International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Practical Quality-Aware Image Quality Analysis System

Duleshwari Gajanan Wankhade[1], R. D. Sushir[2]

[1]Sant Gadge Baba Amravati University, Department of Electronics and Telecommunication Engineering, Kathora Road 444604, Amravati

[2]Professor, Department of Electronics and Telecommunication Engineering, Sant Gadge Baba Amravati University, Kathora Road 444604, Amravati

Abstract*: In this paper the focus is on maintaining secrecy between two communication parties using steganography and cryptography technique. In this system cover data (Image) and secret data (Image / Text) by using DWT (Discrete wavelet transform) then secret data is first embedded in to cover image by using LSB (Least Significant Bits) algorithm and then resulted embedded image by using IDWT (Inverse Discrete Wavelets Transform) algorithm to form Stego-image. Then DWT (Discrete Wavelets Transform) algorithm on the stego image then resulted image by using LSB extraction to form recovered secret data. For the analysis of the proposed method MSE, RMSE, PSNR, Correlation and SNR was calculated for each of the cover and recovered secret data. The DWT (Discrete Wavelets Transform) algorithm is found to be better in the terms of efficiency, robustness, highly security and embedding capacity. With rapid growth of World Wide Web and advance computer network, we need security, privacy, integrity and authentication in the data communication. A steganography is art of hiding sensitive information in another cover medium. The main objective of this paper is to achieve quality and secure communication.*

Keywords: Steganography, Cryptography, LSB, DWT, Security, MSE, PSNR, Correlation.

1. Introduction

Cryptography is a technique for securing the secrecy of communication. Many different encrypt and decrypt methods have been implemented to maintain the secrecy of the message. , it may also be necessary to keep the existence of the message secret. Steganography is the art and science of invisible communication of messages. It is done by hiding information in other information, i.e. hiding the existence of the communicated information. In image steganography the information is hidden in images. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. The difference between Steganography and Cryptography is that the cryptography focuses on keeping the message content secret whereas in steganography focus on keeping the existence of a message secret. Steganography and cryptography are the ways for protecting information from unwanted parties. Cryptography is the two sides, first is the sender side and another is receiver side. Sender side included the plaintext is a message, data, image and code etc. We want to send on telecommunication. Encryption is the process by which a plaintext into delivered ciphertext with the predefined key. Ciphertext is nothing but a converted on plaintext, output of encryption process. Receiver side ciphertext as same as the sender side then decryption process by which convert a ciphertext into plaintext. Encryption of sender side and decryption of receiver side are using same key is called symmetric key and different key is called asymmetric key.

Steganography is defined as the art of hiding data in order to prevent the detection of the secret message. Steganography process is the cover data the term “cover” is used to describe the original innocent message, image, audio, video etc. Then embedding process the information which is to be concealed. The information to be hidden in the cover data is known as the “embedded” data. The secret data is encrypted using a secret key and then embedded in a cover image. This produced a stego image and sent through a communication channel. Then extraction process in which the embedded message is extracted from the stego image or data to complete the hidden communication process. Since the stego key is used in the embedding process, it needs to be used in the extracting process. They produced extracted secret data.

2. Literature Review

Possible techniques for Quality Image quality analysis system can be generally divided into the following categories:

Mohit Kalra, D. Ghosh [1] proposed a new framework for image compression that combines compressed sensing theory with wavelet and vector quantization. Wavelet transform is used to sparsify the input image while measurement vectors generated from the sparse vectors are transmitted using vector quantization. Simulation experiments are carried out to analyze the effects of various parameters on the image reconstruction quality. The algorithm proposed in this paper first decomposes the original image using 2-dimensional discrete wavelet transform which produces multi-scale image decomposition revealing data redundancy in several scales. The purpose served by DWT is that it produces a large number of values having zero, or near zero, magnitudes. Therefore, with proper thresholding, they can have a sparse representation of the image with only a few non-zero values in the thresholded transform domain. Experimental results demonstrate that the selection of the number of vectors to be combined, threshold value, number of measurements, dictionary matrix and the wavelet function, all affect the quality of the reconstructed image. Therefore, the performance of our algorithm can be improved by making proper selection of these parameters.

Lip Yee Por, Delina Beh, Tan Fong Ang and Sim Ying Ong [2] proposed a scheme has been developed with the aims to help in improving the payload of the secret data at the same time retaining the quality of the stego-image produced within an acceptance threshold. The modification of the current LSB substitution algorithm by delivering a new algorithm namely sequential colour cycle. For achieving a higher security, multi-layered steganography can be performed by embedding a secret data into multiple layers of cover-images. The performance evaluation has been tested and proven that the improvement of embedding ratio at 1:2 for the proposed algorithm can be achieved and the value of the image quality is not falling below the threshold of distortion. The proposed scheme is to improve the embedding ratio in comparison with the current existing method; Morkel recommended using lossless images such as BMP and GIF for steganography because lossless compression will not remove any information from the image. In fact, using lossless compression on digital bitmap images keep the original information intact. Lempel-Ziv-Welch (LZW) data compression reduces the size of GIF files without degrading the image visually. Apparently, the most widely used GIF format supports up to 8bits per pixel which limits its palette to just 256 colours. In steganography perspective, GIF restricts the types of data file (i.e., only text message) during the embedding process.

With the exception of transform domain based steganography, lossy compression is avoided because it discards excessive amount of image data consequently destroying properties of the stego image. BMP-24 on the other hand supports up to 16,777,216 colours giving it an advantage in manipulating colours to embed secret data. Therefore BMP-24 is a favorable format choice for cover images in the proposed. A new algorithm using sequential colour cycle is proposed to optimize the current LSB mechanism by utilizing and integrating stego one LSB to stego four LSBs and also stego colour cycle LSB. As a result, the proposed scheme is able to encode up to four LSBs in the each of the RGB pixels according to the contents of the secret data without visually degrading the stego-image.

Preeti Chaturvedi, R. K. Bairwa [3] proposed by steganography is a medium to hide the secret messaging in such a way that only sender and receiver only know about it. No other one on network cannot suspects the existence of the messages. The proposed image steganography methods for hiding secret message in colored images by using integer wavelet transform. Steganography method is provides more security to images that contain secret message. The proposed techniques use the LSB technique. This is the method flow sheet for data embedding module to illustrate the initiation of security measures at the side of implementation of IWT and Genetic rule. The main purpose of this application is to point out the flow of information embedding operation involved in the process. The frequency domain illustration of the individual created blocks is calculable by 2 dimensional integer ripple transform in order to accomplish 4 sub bands LL1, HL1, LH1, and HH1. One to sixty four genes area unit generated containing the pixels numbers of each 8x8 blocks because the mapping operates. The bits of message in 4-LSBs IWT coefficients each component consistent with mapping functions area unit embedded. Consistent with fitness analysis, optimal component Adjustment process applied on the Image. At the end, inverse 2nd IWT is computed during this module in order to generate the stego image.

Anu, Komal, Shipra Khurana, Amit Kumar [4] described the image quality assessment techniques i.e. used for assessing the qualities of the images sending over the different mediums. Full reference model of objective quality assessment is used. Full reference model is a method, in which they have access to a perfect version of the image against which we compare it with a „distorted version‟ of that image. The effects are calculated in terms of some mathematical metrics PSNR, SNR and MSSIM. In this method QA algorithm have access to a 'perfect version' of the image or video against which it can compare a 'distorted version'. The 'perfect version' generally comes from a high-quality acquisition device, before it is distorted by, say, compression artifacts and transmission errors. However, the reference image or video generally requires much more resources than the distorted version, and hence FR QA is generally only used as a tool for designing image and video processing algorithms for in-lab testing, and cannot be deployed as an application**.** To evaluate the quality of a distorted image, FR metrics, which have access to both whole original and reconstructed information, provide the most precise evaluation results compared with NR and RR.

In the field of image processing, image quality assessment is a fundamental and challenging problem with many interests in a variety of applications, such as dynamic monitoring and adjusting image quality, optimizing algorithms and parameter settings of image processing systems, and benchmarking image processing system and algorithms. Earlier techniques were based on mathematical metrics like PSNR, MSE but they do not correlate well with subjective perception values. MSSIM is a human visual system based metric which uses the luminance, structural and contrast information present in the given image as like in HVS model. These validation results show the robustness, feasibility of the MSSIM and it can perform better than PSNR and SNR.

Reyadh Naoum, Ahmed Shihab, Sadeq AlHamouz [5] proposed a novel image steganography system, which embeds (RGB) secret image within (RGB) cover image chosen by an enhanced resilient back propagation neural network. Three main stages are included within the embedding phase, which are; best cover image selection and processing stage, secret image selection and processing stage and best embedding threshold selection stage respectively. Best cover image is performed using SOM and ERBP algorithms. Secret image is processed by separating it into color layers and DWT is then applied. The color layers are then converted to bit streams; modified FLFSR in turns will be used to encrypt these streams to get more secure system. ERBP is again used to select the best embedding threshold values. The extraction phase will be performed the stego image result from embedding process. The performance has been evaluated during embedding and extraction stages considering using several cover and secret images and considering several sizes. Experiments show that (PSNR) is improved efficiently.

The embedding phase is proceeded by three main stages: best cover image selection and processing stage, secret image selection and processing stage and best embedding threshold selection stage. The first step of extraction process is to separate the stego image into its color layers (R,G,B) and then each color layer will be processed separately to get the color layers of secret image, then these color layers will be combined together to get the full (RGB) recovered secret image and this is considered the first security layer of our proposed system. Then each color layer of stego image is decomposed into 4 level/ DWT to get the stego image sub bands that hide the secret image bit streams. Starting with the approximate sub band, where the secret key which consists of embedding threshold is extracted; seed value and secret image size that are embedded in the first three coefficients of approximate sub band coefficients vector. Each coefficient is compared with the extracted embedding threshold; if the coefficient is greater than the threshold, ignore it. If it is less or equal to threshold then convert it to binary number and extract the 4 Least Significant Bits.

3. Proposed Work

The proposed method is used in this thesis their block diagram and short summary of this system are used. The proposed method is used brief description are given below:

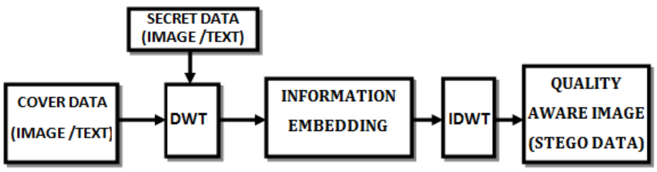

Figure 1: Sender Side

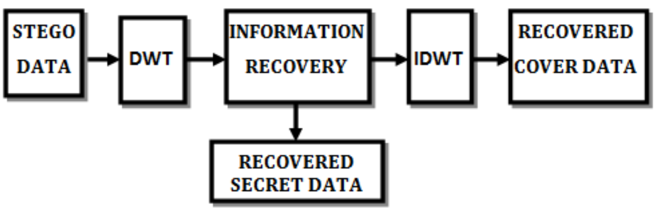

Figure 2: Receiver Side

The brief description of the sender side and receiver side of the image quality assessment is given below:

3.1 Cover / Secret Data

The term "cover" is used to describe the original innocent message, image. It is input of the sender side of the system. The term "secret" is used to describe the hidden innocent message, image. It is also input of the sender side of the system.

3.2 Discrete Wavelet Transform and its Inverse

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information (location in time).The various type of discrete wavelet transform is Haar wavelet, Daubechies wavelets, Symlets, Coiflets Biorthogonal wavelets, Reverse biorthogonal wavelets, Meyer wavelet, Discrete approximation of Meyer wavelet, Gaussian wavelets, Mexican hat wavelet, Morlet wavelet, Complex Gaussian wavelets, Shannon wavelets, Frequency Bspline wavelets, Complex Morlet wavelets. The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. In other words, this transform decomposes the signal into mutually orthogonal set of wavelets, which is the main difference from the continuous wavelet transform (CWT), or its implementation for the discrete time series sometimes called discrete time continuous wavelet transform (DTCWT).

The wavelet can be constructed from a scaling function which describes its scaling properties. The restriction that the scaling functions must be orthogonal to its discrete translations implies some mathematical conditions on them which are mentioned everywhere, e.g. the dilation equation

$$\phi(x) = \sum_{k=-\infty}^{\infty} a_k \phi(Sx - k)$$

Where S is a scaling factor (usually chosen as 2). Moreover, the area between the function must be normalized and scaling function must be orthogonal to its integer translations, i.e.

$$\int_{-\infty}^{\infty} \phi(x)\, \phi(x + l)\, \mathrm{d}x = \delta_{0,l}$$

After introducing some more conditions (as the restrictions above does not produce unique solution) we can obtain results of all these equations, i.e. the finite set of coefficients *ak* that define the scaling function and also the wavelet. The wavelet is obtained from the scaling function as N where N is an even integer. The set of wavelets then forms an orthonormal basis which we use to decompose the signal. Note that usually only few of the coefficients ak are nonzero, which simplifies the calculations.

3.2.1 One Level of the Transform:

The DWT of a signal is calculated by passing it through a series of filters. First the samples are passed through a low pass filter with impulse response resulting in a convolution of the two:

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k]$$

The signal is also decomposed simultaneously using a high pass filter h. The outputs giving the detail coefficients (from the high pass filter) and approximation coefficients (from the low pass). It is important that the two filters are related to each other and they are known as a quadrature mirror filter. However, since half the frequencies of the signal have now been removed, half the samples can be discarded according to Nyquist's rule. The filter outputs are then subsampled by 2 (Mallat's and the common notation is the opposite, g-high pass and h-low pass):

$$y_{\mathrm{low}}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k]$$
$$y_{\mathrm{high}}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n-k]$$

This decomposition has halved the time resolution since only half of each filter output characterizes the signal. However, each output has half the frequency band of the input so the frequency resolution has been doubled.

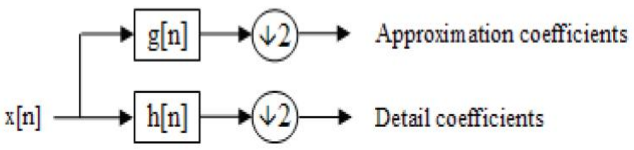

Figure 3: Block diagram of one level transformation

With the subsampling operator ↓

$$(y \downarrow k)[n] = y[kn]$$

The above summation can be written more concisely.

$$y_{\mathrm{low}} = (x * g) \downarrow 2$$
$$y_{\mathrm{high}} = (x * h) \downarrow 2$$

However computing a complete convolution $x * g$ with subsequent downsampling would waste computation time. The Lifting scheme is an optimization where these two computations are interleaved.

3.2.2 Two Level of the Transformation:

This decomposition is repeated to further increase the frequency resolution and the approximation coefficients decomposed with high and low pass filters and then downsampled. This is represented as a binary tree with nodes representing a subspace with a different time frequency localisation. The tree is known as a filter bank.

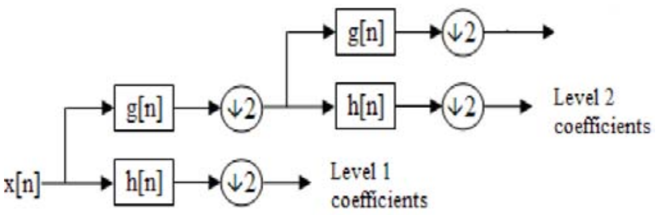

Figure 4: Block diagram of two level transformations

At each level in the above diagram the signal is decomposed into low and high frequencies. Due to the decomposition process the input signal must be a multiple of 2^n where n is the number of levels.

3.2.3 Haar-Dwt

The first DWT was invented by Hungarian mathematician Alfred Haar. For an input represented by a list of 2^n numbers, the Haar wavelet transform may be considered to pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale, which leads to $2^n - 1$ differences and a final sum. Two dimensional DWT (2D-DWT) converts the image into Low frequency and High frequency coefficients. Four bands are obtained from the 2D-DWT. They are LL1 (Approximation coefficients), LH1 (Horizontal coefficients), HL1 (Vertical coefficients), and HH1 (Diagonal coefficients) as shown in Figure 2.3. Figure 2.4 shows an example of decomposition for an image.

The Wavelet transform can be used for steganography to achieve high capacity and robustness. The Haar Wavelet Transform is the simplest of all the wavelet transforms. In this, the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The LL band is called as approximation band, which consists of low frequency wavelet coefficients, and contains significant part of the spatial domain image.

The whole procedure described above is called the first-order 2-D Haar-DWT. The first-order 2-D Haar-DWT applied on the image "Lena" is illustrated in Figure 6.

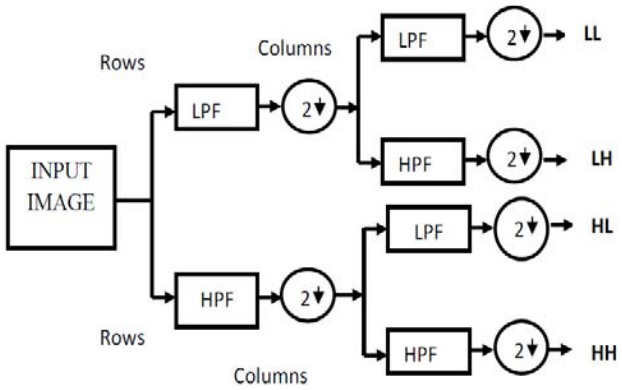

Figure 5: Decomposition of an image using DWT

(a)

(b)

Figure 6: (a) Original image-Lena, (b) Result after the first-order 2-D Haar-DWT

3.3. Information Embedding / Recovery

Least significant bit insertion is a common, simple approach to embed information in a cover file. The LSB is the lowest order bit in a binary value. This is an important concept in computer data storage and programming that applies to the order in which data are organized, stored or transmitted. Usually, three bits from each pixel can be stored to hide an image in the LSBs of each byte of a 24-bit image. Consequently, LSB requires that only half of the bits in an image be changed when data can be hidden in least and second least significant bits and yet the resulting stego-image which will be displayed is indistinguishable to the cover image to the human visual system.

In one byte, the 1 bit LSB is indicated:

1	0	0	1	0	0	0	1

Figure 7: Least Significant Bit

The last bit of the byte is selected as the least significant bit (as illustrated in Figure 6.5) because of the impact of the bit to the minimum degradation of images. The last bit is also known as right-most bit, due to the convention in positional notation of writing less significant digit further to the right.

In bit addition, the least significant bit has the useful property of changing rapidly if the number changes slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). The one bit addition is done as shown in Fig 8
(1 Bit Addition 1+2=3)

i) Value inserted

0	0	0	0	0	0	0	1

ii) Original Value

0	0	0	0	0	0	1	1

iii) Final modified Value

0	0	0	0	0	1	0	0

Figure 8: Example of bit addition

Basically, by modifying the insignificant bits, the cover image is typically altered in a nearly imperceptible manner thereby ensuring that any observer would be unaware of the alteration made. Employing the LSB technique for data hiding achieves both invisibility and reasonably high storage payload, a maximum of one bit per pixel (bpp) for gray scale and three bpp for Red-Green- Blue (RGB) images.

3.4 Stego Data

The "stego" data is the data containing both the cover image and the "embedded" information. The input of the system is cover data in the form of image or text and secret data in the form of image or text. Containing of the both data they produced stego data.

Algorithm to embed the text message:-
Step 1: Read the cover image and the text message which is to be hidden in the cover image.
Step 2: Convert the text message in binary format. Apply 2D-Haar transform on the cover image.
Step 3: Obtain horizontal and vertical filtering coefficients of the cover image and the cover image is then added with data bits for DWT coefficients.
Step 4: Calculate the LSB of each pixel of the cover image.
Step 5: Replace the cover image of the LSB with each bit of secret message one by one.
Step 6: Obtain stego image
Step 7: Calculate the Mean square Error (MSE) and the Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Obtain horizontal and vertical filtering coefficients of the cover image and then extract the message bit by bit and recomposing the cover image.
Step 3: Calculate LSB of each pixels of stego image.
Step 4: Retrieve bits and convert each 8 bit into character.

4. Result and Discussion

The embedding and extraction process and also evaluation of the quality of image in the MATLAB. Code is developed for opening GUI for this implementation. After the developed a code for the loading the input image and message file in the MATLAB. Then code is developed for secret image and then applies discrete wavelet transform of the cover image, for the four sub-bands which separate the high and low frequency information. Code is developed for LSB using discrete wavelet transform. Apply both LSB methods to embedded secret data in cover data. Then apply the Inverse Discrete Wavelet Transformation (IDWT) so that can get the stego-image.

The extraction process is the code for the loading the input stego-image and cover image or message text file in the

MATLAB. Then apply discrete wavelet transform on input of the stego data and cover data. Extraction process of the first check of the 8 bit, it is equal then displayed the recovered secret data and it is not equal then process is repeated. In recovered secret data apply Inverse Discrete Wavelet Transformation (IDWT) so that can get the recovered covered data. After the code is developed for the analysis of results obtained using various parameters like MSE, RMSE, SNR, PSNR and correlation.

The code developed for opening GUI in the MATLAB for this implementation. There are two push button for input of the load cover and secret data it is form of image or text. There are used two panels. One is Formation panel include in wavelet transformation, embedding and inverse wavelet transformation. Second is recovery panel including in wavelet transformation and extraction. Then secret data and recovered secret data analyzed performance parameter is MSE, RMSE, SNR, PSNR and correlation. Finally exit button is used exit the program.

4.1 Evaluation of Image Quality

For comparing the stego image with cover results it requires a measure of image quality and the commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio.

4.2 Mean-Squared Error

The mean-squared errors (MSE) between two images are I1 (m, n) and I2 (m, n) is:

MSE = ∑ [I1 (m, n) – I2 (m, n)] ^{2} ÷ M * N

In the above formula M and N are the number of rows and columns in a input images, respectively.

4.3 Root Mean-Square-Error:

The Root Mean Square Error (RMSE) firstly calculated MSE then square root of the MSE.

RMSE = $\sqrt{\sum [I1 (m, n) - I2 (m, n)]^2 \div M * N}$

4.4 Signal –To-Noise Ratio:

Signal-to-noise ratio is defined as the ratio of the power of a signal (meaningful information) and the power background noise (unwanted signal):

$$SNR = P_{(signal)} / P_{(noise)}$$

Where P is average power, both signal and noise must be measured at the same or equivalent point in a system.

4.5 Peak Signal-To-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) will help to avoid this problem by scaling the MSE according to the given image range:

$$PSNR = 10\log 10\,(256^2 \div MSE)$$

PSNR is measured in decibels (dB) and it is a good measure for comparing restoration results for the same image.

4.6 Correlation

If we have a series of n measurements of *X* and *Y* written as *xi* and *yi* where i = 1, 2… n, then the sample correlation coefficient can be used to estimate the population Pearson correlation *r* between *X* and *Y*. The sample correlation coefficient is written:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{(n-1)s_x s_y} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}},$$

Where $\bar{x}$ and $\bar{y}$ are the sample means of *X* and *Y*, and *sx* and *sy* are the sample standard deviations of X and Y.

4.7 Performance Parameter Table

The various images evaluate the parameter values in the MATLAB code. The separate parameter verses no. of images graph is shown below and also performance table is given below:

Performance parameter table observe that various images evaluated in GUI Matlab code embedding and extraction function. Observe the MSE is low and PSNR is greater. The correlation observed in table approximately 1. The RMSE is also low

Table 1: Performance Parameter Table: Cover Data as color Image and Secrete Data as Text

No. of Images	No. of performance parameter				
	MSE	RMSE	PSNR	Correlation	SNR
1. Girl	0.1192	0.1597	79.9947	1.0000	Inf
2. Lena	0.1015	0.1534	80.6926	1.0000	Inf
3. sailboat	0.0968	0.1517	80.8965	1.0000	Inf
4. Baboon	0.1145	0.1582	80.1678	1.0000	Inf
5. Pepper	0.0875	0.1479	81.3355	1.0000	Inf
6. Airplane	0.0754	0.1425	81.9820	1.0000	Inf
7. Boat	0.1052	0.1548	80.5360	1.0000	Inf

Table 2: Performance Parameter Table: Cover Data as Grayscale Image and Secrete Data as Text

No. of Images	No. of performance parameter				
	MSE	RMSE	PSNR	Correlation	SNR
1.Cameraman	0.1173	0.1591	80.0631	1.0000	40.0129
2. Airfield2	0.1425	0.1670	79.2199	1.0000	38.8751
3. Kiel	0.0012	0.1851	77.4307	1.0000	38.6995
4. Lena Test 2	0.1620	0.1725	78.6613	1.0000	39.0892
5. Flintstone	0.1732	0.1754	78.3717	1.0000	39.2973

Table 3: Performance Parameter Table: Cover Data as Color Image and Secrete Data as color or Grayscale Image

No. of Images		No. of performance parameter				
Cover Data	Secret Data	MSE	RMSE	PSNR	Correlation	SNR
1. Baboon	Barbara (color)	0.0406	0.4489	62.0452	1.0000	Inf
2.Goldhill	Houses (gray scale)	0.0420	0.4526	61.9007	1.0000	Inf
3. Airplane	Boats (color)	0.0384	0.4427	62.2850	1.0000	Inf
4. Flowers	Fingerprint (grayscale)	0.0277	0.4078	63.7110	1.0000	Inf
5. Pepper	Fruits (color)	0.0382	0.4422	62.3052	1.0000	Inf

Table 4: Performance Parameter Table: Cover Data as Grayscale Image and Secrete Data as color or Grayscale Image

No. of Images		No. of performance parameter				
Cover Data	Secret Data	MSE	RMSE	PSNR	Correlation	SNR
1.Camera--man	Moon (color)	0.0955	0.5559	58.3295	1.0000	29.8675
2. Man	Lighthouse (gray scale)	0.1218	0.5908	57.2739	1.0000	28.9503
3. Girlface	Houses (grayscale)	0.1272	0.5973	57.0845	1.0000	28.9213
4. Clown	Lighthouse (color)	0.1185	0.5868	57.3925	1.0000	28.6637
5. Couple	Finger (grayscale)	0.1276	0.5977	57.0720	0.9999	29.4658

4.3 Comparison Parameter Table

The comparison parameter table observes the previous work values of the parameter and proposed work values are given below:

Table 5: Comparison Table

Performance parameter	Reference No.		Proposed work
	[14]	[15]	
MSE	4.617	-	0.0754
RMSE	-	-	0.1425
PSNR	41.55	49.5629	81.9820
Correlation	-	0.9999	1.0000
SNR	-	-	Inf

The proposed work is best result as compare to previous work result. Shown in above Comparison parameter table and best result MSE is 0.0754, RMSE is 0.1425, PSNR is 81.9820, correlation is 1 and SNR is infinite.

5. Conclusion and Future Work

In this paper is the embedding function applies on cover data and secret data. Cover data and secret data are the input of the system. Embedding function using least significant bit on input is forming either image or text. They produced stego data in the form of image. The extraction function evaluated. The extraction function on the input cover data and stego data discrete wavelet transform. Then apply inverse discrete wavelet transform they produced recovered secret data. Then evaluated the performance parameter is observed through various self-developed image processing algorithms in Matlab. The implement and perform comparative analysis on LSB and DWT algorithm. The parameters like PSNR, MSE, RMSE, and Correlation on the different images and the results are evaluated to check best quality of Images having high PSNR ratio, less MSE, less RMSE and correlation is 1. Future work will focus on diversifying the various types of cover-medium and to increase the PSNR and less MSE using other alternative methods. To explore and discover more options for users in the selection of cover mediums as well as ways to embed more secret data. Besides, also like to focus on the information hiding method and authentication method.

References

[1] Mohit Kalra, D. Ghosh "Image Compression Using Wavelet Based Compressed Sensing and Vector Quantization" ICSP2012 Proceedings 978-1-4673-2197-6/12/$31.00 ©2012 IEEE.

[2] Lip Yee Por, Delina Beh, Tan Fong Ang and Sim Ying Ong "An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm" The International Arab Journal of Information Technology, Vol. 10, No. 1, January 2013.

[3] Preeti Chaturvedi, R. K. Bairwa "Image Steganography Method for Hiding Secret Message in Colored Images by Using IWT" International Journal of Recent Research and Review, Vol. VI, Issue 3, December 2013.

[4] Anu, Komal, Shipra Khurana, Amit Kumar "Comparative Analysis of Image Quality Assessment Using HVS Model "International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 7, July 2014.

[5] Reyadh Naoum, Ahmed Shihab, Sadeq AlHamouz " Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation" IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.1, January 2015.

[6] Geeta D. Rote1, Dr. A. M. Patil2 **"**Steganography with Cryptography Technique For Data Hiding" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013).

[7] Nisha, Sunil Kumar **"**Image Quality Assessment Techniques" Volume 3, Issue 7, July 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[8] Gauresh Vanjare, Saylee Gharge "Performance Evaluation of LSB Substitution and DWT Method for Steganography" Volume 5, Issue 3, March 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[9] Zhou Wang, Member, IEEE, Guixing Wu, Hamid Rahim Sheikh, "Quality-Aware Images" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 6, JUNE 2006.

[10] K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, "Hiding secret message in edges of the image," in Proc. Int. Conf. Information and Communication Technology, pp. 238–241,2007.

[11] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–497, 2008.

[12] Por L-Y., Wong K-S., and Chee K-O., "UniSpaCh: A Textbased Data Hiding Method Using Unicode Space Characters" *Journal of Systems and Software*, vol. 85, no. 5, pp. 1075- 1082, 2012.

[13] Yee P-L, and Kiah M-L-M, "Shoulder Surfing Resistance Using Penup Event and Neighbouring Connectivity Manipulation," *Malaysian Journal of Computer Science*, vol. 23, no. 2, pp. 121-140, 2010.

[14] Avinash K. Gulve and Madhuri S. Joshi "A High Capacity Secured Image Steganography Method with Five Pixel Pair Differencing and LSB Substitution" *I.J. Image, Graphics and Signal Processing*, 2015, 5, 66-74.

[15] Parul, Manju, Dr. Harish Rohi "Optimized Image Steganography using Discrete Wavelet Transform (DWT)" International Journal of Recent Development in Engineering and Technology Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 2, February 2014).

Author Profile

Duleshwari Gajanan Wankhade received the B.E. degree in Electronics and Telecommunication Engineering from Sant Gadge Baba Amravati University in 2014.