, IES College of Tech., Bhopal, India, IJAREEIE,Vol. 4, Issue 7, July 2015.

[4] Yıldıray YALMAN, Dsmail ERTÜRK, "A new color image quality measure based on YUV transformation and PSNR for human vision system", Computer Engineering, Turgut Ozal University, 06010 Ankara, Turkey, Turk J Elec Eng & Comp Sci (2013) 21: 603 – 612.

[5] Vijay Kumar, "Performance Evaluation of DWT based Steganography", IEEE 2nd International Advance Computing Conference, 2010. pg 223-228.

[6] M. I. Khalil,"Image steganography: Hiding short messages within digital images", JCS&T, Vol.11, No. 2. pp 68-73.

[7] Manashee Kalita, "A Comparative Study of Steganography Algorithms of Spatial and Transform Domain", North Eastern Regional Institute of Science and Technology, IJCA,2015.

[8] Vanitha T, Anjalin D Souza , Rashmi B, Sweeta DSouza, "A Review on Steganography Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm", Information Technology, ST Aloysius College, AIMIT Mangalore, India, IJAREEIE, Vol.2, Special Issue 5, October 2014.

[9] Dr. Mahesh Kumar, "Image Steganography Using Frequency Domain", International Journal Of Scientific & Technology Research Volume 3, Issue 9, September 2014.