ISSN 2277-3061

Study of Image steganography using LSB, DFT and DWT

Juned Ahmed Mazumder, K.Hemachandran
Department of Computer Science, Assam University, Silchar
Junedmazumder29@yahoo.in
Department of Computer Science, Assam University, Silchar
khchandran@rediffmail.com

ABSTRACT

In this paper we have studied and implement the color image steganography using LSB, DFT and DWT. First we have studied the various literatures of LSB, DFT and DWT and then implemented one system in which we can do steganography using these techniques, after implementation we have evaluated the results using these techniques applying various image formats against different message size. For each of the cases we have calculated the MSE and PSNR and presented here in a tabulated form. Our main intention is to show how MSE and PSNR changes with respect to different image formats and different message sizes using these techniques. Besides the analysis of MSE and PSNR we have also analyzed the message insertion and message extraction time for all the cases.

INDEX TERMS

Steganography, LSB, DFT, DWT, MSE, PSNR, PNG, BMP, JPEG, TIFF

Council for Innovative Research

Peer Review Research Publishing System

Journal: International Journal of Computers & Technology

Vol 11, No.5

editor@cirworld.com

www.cirworld.com, member.cirworld.com

INTRODUCTION

Steganography is a very old technique of information hiding. Steganography refers to the science of invisible communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer [2]. The term Steganography is forked from the Greek words “steganos” meaning “cover” and “graphia” meaning “writing” defining it as “covered writing” [1]. Before performing steganography we need three primary accessories which are Secret message, Cover medium and one or more embedding algorithm(s) besides these we can also use secret key for better security purpose.

A special case of information hiding is digital watermarking [2]. In digital watermarking the informations which are embedded into digital multimedia content (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Steganography and watermarking differ in a number of ways, including purpose, specifications, and detection/extraction methods [3]. The most fundamental difference is that the object of communication in watermarking is the host signal, with the embedded data providing copyright protection. In steganography the object to be transmitted is the embedded message, and the cover signal serves as an innocuous disguise chosen fairly arbitrarily by the user based on its technical suitability. In addition, the existence of a watermark is often declared openly, and any attempt to remove or invalidate the embedded content renders the host useless.

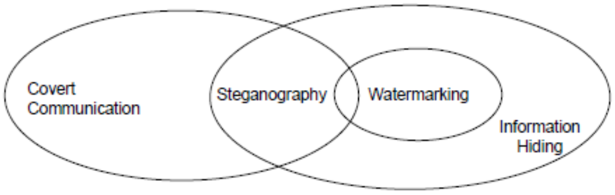


Fig. 1. Relationship of steganography to related fields [2].

In the process of steganography the cover medium can be a text file, an image, an audio file or it can be a video file but among these most popular is the image steganography, so here are the some advantages of using images as cover medium in performing steganography.

- It is the most widely used medium being used today
- Takes advantage of our limited visual perception of colors
- This field is expected to continually grow as computer graphics power also grows

CLASSIFICATION OF STEGANOGRAPHY

Primarily steganography can be classified into two categories

Spatial domain steganography:

In spatial domain steganography we directly deal with the pixel value of the image which means that we directly embed our secret information into some specific value of the pixel. One of the most common and popular spatial domain steganography is the LSB (least significant bit) modification method, it is the most common and also it is a high capacity steganographic method but it is not so much robust against certain attacks like low pass filtering and image compression.

QIM: In terms of insertion schemes, several methods (such as substitution, addition, and adjustment) can be used. One adjustment approach is Quantization Index Modulation (QIM), which uses different quantizers to carry different bits of the secret data.

Masking approaches. These techniques are similar to visible watermarking in which pixel values in masked areas are increased or decreased by some percentage. Reducing the increment to a certain degree makes the mark invisible. In the Patchwork methods, pairs of patches are selected pseudo-randomly; pixel values in each pair are raised by a small constant value in one patch and lowered by the same amount in the other.

Frequency domain steganography:

It is also known as transform domain steganography because before doing steganography we have to convert the original image from its spatial domain to frequency domain using certain methods like Discrete cosine transformation (DCT), Discrete fourier transformation (DFT), Discrete wavelet transformation (DFT) etc. After that we embed our secret information into the coefficients of its transform domain. In this case detection of steganography is very difficult because we embed our secret information into the frequency domain not in the visual domain.

Steganography in compressed domain- In this type of techniques steganographic scheme is combined with an image-compression algorithm (such as JPEG). For example, the steganographic tool Jpeg-Jsteg takes a lossless cover-image and the message to be hidden to generate a JPEG stego-image. In the coding process, DCT coefficients are rounded up or down according to individual bits to be embedded. Such techniques are attractive because JPEG images are popular on the Internet. Other transforms (such as DFT and wavelet transform) can also be used.

Spread-spectrum technique- The hidden data is spread throughout the cover-image based on spreadspectrum techniques (such as frequency hopping). A stego-key is used for encryption to randomly select the frequency channels [3].

RECENT TECHNIQUES OF STEGANOGRAPHY

In the digital era of communication there are various steganographic techniques have been proposed. In this section we have discussed some of the steganographic techniques which were implemented in last couple of years. Gutum at el. [4] proposed an image steganography based on pixel indicator of the cover image. The technique uses least two significant bits of one of the channels Red, Green or Blue as an indicator of data existence in the other two channels. The indicator bits are set randomly (based on the image nature) in the channel. To improve security, the indicator channel is not fixed. The indicators are chosen based on a sequence. In the first pixel Red is the indicator, while Green is Channel 1 and Blue is the channel 2. In the second pixel, Green is the indicator, while Red is channel 1 and Blue is channel 2. In third pixel Blue is the indicator, while Red is channel 1 and Green is channel 2.

The following table describes the meaning of indicator.

Table 1 Meaning of Indicator.

Indicator	Ch1	Ch2
00	No hidden data	No hidden data
01	No hidden data	2 bits of hidden data
10	2 bits of hidden data	No hidden data
11	2 bits of hidden data	2 bits of hidden data

The primary drawback of this method is the robustness as the robustness of this algorithm is not investigated thoroughly.

Ataby, and Fawzi [5] uses DWT to transform cover image from spatial domain to frequency domain. In this technique before applying DWT image statistics-aware test have employed. If the cover image contains unrecognizable patterns and passes the histogram test then the cover image is accepted

For each pixel in the cover image apply level Correction, contrast correction and balance correction. After applying DWT to the cover image threshold calculation was done that will be used to define what is the size (the space) of the redundancy in the cover image that can be used to imbed the message. The drawback of the proposed method is the computational overhead. The method requires resources from the computer hardware (mainly processor speed and memory (RAM)).

Brisbane et al. [6] proposed a method which improves both the imperceptibility and capacity of SMK algorithm. Seppanen, Makela and Keskinarkaus (SMK) have proposed a high-capacity steganographic technique to conceal information within a color image. The technique is significant because of the high volume of data that is embedded into pixels but it results in a high level of noise and so the quality of the resulting image is not acceptable. A new type of coding structure is proposed, which maintains a high capacity but lowers the level of noise. Secondly, an adaptive algorithm is used to identify pixel values that have a high capacity to distortion ratio. Also the maximum size of the coding structures is limited to improve the capacity/distortion tradeoff.

Lin and Shiu [7] proposed a steganographic scheme based on DCT to overcome the limitations of hiding capacity of DCT-based images, they explore the upper bound of hiding capacity of DCT-based images when reversibility is not concerned. To explore the upper bound of hiding capacity of a DCT based image, first divide the coefficients in the middle frequency of a DCT-based image into the six sub-areas. Next, design a hiding strategy based on a notational transformation concept. The most significant difference between the proposed data hiding scheme and existing DCT-based data hiding schemes is the data hiding strategy. Although the cover images used in this scheme are only achieved by quantization, they remain the same as those generated by JPEG compression because quantization is the only lossy process in JPEG compression. Moreover, the image quality of stego-images with this scheme remains above 30 dB for most test images when the hiding capacity is above 90000 bits, which is better than the best image quality offered by existing DCT-based loss or lossless data hiding schemes.

Emam and Nameer [8] implemented a new algorithm based on hiding a large amount of data (image, audio, text) file into color BMP image. They used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel. High security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too. The algorithm can embed efficiently a large amount of data that has been reached to 75% of the image size with high quality of the output.

Chu Wu et al. [9] introduced a novel steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method. First, obtain a different value from two consecutive pixels by utilizing the PVD method. A small difference value can be located on a smooth area and the large one is located on an edged area. In the smooth areas, hide the secret data into the cover image by LSB method while using the PVD method in the edged areas. Because the range width is variable, and the area in which the secret data is concealed by LSB or PVD method are hard to guess, the security level is the same as that of a single using the PVD method of the proposed method.

In this paper we have studied, implemented and analyzed results of steganography in three different techniques one is the LSB method which is a spatial domain steganography and others two techniques are based on frequency domain steganography that is we have used two techniques for converting the cover image from spatial domain to its frequency domain one is the DFT and another is the DWT.

LEAST SIGNIFICANT BIT (LSB) REPLACEMENT METHOD

It is the most simple and common Steganographic process [10,11,12] in which least significant bit of all the bytes or some of the bytes of the value of the pixels are replaced by the bits of the secret message. A sample raster data for 3 pixels (9 bytes) may be represented as

00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101011

↓

Inserting the binary value for

A

(10000001)

Changes 4 bits

↓

00100111 1110100**0** 11001000

0010011**0** 11001000 1110100**0**

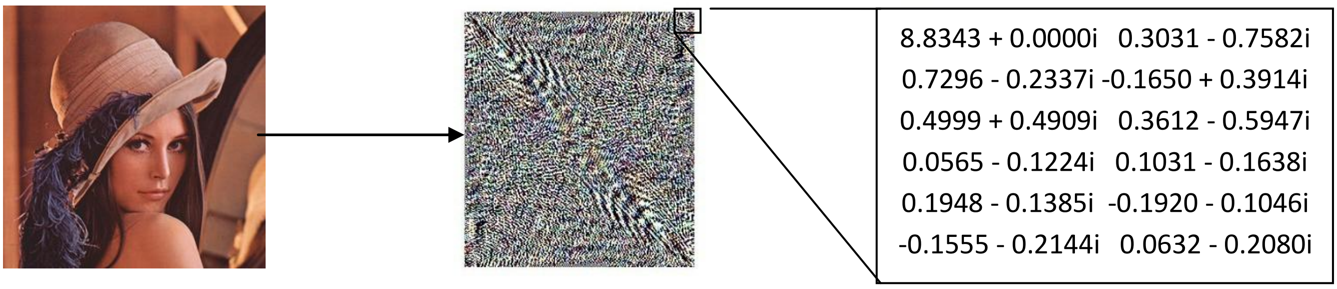
1100100**1** 00100111 11101011

We have implemented one color image steganographic system using this technique in MATLAB in which first we have calculated the length of the message and save it into some specific value of the pixels after converting into binary and this value of the length of the secret message is required during the extraction of the message. After that embed bits of the secret information into all the color components of the cover image starting from the red component and then green and blue. After finishing the insertion processes again we convert these binary values of the pixel into integer for getting the stego-image. For extraction of the secret message at the receiver end we apply the reverse process. We evaluate the result and analyzed these results which will discuss into the later section.

STEGANOGRAPHY USING DISCRETE FOURIER TRANSFORMATION (DFT)

We know that an image (**f(x,y)** of size **M** x **N**) can be represented in the frequency domain (**F(u,v)**) using the equation for the two-dimensional discrete Fourier transform (DFT)[13,14] which is given by the following equation

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\,e^{-i2\pi\left(\frac{ux}{M}+\frac{vx}{N}\right)} \quad ....(1)$$



8.8343 + 0.0000i	0.3031 - 0.7582i
0.7296 - 0.2337i	-0.1650 + 0.3914i
0.4999 + 0.4909i	0.3612 - 0.5947i
0.0565 - 0.1224i	0.1031 - 0.1638i
0.1948 - 0.1385i	-0.1920 - 0.1046i
-0.1555 - 0.2144i	0.0632 - 0.2080i

Original Image DFT representation Coefficients of DFT

Fig.2: DFT representation of an image

The concept behind the Fourier transform is that any waveform can be constructed using a sum of sine and cosine waves of different frequencies. The exponential in the above formula can be expanded into sines and cosines with the variables **u** and **v** determining these frequencies. The inverse of the above discrete Fourier transform is given by the following equation:

$$f(x,y)= \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v)e^{i2\pi(\frac{ux}{M}+\frac{vx}{N})} \text{ ....(2)}$$

Thus from the above inverse relationship we can say that if we have **F(u,v)**, we can obtain the corresponding image (**f(x,y)**) using the inverse discrete Fourier transform. The values of the Fourier transform are complex, meaning they have real and imaginary parts. The imaginary parts are represented by i, which is defined solely by the property that its square is −1, ie: $i^2 = -1$.

MATLAB has three functions to compute the DFT:

1. fft -for one dimension (useful for audio)

2. fft2 -for two dimensions (useful for images)

3. fftn -for n dimensions

In this paper we have developed a color image steganographic system using discrete fourier transformation. In our system first we calculate the length of the secret message and then convert the message into ASCII format, after that we transform the cover image from its spatial domain into its frequency domain using DFT by applying the equation (1). Since we know that Fourier transform are complex and they have real and imaginary parts, so we embed our secret information into only the real parts of the furrier transform. After finishing insertion of secret information we take Inverse DFT by applying equation(2) so that we can get the stego-image.

Again in the process of secret message extraction inverse DFT is applied to the stego-image and find the length of the message and then extract the real coefficients from the DFT representation up to the length of the message.

STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORMATION (DWT)

A wavelet is a wave like oscillation which starts with zero, increases and again decreases and at a certain period of time it backs to zero[15]. If we tell about furrier analysis we say that furrier analysis can able to construct only the frequency representation of a signal where as wavelet analysis can able to represent time-frequency representation of a signal simultaneously. The most basic wavelet transform is the Haar transform described by Alfred Haar in 1910 [16]. It serves as the prototypical wavelet transform. In this paper we have also applied Haar wavelet transformation in the cover image before steganography. In Haar wavelet transformation at each level, the Haar transform decomposes a discrete signal into two components with half of its length: an approximation and a detail component [17]. The first level of approximation $a^1=(a_1,a_2,..a_{N/2})$ is defined as

$$a_m = \frac{X_{2m-1}+X_{2m}}{2} \text{ .... (3)}$$

For m= 1,2,3,.....N/2 , where X is the input signal. The multiplication of 1/2 ensures that the Haar transform preserves the energy of the signal.

The first level detail $d^1 = (d_1,d_2,..d_{N/2})$ is defined by

$$a_m = \frac{X_{2m-1}-X_{2m}}{2} \text{ .... (4)}$$

Let us take an example: X=(4,6,8,10,13,9,3,3) the first and second level approximation and detail components are

$a^{1=}$ (5, 9, 11, 3)

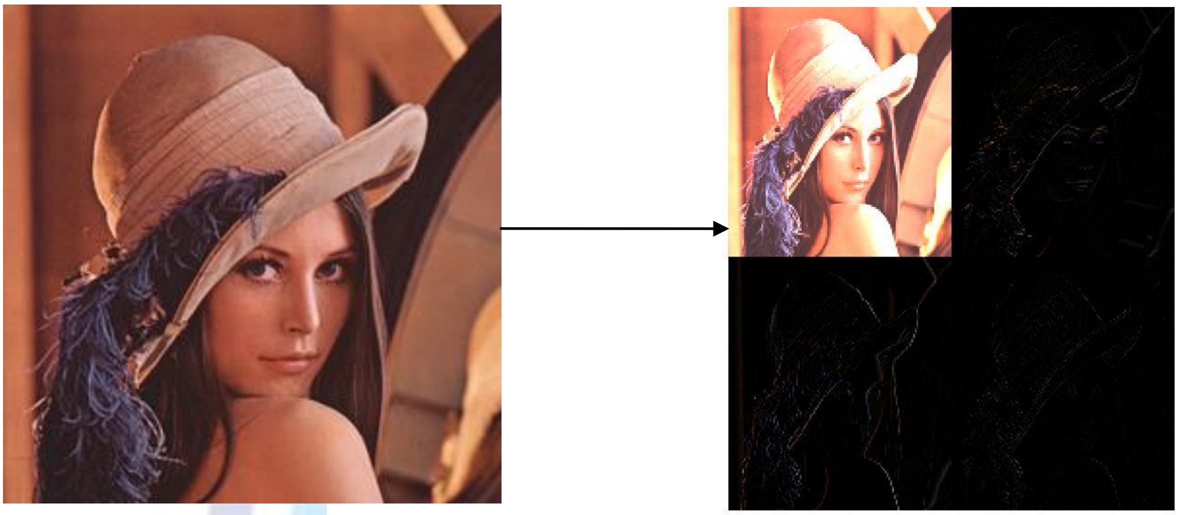
d^1 = (-1,-1, 2, 0)

$a^{2=}$ (7, 7)

d^2 = (-2, 4)

We know that image is a two dimensional representation of the pixel values, so when we apply Haar wavelet transformation to an image it is called 2-D Haar wavelet transformation. In the present system first we apply 2-D Haar wavelet transformation to the cover image where we get the four sub-bands which separate the high and low frequency information. Then we calculate the length of the secret message and save it to the low high frequency sub-band of the wavelet transform. After that convert the secret information into ASCII format which means converting from character to integer format and normalized these integer dividing by length of the message and insert these normalized message into the high frequency sub-bands. At the last step apply Inverse Discrete Wavelet Transformation so that we can get the stego-image. For extracting the secret message we can apply the reverse procedure.

When we apply 2-D Haar DWT to the image “lena.png” we get the following four sub-bands which separate high-frequency and low frequency information.



Original Image

DWT representation

Fig. 3: DWT representation of image “lena.png”

EXPERIMENTAL ANALYSIS

For analysis our results obtained by steganography using LSB, DFT and DWT primarily we used two parameters one is the Mean Squared Error (MSE) and another is the Peak Signal to Noise ratio (PSNR). The MSE is the cumulative squared error between the cover image and the stego-image, whereas PSNR is a measure of the peak error [18,19]. The mathematical formulae for the two are

$$\mathrm{PSNR(f,g)} = 10\log_{10}\frac{255^2}{MSE\,(f,g)} \text{.....................(5)}$$

$$MSE(f,g) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(f_{ij} - g_{ij}\right)^2 \text{.....................(6)}$$

Where f and g are the cover image and stego-image respectively and M and N are the dimensions of the images. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this translates to a high value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the 'signal' is the original image, and the 'noise' is the error in reconstruction.

For this experiment we have taken four image formats: PNG, BMP, JPEG and TIFF and for each image format we insert ten secret messages of sizes starting from 5KB to 50 KB and evaluate their corresponding MSR and PSNR. The following table describes the MSE and PSNR for different image formats and for different message size.

Table 2: Comparison between steganography using LSB, DFT and DWT

Image Format	Image Size (KB)	Message Size (KB)	MSE			PSNR		
			LSB	DFT	DWT	LSB	DFT	DWT
PNG	131	5	0.347493	0.05830	0.0919383	52.7213	60.4741	58.4958
PNG	131	10	0.693071	0.163306	0.355384	49.7230	56.0008	53.6238
PNG	131	15	1.04092	0.407084	0.564821	47.9566	52.034	50.6117
PNG	131	20	1.38824	0.868154	0.776475	46.7061	48.7448	49.2295
PNG	131	25	3.67980	1.944420	1.202720	39.3609	45.2429	47.3292
PNG	131	30	N/A	7.53332	1.550310	N/A	39.3609	46.2266
PNG	131	35	N/A	1015.55	1.637180	N/A	18.0638	45.9898
PNG	131	40	N/A	1045.09	1.9454	N/A	17.9393	45.2407
PNG	131	45	N/A	1053.36	2.1363	N/A	17.9050	44.8342
PNG	131	50	N/A	1059.48	2.31199	N/A	17.8799	44.4909
BMP	192	5	0.347493	0.0583	0.0919383	52.7213	60.4741	58.4958
BMP	192	10	0.693071	0.163306	0.355384	49.723	56.0008	52.6238
BMP	192	15	1.04092	0.407084	0.564821	47.9566	52.034	50.6117
BMP	192	20	1.38824	0.868154	0.776475	46.7061	48.7448	49.2295
BMP	192	25	1.9875	1.94442	1.20272	40.7654	45.2429	47.3292
BMP	192	30	N/A	7.53332	1.55031	N/A	39.3609	46.2266
BMP	192	35	N/A	1015.55	1.63718	N/A	18.0638	45.9898
BMP	192	40	N/A	1045.09	1.9454	N/A	17.9393	45.2407
BMP	192	45	N/A	1053.36	2.1363	N/A	17.905	44.8342
BMP	192	50	N/A	1059.48	2.31199	N/A	17.8799	44.4909
JPEG	101	5	0.350206	8.02293	0.233181	52.6876	39.0875	54.4539
JPEG	101	10	0.695869	8.02099	0.403995	49.7055	39.0885	52.067
JPEG	101	15	1.04346	8.05288	0.691771	47.946	39.0713	49.7312
JPEG	101	20	1.38941	8.08527	0.933584	46.7025	39.0539	48.4293
JPEG	101	25	1.87634	8.23471	1.12332	41.6523	38.9743	47.6258
JPEG	101	30	N/A	9.50374	1.39004	N/A	38.3519	46.7005
JPEG	101	35	N/A	290.268	1.63514	N/A	23.5028	45.9952
JPEG	101	40	N/A	298.93	1.89649	N/A	23.3751	45.3513
JPEG	101	45	N/A	301.467	2.13874	N/A	23.3384	44.8292
JPEG	101	50	N/A	304	2.50382	N/A	23.3021	44.1448
TIFF	207	5	0.347866	0.0628014	0.164745	52.7167	60.1511	55.9627
TIFF	207	10	0.696157	0.175939	0.485681	49.7037	55.6772	51.2673
TIFF	207	15	1.043500	0.425615	0.745267	47.9459	51.8406	49.4077
TIFF	207	20	1.390800	0.929987	1.40609	46.6981	48.4460	46.6507
TIFF	207	25	1.784500	1.990640	1.807	41.6346	45.1409	45.5612
TIFF	207	30	N/A	4.921070	2.14137	N/A	41.2102	44.8239
TIFF	207	35	N/A	463.1440	2.32473	N/A	21.4736	44.4671
TIFF	207	40	N/A	479.8910	2.66345	N/A	21.3194	43.8764
TIFF	207	45	N/A	486.8650	2.83955	N/A	21.2567	43.5983
TIFF	207	50	N/A	492.6740	3.27993	N/A	21.2052	42.9722

Table 3: Message Embedding and Message Extraction Time Comparison between Steganography using LSB, DFT and DWT

Image Format	Image Size	Message Size	Message Embedding Time			Message Extraction Time		
			LSB	DFT	DWT	LSB	DFT	DWT
PNG	131	5	3.28845	0.386106	0.0464568	3.33646	0.913153	1.20287
PNG	131	10	4.47846	0.488725	0.0593641	7.00002	1.60768	2.81804
PNG	131	15	6.93794	0.530178	0.0611298	14.5723	2.33005	4.86875
PNG	131	20	10.8975	1.74393	0.667499	23.7607	3.40601	7.57466
PNG	131	25	14.6745	0.775574	0.767517	31.4512	3.57493	10.3154
PNG	131	30	N/A	0.955237	0.8493137	N/A	4.20299	13.788
PNG	131	35	N/A	1.14236	0.9652568	N/A	4.97154	17.7564
PNG	131	40	N/A	1.40749	0.9944928	N/A	5.53494	22.6268
PNG	131	45	N/A	1.61533	1.056621	N/A	6.12268	26.9396
PNG	131	50	N/A	1.95822	1.6598706	N/A	6.8466	33.2301
BMP	192	5	3.54264	0.370348	0.0517838	3.64535	0.877405	1.20405
BMP	192	10	6.06587	0.412432	0.05394	7.87892	1.55533	2.69825
BMP	192	15	8.23132	0.496792	0.0573399	15.1170	2.07578	4.70013
BMP	192	20	10.2780	0.586761	0.0669027	24.0822	2.75667	7.20858
BMP	192	25	13.2134	0.741373	0.074807	29.5123	3.52606	10.2564
BMP	192	30	N/A	0.90688	0.0811712	N/A	4.17792	13.7166
BMP	192	35	N/A	1.09865	0.0878311	N/A	4.85999	17.6781
BMP	192	40	N/A	1.35343	0.0946617	N/A	5.57951	22.6537
BMP	192	45	N/A	1.58711	0.1577046	N/A	6.15232	27.0635
JPEG	101	5	3.39276	0.402627	0.0703104	3.26611	0.859741	1.2429
JPEG	101	10	49.7055	0.412956	0.0771458	7.21033	1.57581	2.72391
JPEG	101	15	9.0124	0.487305	0.079376	13.7719	2.19262	4.7325
JPEG	101	20	10.0798	0.58985	0.080747	23.8811	2.87872	7.23236
JPEG	101	25	13.0634	0.722868	0.0851928	29.4312	3.54681	10.2997
JPEG	101	30	N/A	0.914052	0.0969749	N/A	4.19884	13.6823
JPEG	101	35	N/A	1.09758	0.1573086	N/A	4.86022	17.8253
JPEG	101	40	N/A	1.36884	0.168771	N/A	5.57255	22.695
JPEG	101	45	N/A	1.56986	0.23987	N/A	6.9875	27.984
JPEG	101	50	N/A	1.78956	0.29078	N/A	7.9854	31.4975
TIFF	207	5	3.48373	0.537719	0.0503232	3.31627	0.889912	1.16967
TIFF	207	10	6.67525	0.538723	0.0555466	7.76445	1.58398	2.73012
TIFF	207	15	8.88232	0.620012	0.0597502	14.2868	2.22284	4.76685
TIFF	207	20	11.5424	0.586761	0.0669025	24.3079	2.75667	7.20858

TIFF	207	25	13.5321	0.741373	0.074804	29.6342	3.52606	10.2564
TIFF	207	30	N/A	0.90688	0.0811713	N/A	4.17792	13.7166
TIFF	207	35	N/A	1.09865	0.0878323	N/A	4.85999	17.6781
TIFF	207	40	N/A	1.35343	0.0946611	N/A	5.57951	22.6537
TIFF	207	45	N/A	1.58711	0.1577032	N/A	6.15232	27.0635

Besides the analysis of MSE and PSNR we have also analyze the message insertion and message extraction time for each of the cases.

CONCLUSION

In this paper an attempt has been made to study and implement the color image steganography using LSB, DFT and DWT. For analysis the results we have used mainly two parameters MSE and PSNR and calculate these values for four image formats and for each image formats we insert ten secret messages of sizes starting from 5 KB to 50 KB. In all the image formats and for all the message sizes LSB gives high MSE and low PSNR as compared to DFT and DWT. When we compare MSE and PSNR for DFT and DWT we found that for lower values of message size that is up to 15 KB, DFT shows better results than that of DWT which means DFT gives lower MSE and Higher PSNR but for large message size DWT shows better results than that of DFT. But in case of JPEG image format for all the message size DWT gives better results than DFT, this is because we know that JPEG is one type of compressed image and also DWT is a technique of image compression, in JPEG200 DWT is use for compressing the image. So we can say that for large payloads DWT is better option for steganography. Besides the analysis of MSE and PSNR we have also analyze the message insertion and message extraction time. In case of time analysis for all the image formats and message size DFT gives better results than that of other two.

REFERENCES

[1] S. Katzenbeisser, F.A.P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking” Artech House, Norwood, MA, 2000

[2] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon,”Image Steganography: Concepts and Practice”, WSPC/Lecture Notes Series: 9in x 6in, April 22, 2004

[3] Huaiqing wang and Shuozhong wang, “Cyber Warfare:

Steganography vs. Steganalysis”, COMMUNICATIONS OF THE ACM, Vol. 47, No. 10, October 2004

[4] Gutub, Adnan, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, and Aleem Alvi. "Pixel indicator high capacity technique for RGB image based Steganography." In WoSPA 2008-5th IEEE International Workshop on Signal Processing and its Applications. 2008.

[5] Al-Ataby, Ali, and Fawzi Al-Naima. "A modified high capacity image steganography technique based on wavelet transform." changes 4 (2008): 6.

[6] Brisbane, G., R. Safavi-Naini, and P. Ogunbona. "High-capacity steganography using a shared colour palette." In Vision, Image and Signal Processing, IEE Proceedings-, vol. 152, no. 6, pp. 787-792. IET, 2005.

[7] Lin, Chia-Chen, and Pei-Feng Shiu. "High capacity data hiding scheme for DCT-based images." Journal of Information Hiding and Multimedia Signal Processing1, no. 3 (2010): 220-240.

[8] EL-Emam, Nameer N. "Hiding a large amount of data with high security using steganography algorithm." Journal of Computer Science 3, no. 4 (2007): 223.

[9] Hsien-Chu Wu, Na-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, “An Image Steganographic Scheme Based on Pixel-Value Di®erencing and LSB Replacement Methods” National Science Council, Taiwan, November 7, 2004

[10] R. J. Anderson and Fabien A. P. Petitcolas, “On the limits of steganography”, IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 474-481, 1998.

[11] Jessica Fridrich, Rui Du, Meng Long, “STEGANALYSIS OF LSB ENCODING IN COLOR IMAGES”; Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference.

[12] S. Katzenbeisser, F.A.P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking” Artech House, Norwood, MA, 2000.

[13] Nabin Ghoshal, Jyotsna Kumar Manda, “A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT)”, Malaysian Journal of Computer Science, Vol. 21(1), 2008

[14] Awanish Kr Kaushik, “A Novel Approach for Digital Watermarking of an Image Using DFT”, International Journal of Electronics and Computer Science Engineering ISSN-2277-1956

[15] LIU Tong, QIU Zheng-ding “A DWT-based color Images Steganography Scheme” IEEE International Conference on Signal Processing, vol. 2, pp.1568-1571, 2002

[16] Nag Amitava, Biswas Sushanta, Sarkar Debasree, Sarkar Partha Pratim, “A Novel Technique for Image Steganography Based on DWT and Huffman Encoding” International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6) (2011): 561-570

[17] Reddy, HS Manjunatha, and K. B. Raja. "High capacity and security steganography using discrete wavelet transform." International Journal of Computer Science and Security (IJCSS) 3, no. 6 (2009): 462.

[18] Pooja Kaushik and Yuvraj Sharma, “Comparison of Different Image Enhancement Techniques Based Upon Psnr & Mse”, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11 (2012)

[19] Hore, Alain, and Djemel Ziou. "Image quality metrics: PSNR vs. SSIM." In Pattern Recognition (ICPR), 2010 20th International Conference on, pp. 2366-2369. IEEE, 2010.

[20] http://www.mathworks.com/access/helpdesk/help/toolbox/images

[21] Mazumder, Juned Ahmed, and Kattamanchi Hemachandran. "A High Capacity and Secured Color Image Steganographic Technique Using Discrete Wavelet Transformation.", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (4) , 2013, 583 – 589

[22] Mazumder, Juned Ahmed, and K. Hemachandran. "Review Of Different Techniques Used In Recent Steganography Researches." International Journal of Engineering 1, no. 8 (2012).

Juned Ahmed Mazumder received his Master of Science in Computer Science (5 years integrated course) degree with first class in 2011 from Department of Computer Science, Assam University, Silchar, where he is currently doing his Ph.D. His research interest includes Image Processing, Steganography, Neural Network and Data Security.

Prof. K. Hemachandran is associated with the Department of Computer Science, Assam University, Silchar, since 1998. Currently he is serving as the Head of the Department in the Department of Computer Science, Assam University, Silchar. He obtained his M.Sc. Degree from Sri Venkateswara University, Tirupati and M.Tech and Ph.D Degrees from Indian School of Mines, Dhanbad. His areas of research interest are Image Processing, Software Engineering and Distributed computing.