A New Approach of Image Security System Based on LSB with IWT

J.Madheswari,
Department of Electrical and Electronics Engineering
JCT College of Engineering and Technology
Coimbatore,India
Jkmadheshwari@gmail.com
R.Mahalakshmi,
Department of Electrical and Electronics Engineering
Kumaraguru College of Technology
Coimbatore,India
mahacbe@gmail.com

***Abstract*—Today, the confidence of digital image transmission became a great substantial issue. Hence, security coverage is required to accomplish the secure image transmission.Steganography method has several advantages including high hiding capacity and undetectability. The secret content has been hidden into cover image using IWT method. It is difficult to detect the hidden information by Steganalyser since Stego Image and Cover image seems to be similar. The current work signifies a novel data hiding use Integer Wavelet Transform (IWT) through lifting scheme that aims to achieve high quality of stego image. This method transforms a spatial domain cover image into a frequency domain cover image. It hides the secret message into detail coefficients (CH, CV, CD) of IWT by construct a binary image in any of selected bit in CH, CV, and CD separately. The Planned approach enhances capacity, strength of image and Compare to existing method DWT, LSB, Contourlet Transform (CT), IWT provides better results in PSNR, SSIM, NCC, PCC value. This experiential result are executing by using MATLAB2013a.**

Keywords: Steganography, Frequency Domain, Spatial domain, Integer Wavelet Transform (IWT), DWT, LSB, Contourlet transform (CT).

I. INTRODUCTION

The word Steganography is formed by the two Greek words that are Stegano means "Hidden or Covered" and Grafia means "writing". The perception of steganography was first introduced with the example of prisoner's secret message by Simmons in 1983.

Steganography Method has to satisfy two basic requirements. The first requirement is perceptual transparency that is a cover object (The object containing any additional data) and second is stego object (The object containing secret messages) must be perceptually invisible. A steganography system is embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion.

Steganographic Terms:

- **Cover File**: It is a file in which hidden information will be stored.
- **Stego Medium:** Medium through which the information is hidden.
- **Message:** The data to be hidden or extracted.
- **Steganalysis:** Identify the existence of the message.

Classification of Steganography:

Steganography methods are classified into 1) Text 2) Image 3) Audio/Video 4) Protocol

Steganography technique is based on the two approaches that are spatial domain and frequency domain approach. In spatial domain approach secret message are embedded into least significant pixels of the cover image. They are fast but sensitive to image processing attacks. In frequency domain transforming the cover image into the frequency domain before embedding secret messages in it. The proposed system uses both transformations Least Significant Bit (LSB) with Integer Wavelet Transform (IWT).

II.LITERATURE REVIEW

Ashish Nimavat, Nitin Kanzariya K in 2014 [4] They design hybrid method is the grouping of spatial domain LSB method and frequency domain DCT method. The humble LSB method is not secure to provide the randomness this combination is used. Huffman coding is used for lossless secret image compression.

This is an online article and it is continuously updated. This link is the best source for the information and study about the various encryption algorithms, their working flow, algorithmic structure, etc. This link proved to be the major source behind my encryption algorithm studies. Chanu Y. J, have given a Survey on Image Steganography and Steganalysis [6].

Gary C.Kessler has written an Overview of Cryptography: Cryptographic [7]. This is an old published paper on cryptography by Gary C. Kessler, and since then it was continuously updated to date. It was last updated in 2014. The author uggested the great source for the cryptography algorithms again. It is very important to understand the encryption algorithm structure before putting it in the use.

A novel image steganography was projected in [10], it is based on integer wavelet transform [IWT], it is used to embed more than a few secret images and keys in color cover image. A quantization based steganography method presented.

Preeti Kumari and Ridhi Kapoor [11] in 2016 this paper author used the image compression, encryption, and image steganography to provide better image steganography. This method offers much security and invisible differences between the cover image and stego image. This combination unsecured powerful method that provides much security for stealthy communiqué.

In 2012 Nlanjan Dey [12] is used the frequency domain method to hide the multiple secret images. In this first, the color image is divided into 3 panels and the relate the DWT method to each panel and DCT method it is applied to HH band of the image.it gives the high robustness.

Vijaya Kumar Sharma [14] the proposed algorithm based on 8bit grayscale or 24bit color image, they used logical operation to ensure the security against stage analysis attack.

III.METHODOLOGY

The proposed model is work for hiding the secret image in the cover image. Arnold algorithm, which hides the secret image into the cover image. In this strategy, secret image is compression is done using LSB with IWT method to insert the data to produce the stego image. It provides the stego image more security and good robustness. This work proposes a stenographic technique for hiding images in a color image based on LSB with IWT.Individual planes are decomposed into sub-bands using LSB with IWT. Secret data are dispersed among the selected LSB with IWT coefficients using a private key. PSNR, MSE, NCC, IMQ, PCC, SIME and RMSE are major aspects in steganography.PSNR value is required high, but it depends on application to various field. When PSNR value is increased, correlation also increased, capacity is decreased and vice-versa.The researcher investigates a problem that is a proper combination of PSNR and correlation is required so that data can be sent through the safe channel without fear of third-party access. The effects in the steganography mainly are governed by on secret data. The larger value of the top-secret data; affect more to the value of stego image rather than a smaller value of secret data.

3.1 Algorithm

I. During the proposed embedding process both the cover image and the secret data by using the Arnold transform method investigator get encrypt image.
II. Apply LSB with IWT on encrypting image to get a stego image.

Algorithm for proposed embedding process:

1. Load the host RGB image.
2. Convert the RGB image to YC_bC_r color space and separate the Y, C_b, Cr components.
3. Choose the 'C_b' component and resize it to [1024, 1024], name it 'I'.
4. Read the secret image, make it a binary image and resize to [64, 64], name it 'W'.
5. Select 'k' as a key, and perform Arnold transform on the binary watermark 'k' times. We consider k = 100.
6. Key generation for security.
7. Perform 4 level 2-dimensional LSB with IWT on 'I'.
8. Apply SVD to HL4 sub-band. Its USV components are U_s, S_s, V_s. HL4 = U_s * S_s * V_sT
9. Apply SVD to the stego 'W'. Its USV components are U_w, S_w, V_w. W = U_w * S_w * V_w.
10. Modify the singular values additively, S = S_s + Ɣ * S_w
11. Set NEW_HL4 as, NEW_HL4 = U_s * S * V_sT
12. Apply 4 level inverse LSB with IWT,
13. Resize 'I' with original image size and rename it 'C_b '.
14. Concatenate Y, C_b, C_r component to get YC_bC_r image.
15. Convert the YC_bC_r image into RGB stego image.

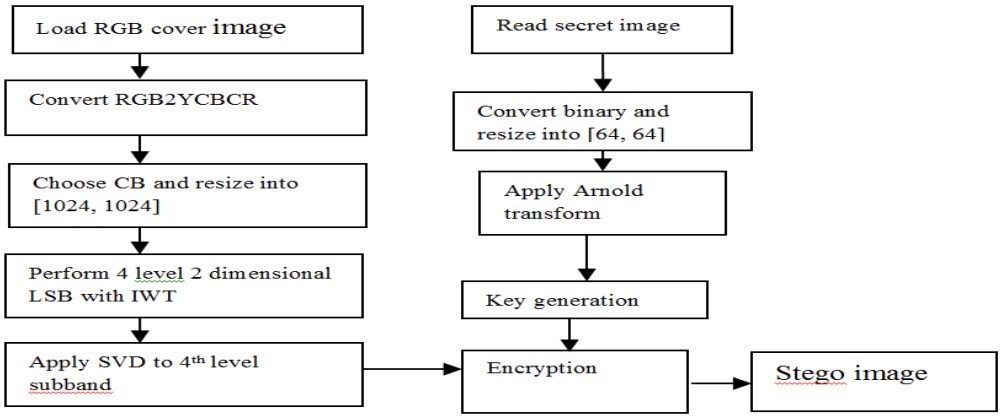


Figure1. Block Diagram of Embedding.

Extraction Algorithm:

1. Read stego image.
2. Convert RGB image into YC_bC_r color space and separate Y, C_b, C_r components.
3. 'C_b' component is resized to [1024, 1024] and rename it as 'I '.
4. Apply 4 level 2-dimensional LSB with IWT on 'I '.
5. Apply SVD to a sub band. Its USV components are U_1, S_1, and V_1. $HL_4 = U_1 * S_1 * V_1T$
6. Set S_new = $|S_1 - S\_s|$/ Į
7. Finally, NEW_ W = U_w *S_new * V_W_t.
8. Apply inverse Arnold transform on 'NEW_W' 'k' (key) times to get secret image W_1.
9. If given key is to match with the secret key, Convert gray scale image 'W_1' to the binary extracted secret image.
10. If it does not match means cover image should be displayed.

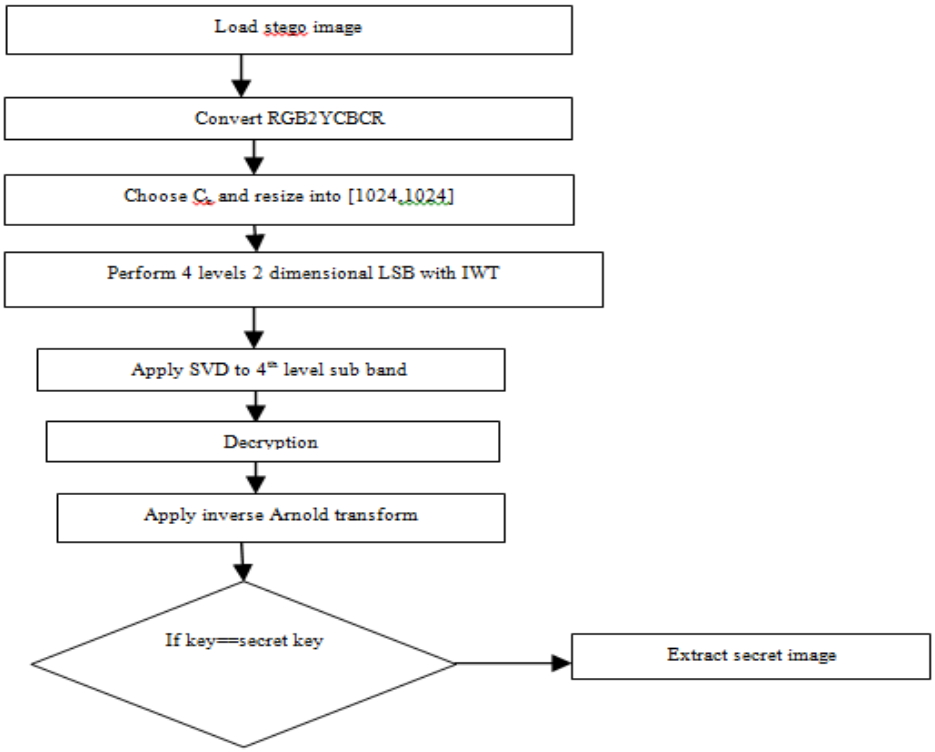


Figure 2. Block Diagram of Extraction.

3.2 Performance Parameter Evaluation

The value of statistical parameters not only preserves the image quality, a stronger robustness and refuge of an image to fight attacks. We used PSNR and MSE to measure the distortion between the original protection image and the stego image. The other Image statistical parameters are normalized cross-correlation, average difference, structural content, maximum difference, and normalized absolute error are taken into consideration.

3.2.1 Mean Square Error(MSE):

The distortion in the image can be measured using MSE and is calculated using Equation MSE can be defined as the measure of the average of the squares of the difference between the intensities of the stego image and the cover image. It is popularly used because of the mathematical tractability it offers. It is represented as follows:

$$MSE = \sum_{M,N} [I_1(X,Y) - I_Z(X,Y)]^2$$

Where,
I_1=Input secret image
I_Z=Extracted image
X=No. Of rows in image
Y=No. of columns in image

3.2.2. Peak Signal to Noise Ratio(PSNR)

It is the measure of the value of the image by comparing the concealment image with the stego image, i.e., it measures the statistical difference between the concealment and stego image. The PSNR depicts the measure of reconstruction of the transformed image. This metric is used for discriminating between the cover and stego image.The PSNR is a measure of distortion in the stego-image. Higher PSNR value means lesser distortion.

$$\text{PSNR} = \frac{10 \log_{10} R^2}{MSE}$$

In the previous equation, R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 255. If it has an 8-bit unsigned integer data type, R is1, etc.

3.2.2 Normalized Correlation Co-efficient

The Normalized Cross- Correlation (NCC) metric is the metric that is used to show the amount of deflection in the stego image with respect to the cover image after insertion of the message. Normalized Cross- Correlation (NCC) is applied to evaluate the performance of various existing methods which is given by the following equation,

$$\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(Xij * Yij)}{\sum_{i=1}^{N}\sum_{j=1}^{M}(Xij)^2} = NCC$$

Where,
Xij is the intensity of Pixel (i, j) in Cover Image. Yij is the intensity of pixel (i, j) in Stego Image

3.2.4 Image Quality Index(IQI)

The qualities of the stego-images are evaluated by using the universal image quality index (Q)

$$\frac{4\sigma_{xy}\,\bar{p}\,\bar{q}}{(\sigma_{x^2}+\sigma_{y^2})[(\bar{p})^2 + (\bar{q})^2]} = Q$$

Where,
$\bar{p}$ is the mean pixel value in the original image,
$\bar{q}$ is the mean pixel value in stego-image,
σ_{x^2} is the standard deviation for the original image,
σ_{y^2} is the standard deviation for stego-image and σ_{xy} is the covariance.

$$\bar{p} = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n} P_{ij}$$

$$\bar{q} = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n} Q_{ij}$$

$$\sigma_{x^2} = \frac{1}{m \times n-1}\sum_{i=1}^{m}\sum_{j=1}^{n} (p_{ij} - \bar{p})^2$$

$$\sigma_{y^2} = \frac{1}{m \times n-1}\sum_{i=1}^{m}\sum_{j=1}^{n} (q_{ij} - \bar{q})^2$$

$$\sigma_{xy} = \frac{1}{m \times n-1}\sum_{i=1}^{m}\sum_{j=1}^{n} (p_{ij} - \bar{p})(q_{ij} - \bar{q})$$

3.2.5 Structure Similarity Index(SSIM)

The SSIM index is another metric for image quality measurement. The original image is divided into B blocks each of size 8×8 pixels. For the block mean pixel value and the standard deviation is calculated. Then for stego-image also the mean pixel value and the standard deviation is calculated. The covariance between the original image and stego-image is calculated.

$$\text{SSIM}=\frac{(2\bar{p}\bar{q}+c_1)(2\sigma_{xy}+c_2)}{(\bar{p}^2+\bar{q}^2+c_1)((\sigma_{x^2}+\sigma_{y^2}+c_2)}$$

Where c1=0, c2=0,

$\bar{p}$ is the mean pixel value in the original image,
$\bar{q}$ is the mean pixel value in stego-image,
σ_{x^2} is the standard deviation for the original image,
σ_{y^2} is the standard deviation for stego-image and σ_{xy} is the covariance.

3.2.5 Root Mean Square Error (RMSE)

The Root Mean Square Error (RMSE) is a frequently used measure of the difference between stego image values and the original image values.

$$\textbf{RMSE}=\sqrt{\frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{ij}-q_{ij})^2}$$

IV Experimentation and Results

4.1 Comparison Graphs for Proposed System with Other Methods

4.1.1. PSNR

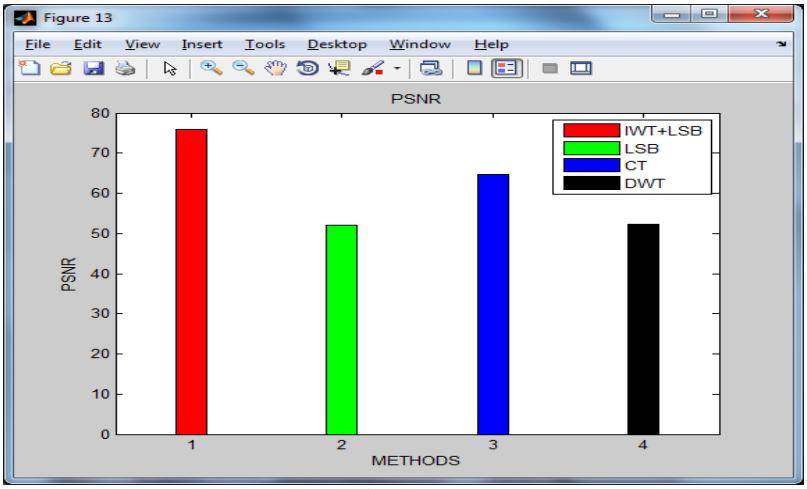


Figure4.1: Graph for PSNR Values.

4.1.2.Normalized cross- correlation

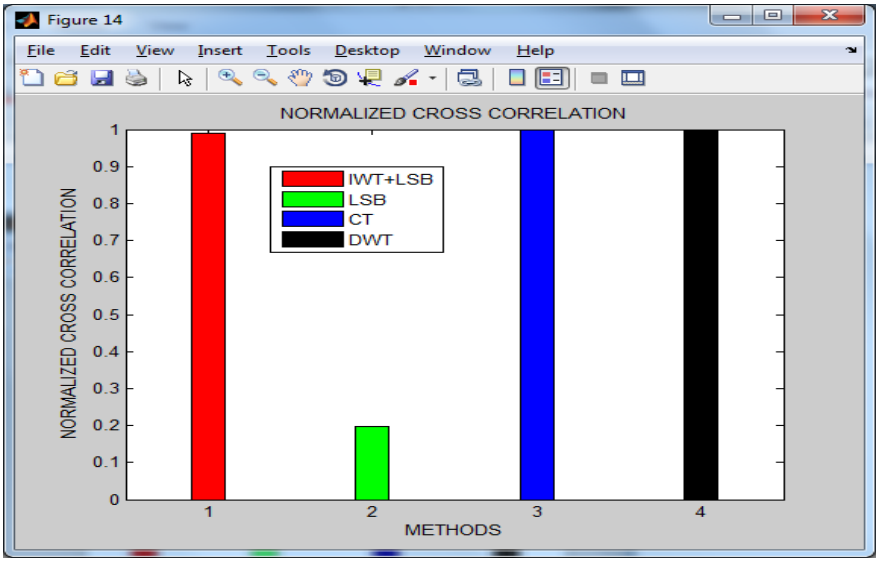


Figure 4.2: Graph for Normalized cross correlation Values.

4.1.3. Structure similarity index

Figure 4.3: Graph for Structure similarity index Values.

4.1.4. Image quality index

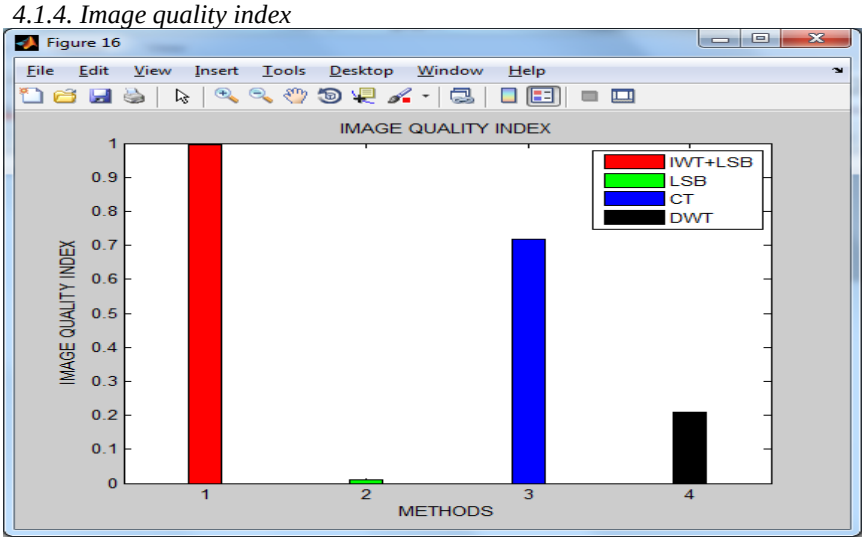


Figure 4.4: Graph for Image quality index values.

4.1.5. Pearson correlation coefficient

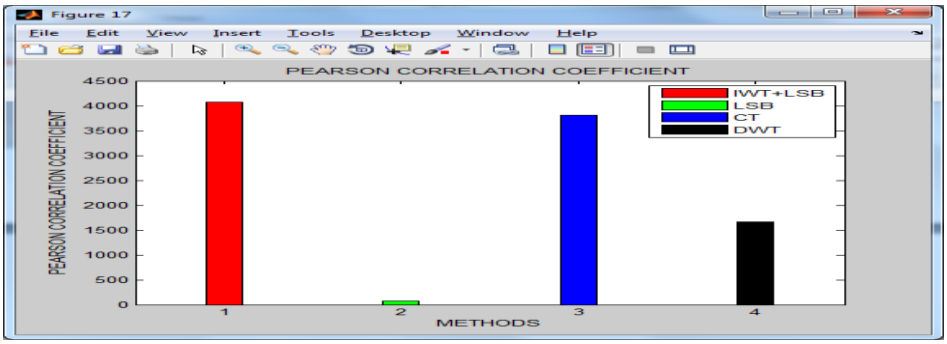


Figure 4.5.: The Graph for Pearson correlation coefficient Values.

4.1.6. RMSE

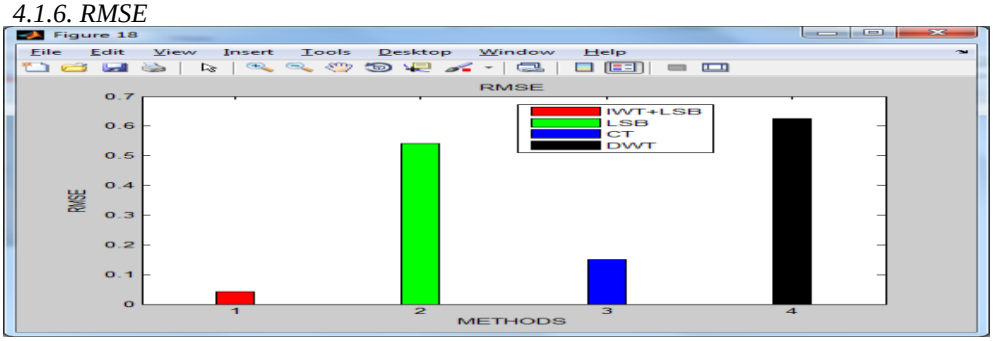


Figure 4.6: Graph for coefficient Values RMSE

From graph various Image Quality metrics like Peak Signal to Noise Ratio (PSNR), Normalized Cross Correlation (NCC), Structure similarity index (SSI), Image quality index (IQI), Pearson correlation coefficient (PCC) and Root Mean square Error (RMSE) are illustrated with various Concealment images and Secret Images. It illustrates that the value is PSNR lies between 2.82 to 5.27, PSNR lies between 79 to 80. NCC values lie in the range from 0 to1, SSI values is in between 0.1 to 1, IQI lies between 0 to 1, PCC values lie in the range from 4000 to 4010 and RMSE lies between 0.0 to 0.04. The performance of PSNR values versus sample image sets shown in the graph. The results of all the method versus one set of the image. Figure 4.1 to 4.6 shows the excellent performance ratio values in IWT with LSB.

The performance of color image steganography based on LSB with IWT various statistical parameters were evaluated. The performance results of our transform domain technique based on LSB with IWT techniques were verified using MATLAB 7 version. The outcomes revealed that capacity and security of image had increased simultaneously. The proposed method pre-adjusts the original concealment image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its supreme value and hence the message will be correctly recovered. So, there is no chance that the intruder may detect the message after a couple of attacks. LSB with IWT is a highly robust method in which the image is not destroyed by extracting the message hidden in it and provides maximum security.

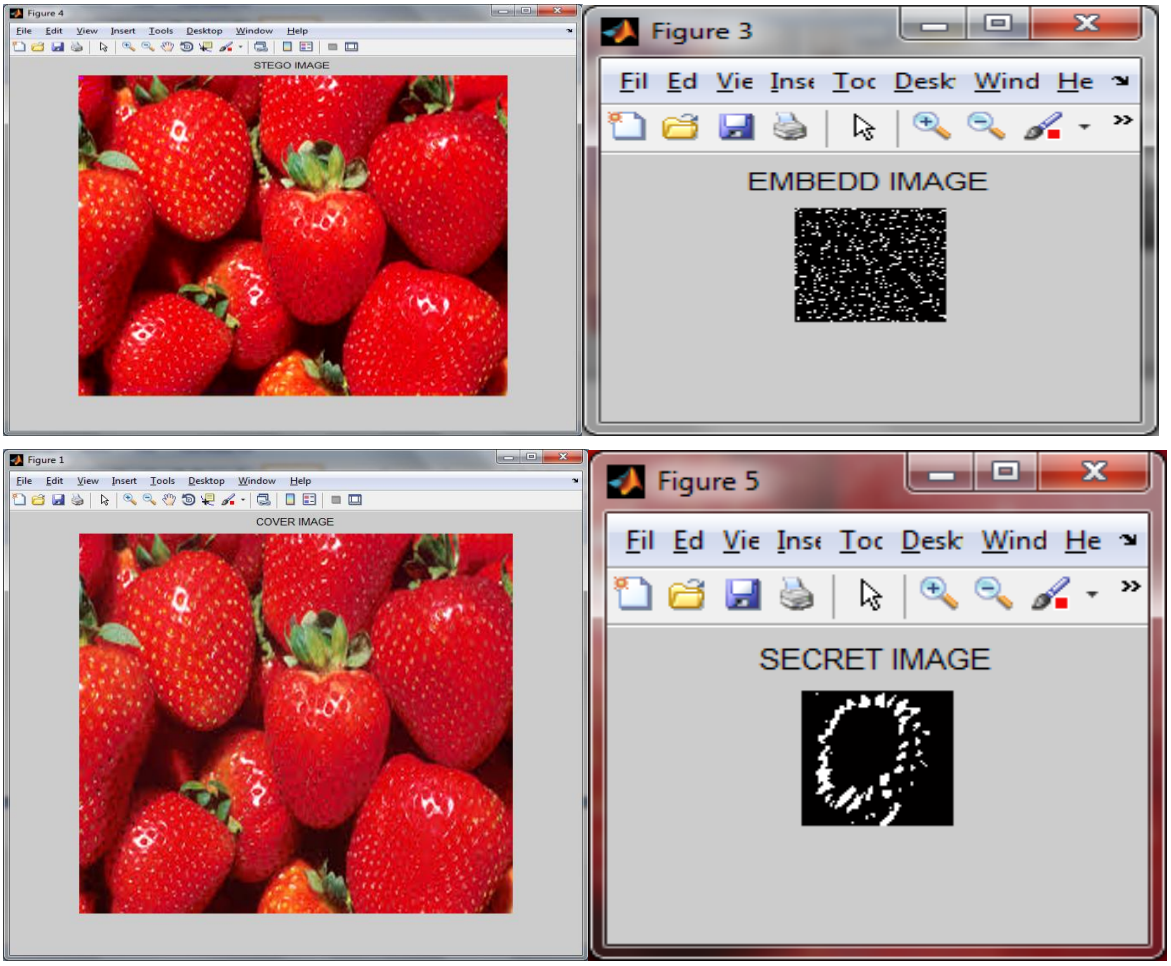
Table 1.Shows The Performance Evaluation With respect To Statistical Parameter Values of the proposed method compared to another method:

PARAMETER	**METHODS**			
	LSB+IWT	***LSB***	***CT***	***DWT***
PSNR	70.8302	50.933	55.92	63.14
NCC	0.9866	0.3979	1	1
SSIM	0.99	0.9734	0.987	0.9989
Image Quality Index	0.945	0.007	0.475	0.7619
Pearson Correlation	40*10^3	2.6*10^3	2.9*10^3	3.8*10^3
RMSE	0.073	0.6956	0.4075	0.1775

Table2.Shows the TIME ANALYSIS of LSB with IWT method

Method	LSB with IWT
Cover image size	512x512
Encryption time(sec)	0.639813
Decryption time(sec)	0.713473

V Experimental result



VI . CONCLUSIONS

The planned method inserts data that is image format in cover images using LSB with IWT method. The secret data is hidden in binary form into cover images due to protection has been provided to confidential data. The experimental results showed that the proposed scheme can be a good alternative for secure communication where two level of security is obtained in conjunction with high capacity and good imperceptibility. In this paper, a secure colour image steganography technique, using LSB with IWT is proposed. In this technique the secret image is hidden using keys. The experimental results are expected to show that the technique produces good quality stego images with better PSNR values compared to similar other techniques.

The proposed approach is implemented in MATLAB 7 and image is used in the implementation. Various images used for the experiment are described as under:

Cover Image: In the implementation, is used as a cover medium as an image. The image produced by the segmentation image is in .jpeg format. Cover images are shown above in Figure.1

Stego Image: After embedding the image in the cover image, stego image obtained. Embedding images are shown above in Figure.4

Secret image: The image recovered is in image format. Secret image is shown above in Figure5

Recovered Images: By applying extraction procedure, we recovered the secret image from stego image.

REFERENCES

[1] Akram AbdelQader and Fadel AlTamimi "A Novel Image Steganography Approach Using Multi-Layers DCT Features Based On Support Vector Machine Classifier", the International Journal of Multimedia & Its Applications, 2017

[2] Abdullah Hamid.,"Stega Image a Technique to Hide Data within Image File, Using Image", International Journal Of Engineering And Computer Science,2017

[3] Anil Kumar, Roshni Sharma," A Secure Image Steganography based on RSA Algorithm and Hash- LSB Techniques", International Journal of Advanced Research in Computer Science and Software engineering, July 2013.

[4] Ashish Nimavat, Nitin Kanzariya kin 2014, they design hybrid method is the combination of spatial domain LSB method and frequency domain DCT method. The simple LSB method is not secure to provide the randomness this combination is used. Huffman coding is used for lossless secret image compression.

[5] W. Bender. D. Gruhl. N.Morimoto, A. Lu., "Technique for data hiding ", IBM systems journal,35(3),2011.

[6] Chanu Y. J, "A short survey on image steganography and steganalysis techniques", NCETAS, vol. 1, pp. 52-55, IEEE, 2012.

[7] Gary C.Kessler, "An Overview of Cryptography: Cryptographic", HLAN, ver. 1, 1999-2014.

[8] Jyotika Kapur and Akshay. J. Baregar "Security using image processing", International Journal of Managing Information Technology,2013

[9] Mr. Mritha Ramalingam., "Stego Machine Video Steganography using Modified LSB Algorithm", World Academy of Science, Engineering and Technology, 2011.

[10] Nitin Kanzariya and Ashish Nimavat, "A Novel Technique for Image Steganography Techniques Based on LSB and DCT Coefficients" – International Journal for Scientific Research & Development| Vol. 1, Issue 11, 2014 |ISSN: 2321-0613(Page No. 2405-2408).

[11] Preeti Kumari, Ridhi Kappor , "Image Steganography for data embedding & extraction using LSB technique", International Journal Computer Applications & Information Technology Vol. 9, Issue 2, July 2016".

[12] Nilanjan Dey, Tanmay Bhattacharya, S. R. Bhadra Chaudhuri " A Session based Multiple Image Hiding Technique using DWT and DCT" International Journal of Computer Applications (0975 – 8887) Volume 38– No.5, January 2012.

[13] Rejani. R, Dr.DMurugan, Deppu V Krishanan, "Comparative study of spatial domain image steganography techniques", Int J Advanced networking and application, volume -07, issue: 02, 2015.

[14] Vijay KumarSharma, Vishalshrivastava, "A Steganography Algorithm for Hiding Images by improved LSB substitution by minimizes detection."Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.

[15] N Sathisha et al., 2013,"Non-Embedding Steganography using Average Technique in Transform Domain", IEEE 9th International Colloquium on Signal Processing and its Applications, pp 1-6.