Optimal Data Embedding in Image Steganography Using CWT and LSB Masking Technique

[1]Sakshi Jindal,[2] Er. Navdeep Kaur
[1]Department of Electronics and Communication Engineering GZSCCET Bathinda(India)
[2] Department of Electronics and Communication Engineering GZSCCET Bathinda(India)

***Abstract* -In today's world of Internet every digitized object can be made exchangeable and transferable over the communication channel for various purposes. There are numerous security threats over the internet for digitized objects and hence they have to be made secure. Therefore, methods like steganography are gaining importance day by day. Steganography is the art which tends to obscure a part of information or useful data into another. Steganography can be applied on different file formats like audio, video, text and image. In image steganography data can be hidden in two domains namely Spatial and Transform domains. This paper proposes a technique for hiding image into another image using Continous Wavelet Transform (CWT) Method which helps in converting the data into higher and lower frequency components and also the LSB method for converting those components into bit stream and hiding the data in the last three bits of the covered medium. At the destination side the hidden data is recovered using Inverse Continous Wavelet Transform. Experimental results show a better PSNR value and lower MSE with increased capacity and security.**

***Index Terms* - Steganography, Spatial and Transform Domains, CWT, LSB, PSNR and MSE**

I. INTRODUCTION

Due to advancement in digital communication and networking , the threats towards the transfer of information from one destination to another are increasing .This has resulted in significant rise in interest of information hiding researchers to develop a method that would not only encrypt the message but also conceal its existence. [2] The related approaches such as cryptography and watermarking make the information unintelligible but do not offer a covert communication. Therefore steganography came into existence. The ultimate objectives of steganography are robustness, undetectability and high capacity.[17] Also the hidden message can be recovered by using appropriate method without any knowledge about the original cover medium.[7] Type of steganography include:

- Medium Based Steganography
- Domain Based Steganography

Further these two types of steganography can be classified as:

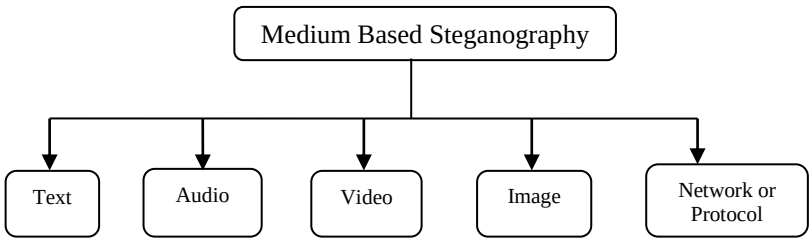


FIGURE1. CLASSIFICATION OF STEGANOGRAPHY

1.1 Text Steganography: It involves hiding of information inside the text files. In this method secret message is hidden behind every n^{th} letter of every word of text message. Number of methods available for hiding data in text file are Format Based Methods, Random and Statistical Methods, Linguistics Methods[17].

1.2 Audio Steganography: It involves hiding the data in audio files. This method hides the data in WAV (Windows Wave) and MP3 (Moving Picture Experts Group Layer-3)sound files. There are different methods for audio steganography such as parity coding and echo coding.

1.3 Video Steganography: It is a technique for hiding data into digital video format. Video comprises of a collection of pictures which are used as carrier for hiding the data. This type of steganography overcomes the capacity issues because video consists of a number of frames.

1.4 Protocol Stegaography: This type of stegaography uses TCP/IP, UDP, ICMP as cover object for hiding the data. It is the message embedding technique in which message is hidden within the network protocols for the messages used on the transmission networks[17].

Image Steganography: Hiding the secret data by taking image as an cover object is known as image steganography. In this steganography the pixel intensities are used to hide the data. In digital steganography images are widely used for the steganographic purpose because there are a number of bits available for hiding the secret message and also the transformations help to achieve the same. There are two types of image steganographic techniques namely Spatial and Transform Domain methods. Spatial Domain involve the direct changes in the bits of the cover image whereas Transform domain involves converting the image components into higher and lower frequency components. This paper deals with Image Steganography in Spatial and Frequency Domains.

DOMAIN BASED STEGANOGRAPHY:

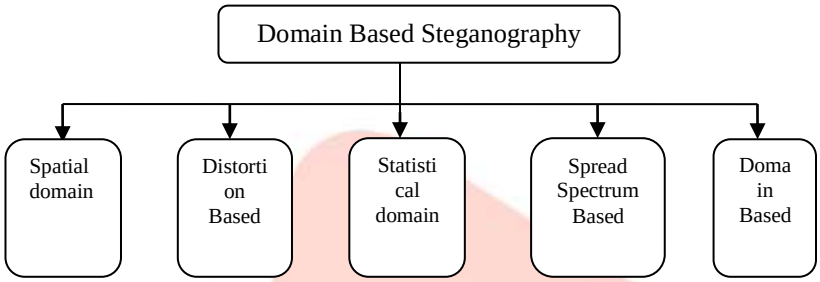


FIGURE 2: Domain Based Steganography

1. Spatial Domain Based Steganography:

In this technique the gray level of pixels and their color values are directly used for encoding the message bits. This technique is the simplest technique in terms of extracting and embedding the message bits. The most common algorithm belonging to this class of techniques is the Least Significant Bits (LSB) technique in which the least significant bit representation of the pixel gray levels is used to represent the message bits [1]. The techniques under LSB are discussed below:

- **Least Significant Bit Replacement:** LSB replacement takes the advantage of human eye [1]. An image consists of many pixels and each pixel can be expressed by a number between 0 to 255, in fact it can be represented by 8 bits. It has been noticed that the LSB of a pixel contains no visual information and human eye never realizes a modification in this bit. The information bit is simply overwritten on the LSB i.e. the first bit plane [4].

- **Least Significant Bit Matching**. In LSBM, if the secret bit is not equal to the LSB of the given pixel then ±1 is added arbitrarily to the pixel while keeping the changed pixel value in the range of [0,255]. Using Pseudo Random Number Generator secret bits are scattered on the cover. In LSBM the possibility of increasing and decreasing for each altered pixel is same and so the irregular artifacts introduced by LSB replacement is avoided [3].

- **Least Significant Bit Matching Revisited:** LSB matching revisited (LSBMR) uses a pair of pixels as an embedding unit in which the LSB of the first pixel carry one bit message and the connection (odd - even combination) of the two successive pixels carries another bit of message. The modification rate of pixels is decreased from 0.5 to 0.375 bits/pixel. This can evade the LSB replacement unevenness and make the recognition a little more difficult than the LSBM approaches [7].

- **LSB Masking:** Masking is a technique that can be used on both color and gray-scale images. It changes the visible properties of an image by masking secret data over the original data by changing luminance of the particular areas. [11]Masking and filtering are similar to introducing watermarks on a printed image. Masking is more vigorous than LSB insertion with respect to compression, cropping, and some image processing techniques.

2. Distortion Based Steganography: These techniques require the knowledge of the original cover in the decoding process. The sender applies a series of modifications to cover object in order to get the stego object. The sequence of modifications to corresponds to a specific secret message the sender wants to transmit. The receiver measures the differences to the original cover

in order to rebuild the sequence of modifications which corresponds to the secret message. The drawback of this system is that the receiver must have access to the original covers.

3. Statistical Domain Based Steganography: Statistical method is also called as "1-bit" Steganography. This method embeds one bit of information in a digital carrier. This is achieved by modifying the cover in such a way that certain statistical characteristics change significantly if '1' is transmitted and if the cover is left unaltered then it indicates as '0'. The receiver must be able to differentiate between modified and unmodified covers in order to receive the secret message.

4. Spread Spectrum Technique: In this method the secret data is spread over a wide range of frequencies. The signal to noise ratio in every frequency band must be small so that it becomes difficult to detect the presence of data. Even if parts are removed from several bands, there would be still enough information present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover. It is very robust technique mostly used in military communication.

5. Transform Domain Technique: In this technique, the secret message is embedded frequency domain of the cover. This is the more complex way of hiding message in an image .Different algorithms and transformations are used on the image to hide the message in it [15]. Transform domain are broadly classified as:

- Discrete Fourier Transform Technique
- Discrete Cosine Transform Technique
- Continous Wavelet Transform Technique
- Discrete Wavelet Transform Technique

Continous Wavelet Transform technique among the above mentioned techniques is an effective technique for hiding the information using wavelet transform. This Transformation involves Scaling which either dilates (expands) or compresses a signal. Large scales (low frequencies) dilate the signal and provide detailed information burried in the signal, while small scales (high frequencies) compress the signal and provide overall information about the signal. The Wavelet Transform performs the convolution operation and the basis function of the signal. The CWT becomes very useful as in most practical applications, as high frequencies (low scales) do not last for a long duration of the signal and appear as short bursts, while low frequencies (high scales) usually last for entire duration of the signal.

II. RELATED WORK

Chin-Chen Chang et al. [1] proposed that LSB substitution is the most commonly used method straightforwardly replacing the LSBs of pixels in the cover image with secret bits to get the stego-image. LSB substitution algorithm is the simplest method to hide message in a host image. It replaces the least significant bit (LSB) of each pixel with the encrypted message bit stream. Authenticated receivers can remove the message by deciphering the LSB of every pixel of the host image with a pre-shared key. Since only the least significant bit of pixels is changed, it is visually imperceptible by human. The capacity of the algorithm is 1 bit per pixel.

Chin-Chen Chang et al. [2] analysed an optimal least-significant-bit substitution method in image hiding using the dynamic programming strategy. The method significantly reduces the computation time and also achieves optimal solution.

Andrew D. Ker et al. [3] suggested a number of improved methods for deciding whether a grayscale bitmap contains LSB steganography or not. The aim was to reduce false positive and the new statistics allow reliable detection between 2 and 6 times less embedded data.

J. Mielikainen et al. [4] explained a new method that used the choice to set a binary function of two cover pixels to the desired value. The embedding was performed using a pair of pixels as a unit, where the LSB of the first pixel conceded one bit of information, and a function of the two pixel values carried a new bit of information. Therefore, the adaptive method allows embedding the same payload as LSB matching but with fewer changes to the cover image. The method offered less distortion and high resistance against steganalysis.

Cheng-Hsing Yang et al. [5] proposed a new adaptive least-significant-bit (LSB) steganographic method using pixel-value differencing (PVD) that provided a larger embedding capacity and unnoticeable stego images. The method exploited the

difference value of two consecutive pixels to approximate how many secret bits will be embedded into the two pixels. The proposed approach provided both larger embedding capacity and higher image quality.

Xiaolong Li et al.[6] suggested the generalized LSB matching (G-LSB-M) scheme, which generalized the method and LSB matching. The lower bound of Expected Number of Modification Per Pixel (ENMPP) for G-LSB-M was investigated, and a construction of G-LSB-M was presented by using the sum and difference covering set of finite cyclic group. The proposed method was highly secure and offered high resistance.

W. Luo et al. [7] worked on the problem of identical embedding at all parts of an image irrespective of size of secret message and proposed LSB matching revisited. This edge adaptive system can decide the embedding regions according to the size of secret message and the dissimilarity between two successive pixels in the cover image. For minor embedding rates, only sharper edge regions are used while maintaining the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. This scheme enhanced the security significantly.

Xin Liao et al. [8] analyzed four-pixel differencing and modified LSB substitution to improve quality. Secret data are concealed into each pixel by the k-bit modified LSB substitution method, where k is determined by the average difference value of a four-pixel block. Readjustment has been executed to extort the secret data exactly and to minimize the perceptual alteration but it compromised resistance to attacks for achieving quality.

Shamim Ahmed Laskar et al. [9] proposed a method in which a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using LSB insertion method. The mixture of the two methods cryptography and steganography improved the security of the data embedded. This combinational methodology contented the requirements such as capacity, security and robustness for secure data broadcast over an open channel.

Chao Wang et al. [10] proposed a method to raise the embedding speed of Matrix embedding by extending the matrix via some referential columns. Compared with the original matrix embedding, the proposed method can exponentially reduce the computational difficulty for identical increment of embedding efficiency. The proposed method achieves higher embedding speed and efficiency than previous fast matrix embedding methods.

J. K. Mandal et al.[11] explained a transformed domain based gray scale image authentication/data hiding technique using Z transform (ZT) termed as FDSZT. Z Transform is practiced on 2×2 masks of the source image in row major order to transform original sub image (cover image) block to its equivalent frequency domain. One bit of the hidden image is embedded in each mask of the source image onto the fourth LSB of transformed coefficient based on median value of the mask. The method offered high PSNR.

Manisha Boora et al. [12] proposed a scheme for hiding a larger size secret-image into smaller size cover- image. Arnold Transformation is performed to acquire scrambled secret image. DWT is performed on both cover image and secret image and this is followed by alpha blending process. This proposed algorithm is highly secured with good perceptual invisibility.

N Sathisha et al. [13] suggested Non Embedding Steganography using Average Technique in Transform domain (NESATT). The Lifting Wavelet Transform (LWT) is practical on both cover image and payload image. The Diagonal band (CD) of cover image and Approximation band (PA) of payload are segmented into N x N blocks. The PA band of payload is divided by CD to create resultant matrix based on Non Embedding Threshold Value (NETV) set by key. The average value of resultant matrix is calculated and used to split PA to generate modified CD. The capacity and PSNR values were high in the case of proposed algorithm.

Ashish Chawla et al. [14] proposed a modified secure and high capacity based steganography system of hiding a large-size secret image into a small-size cover image. Matrix Rotation is performed to scramble the secret image. Discrete Wavelet Transform (DWT) is performed in both images and followed by Alpha blending operation. Then the Inverse Discrete Wavelet Transformation (IDWT) is practiced to get the stego image. Proposed algorithm for modified steganography is exceedingly secured with assured strength in addition to good perceptual invisibility.

A.Antony Judice et al. [15] explained a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel

adjustment (OPA) algorithm. The proposed system offered high hiding rates with evenhanded imperceptibility compared to other steganographic system.

G.Prabhakaran et al. [16] proposed an Adaptive Image Steganography utilizing Image denoising algorithm by wavelet thresholding. Adaptive Steganography is a special case of both Spatial and Transform domain techniques. At first Arnold Transformation is done to scramble the secret message then both cover and secret message are decomposed using Integer wavelet transform. The proposed method improved the capacity, Peak Signal to Noise Ratio (PSNR) and provided high security and certain robustness**.**

Anamika Sharma et al. [17] suggested an image steganography scheme based on neural network fusion in wavelet transform domain. The cover and stego image were separated in its frequency coefficients components by wavelet transform domain, and neural network used as classifier**.** It offered satisfactory imperceptibility and robustness.

III. METHODOGY

A. **COVER IMAGE:** The cover image is the carrier of the message. Image file is most popularly used for this purpose because it is easy to send during the communication process and offer high capacity for the message to be embedded. The aim of steganography is to embed secret data into a cover in such a way that no one apart from the sender and intended recipients even realizes there is secret data. The cover image is firstly read in which another image is to be hidden.

B. **CONTINOUS WAVELET TRANSFORM:** In the proposed paper, continuous wavelet transform is applied using MATLAB. In the CWT, the analyzing function is a wavelet, 'ψ'. The CWT compares the signal to shifted and compressed or stretched versions of a wavelet. Stretching or compressing a function is collectively referred to as dilation or scaling and corresponds to the physical notion of scale. By comparing the signal to the wavelet at various scales and positions, obtain a function of two variables. The two-dimensional representation of a one-dimensional signal is redundant. If the wavelet is complex-valued, the CWT is a complex-valued function of scale and position. If the signal is real-valued, the CWT is a real-valued function of scale and position. For a scale parameter, a>0, and position, b, the CWT is:

$$C(a,b;\ f(t),\Psi(t)=\int_{-\infty}^{\infty} f(t)\frac{1}{\sqrt{a}}\Psi^{*}\ (t\text{-}b/a)dt$$

where * denotes the complex conjugate. Not only do the values of scale and position affect the CWT coefficients, the choice of wavelet also affects the values of the coefficients.

By continuously varying the values of the scale parameter, a, and the position parameter, b, the values of cwt coefficients C(a,b) are obtained.

C. **THRESHOLD CALCULATION USING EM ALGORITHM:** The choice of threshold calculation method is the main issue in Wavelet transformation methods. Generally threshold calculation is done by statistical means and it can be solved using Expectation Maximization Algorithm. The EM algorithm is used to find maximum likelihood parameters of a statistical model. These models involve latent variables in addition to unknown parameters and known data observations. That is, either there are missing values among the data, or the model can be formulated more simply by assuming the existence of additional unobserved data points.

One can simply select arbitrary values for one of the two sets of unknowns, use them to predict or estimate the second set, then use these new values to find a better estimate of the first set, and then keep alternating between the two until the resulting values both converge to fixed points. The statistical model generates a set of observed data, a set of unobserved latent data or missing values , and a vector of unknown parameters , along with a likelihood function , the maximum likelihood estimate (MLE) of the unknown parameters is determined by the marginal likelihood of the observed data.

The EM algorithm seeks to find the MLE of the marginal likelihood by iteratively applying the following two steps:

Expectation step (E step): Calculate the expected value of the log likelihood function, with respect to the conditional distribution of given under the current estimate of the parameters.

$$P(\text{model/data}) = \frac{P(\text{data/model})\ P(\text{model})}{P\ (\text{data})}$$

Maximization step (M step): Find the parameter that maximizes this quantity.

D. CONVERSION OF COEFFICIENTS INTO BIT STREAM: When the image has been converted into uint8 format by taking uint8 (Image), it already exists in ASCII format and after this we have reshaped the resulting matrix into a single row or column to get a byte stream using MATLAB.

E. EMBEDDING USING LSB MASKING: LSB based technique is most simple and straightforward approach in which message bits are embed in least significant bits of cover image. In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the secret message. The cover image and the secret message are converted from RGB to Gray Scale. New row size and column size are formed after converting them into bit stream. Masking can be achieved by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies. Here masking is done in last three bits of the cover image after converting it into 8-bit gray scale formation.

F. STEGO IMAGE: The image obtained after the above processes is called as stego image. The message is embedded into the intensity values of image obtained during image to gray scale conversion.This particular image consists of both cover and secret message.

IV. THE PROPOSED EMBEDDING METHOD

The fundamental concept of the proposed method is the embedding of the hidden information within noisy data of an image which originally spreads over cover image. Block Diagram of the proposed Steganography system is depicted in figure below. According to these figures the process of the embedding and extracting are described:

Algorithm for Embedding Process:

Input: Cover Image, Secret Image
Output: Stego Image

Step 1: Read the cover and the secret image.

Step2: Perform Continous Wavelet Transformation on both the images.

Step3:Threshold Calculation using Expectation Maximization Algorithm.

Step 4:Conversion of Image into Bit Stream.

Step5: Embedding of the image bits using LSB masking.

Step 6:Obtain the Stego Image.

EMBEDDING PROCESS:

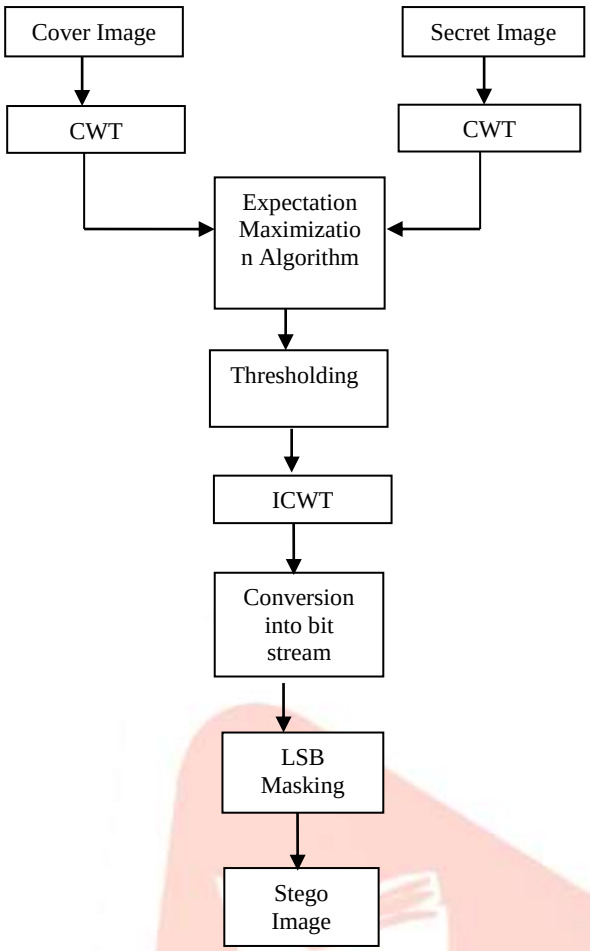


FIGURE3. Block Diagram of Proposed Method

Algorithm for Extraction Process:

- Input: Stego Image
- Output: Secret Image

Step1: Read the Stego Image.

Step 2: The coefficients of this image are calculated using Continous Wavelet Transform.

Step 3: Set the threshold using Expectation Maximization Algorithm.

Step 4: Perform Inverse Continous Wavelet Transformation .

Step 5: Secret Image Formation.

EXTRACTION PROCESS:

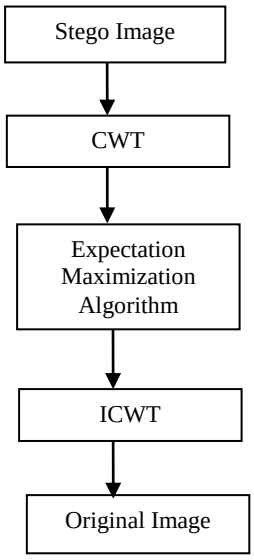
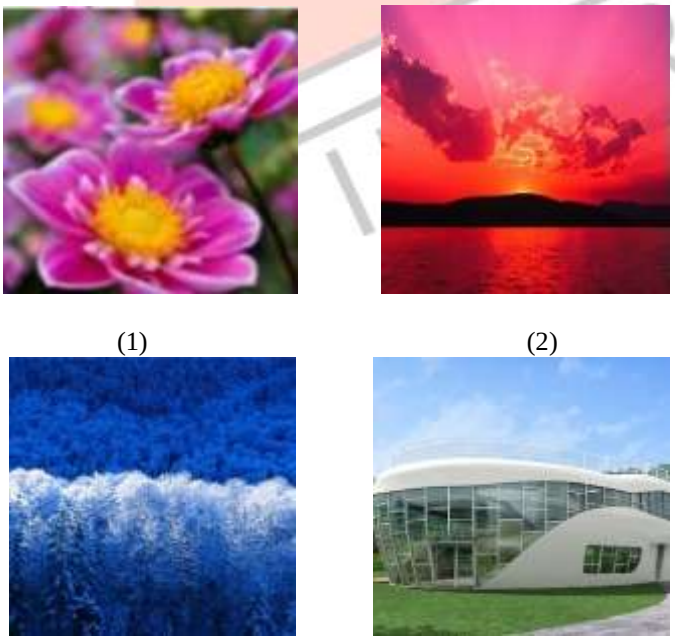


FIGURE 4. Block Diagram of Extraction Process

IV. RESULTS AND DISCUSSION

Images with different formats and different sizes are used to examine the performance of the proposed steganographic system. The original images shown in figure which are Lavender(300×300),Sunset(300×209),Winter(250×250),House(436×301), Tiger(320×240). In the following procedure the target image and the secret image are decomposed using Continous Wavelet Transform and converted into bit Stream. After this LSB masking has been used to hide the secret bits. The payload which are Apple of size(150×150) and Kid(251×201) alongwith target images are shown in Figure 5.Then Figure 6 shows the cover image, secret image and results after transformation and embedding.



(1) (2)

(3) (4)

(5)

(6)

(7)

Figure 5: Basic Test images for Steganography

(1) Lavender (2) Winter (3) Sunset (4) House (5) Tiger (6) Apple (7) Kid

(a)

(b)

(c)

FIGURE 6: Experimental results for CWT

(a) Cover Image (b) Secret Image (c) Stego Image

Table 1. Performance of proposed method for different cover and secret images.

Cover	Secret	MSE	PSNR
Lavender.png	Apple.jpg	0.92	48.49
Sunset.png	Apple.jpg	1.32	46.92
Winter.jpg	Apple.jpg	1.33	46.91
House.jpg	Kid.jpg	1.43	46.59
Tiger.jpg	Kid.jpg	2.45	44.26
Sunset.png	Kid.jpg	3.00	43.38

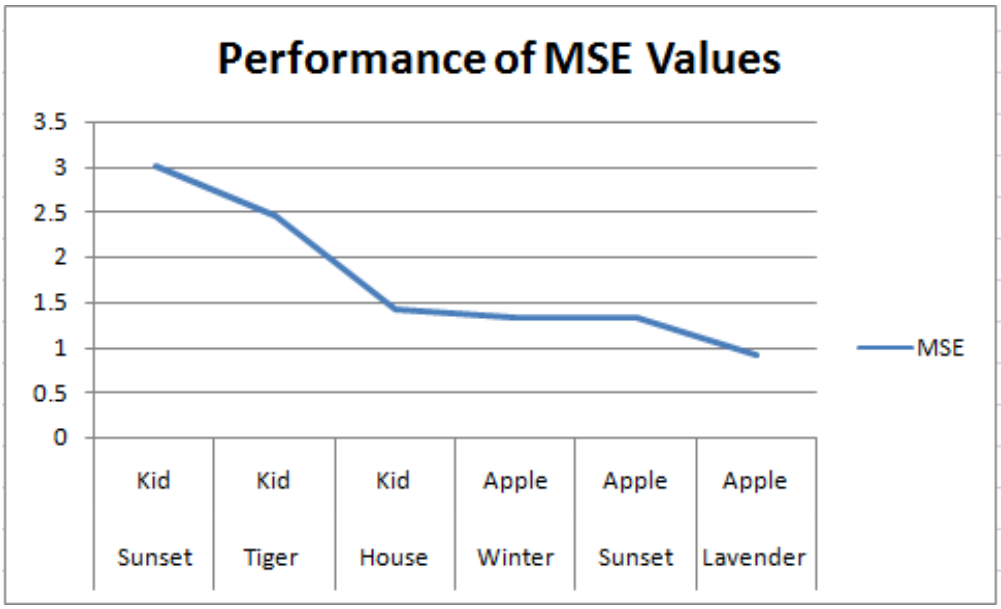


FIGURE7. The MSE vs Sample Image Set

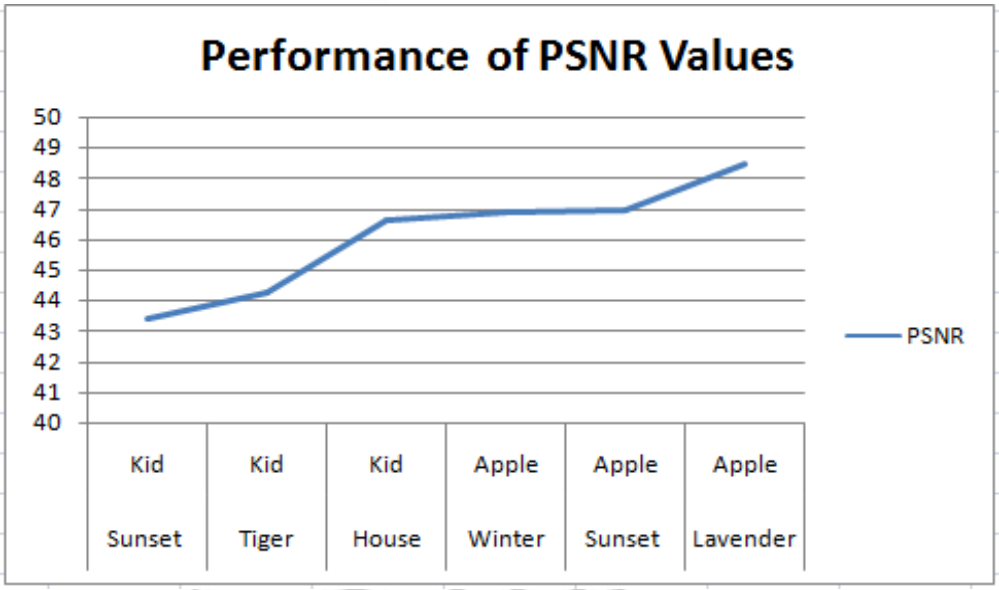


FIGURE8. The PSNR vs Sample Image Set

From Table1various Image Metrics like Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR). It illustrates that the value of MSE lies between 0.92 to 3 and PSNR between 43.38 to 48.49. The performance of PSNR values versus sample Image sets shown in the Line Graph. Figure5 and Figure6 shows the excellent performance ratio values in CWT and LSB.

V. CONCLUSION

The paper presents a new method for Steganography that utilizes 2-D Continous Wavelet Transform with Expectation Maximization Algorithm and LSB Masking Technique. The process provides a method for concealing digital data within a cover image by adjusting a threshold value from the EM algorithm. By applying a threshold from calculated detailed coefficients, embedding points are detected and filled by LSB bits. The methods exhibits high payload capacity with very little effects on statistical properties and improved values of PSNR and MSE.

VI. FUTURE SCOPE

As future extension the implementation of finding the threshold can be done by using Neural Networks in place of using Expectation Maximization Method.

REFERENCES

[1] Chin-Chen Chang et al., "A Fast And Secure Image Hiding Scheme Based on LSB Substitution", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 16, No. 4, pp. 399-416, 2002

[2] Chin-Chen Chang et al., "Finding Optimal Least-Significant-Bit Substitution in Image Hiding By Dynamic Programming Strategy", Pattern Recognition, Vol. 36, pp.1538-1595, 2003

[3] Andrew D. Ker, "Improved Detection of LSB Steganography in Grayscale Images", In Proc. 6th International Workshop. Toronto (Canada), Springer LNCS, Vol. 3200, pp. 97–115, 2004.

[4] Jarno Mielikainen , "LSB Matching Revisited", IEEE Signal Processing Letters, Vol. 13, No. 5, pp. 285-287,2006.

[5] Cheng-Hsing Yang et al., "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems". IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, pp. 488-497, 2008.

[6] Xiaolong Li et al., , "A Generalization of LSB Matching". IEEE Signal Processing Letters, Vol 16, No. 2, pp. 69-72, 2009.

[7] W. Luo et al., "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Trans. Inf. Forensics Security, Vol. 5, No. 2, pp.201 -214, 2010.

[8] X. Liao et al., "A Steganographic Method for Digital Images with Four-Pixel Differencing and Modified LSB substitution", Journal of Visual Communication and Image Representation, Vol. 22, No. 1, pp. 1−8, 2011.

[9] Shamim Ahmed Laskar and Kattamanchi Hemachandran , "High Capacity data hiding using LSB Steganography and Encryption" International Journal of Database Management Systems (IJDMS) Vol.4, No.6,pp.57-68, 2012.

[10] Chao Wang et al., "Fast Matrix Embedding by Matrix Extending", IEEE Transactions of Information Forensics and Security,Vol.7,No.1, pp.346-350, 2012.

[11] J.K Mandal et al., "A Novel Genetic Algorithm Based Data Embedding Technique in Frequency Domain using Z Transform(ANGAFDZT)", pp. 885-893, 2013.

[12] Manisha Boora and Monika Gambhir, " Arnold Transform Based Steganography", International Journal of Soft Computing and Engineering (IJSCE), Vol.3, No.4.pp.136-140, 2013.

[13] N Sathisha et al., "Non Embedding Steganography using Average Technique in Transform Domain", IEEE 9th International Colloquium on Signal Processing and its Applications ,Vol.8, No.10, pp.1-6, 2013.

[14] Ashish Chawla and Pranjal Shukla, "A Modified Secure Digital Image Steganography Based on Dwt Using Matrix Rotation Method", International Journal of Computer Science and Communication Engineering, Vol.2, No.2,pp.20-25, 2013.

[15] A.Antony Judice et al., "An Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform", International Journal of Computer Science and Network Security,Vol.14,No.7,pp.125-132, 2014.

[16] G.Prabakaran, R.Bhavani, M.Kiruthika, "Adaptive Image Steganography based on Denoising Methods in IWT", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.5.No.1,pp.567-574, 2015.

[17] Anamika Sharma and Ajay Kushwaha, "Image Steaganography Scheme Using in Wavelet Transform Domain" International Journal of Scientific Engineering and Research, Vol 3, No. 10, pp. 153-158, 2015.