ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

Advanced Image Steganography Technique using DWT and SVD with High PSNR

Tejal[1], Divyanshu Rao[2]
PG Student[1], Assistant professor[2]
Department of Electronics & Communication
SRIT, Jabalpur, M.P. India

Abstract:
This paper describes the enhanced technique for data hiding for more secure transmission. Steganography is the method for hiding the data into the cover image so that no one can detect the original data without having the key. In this paper proposed advance method of steganography using discrete wavelet transform (DWT) for achieving very high signal to noise ratio (SNR) and low mean square error (MSE) even if the size of original data is less.

Keywords: Steganography, Discrete Wavelet Transform (DWT), Signal to noise ratio (SNR), Mean square error (MSE).

I. INTRODUCTION

Steganography is the data hiding method in which we can hide information within the covering objects like image, audio and video with the help of this method and we can secure important information from others. In this paper we used image steganography technique where we can hide the information within the covering image without changes its parameters and its original size. In present time there are many methods available for steganography the most common method is least significant bit (LSB) method. With the help LSB steganography technique it's very easy to encrypt the information within the covering image but now hackers can easily detect the hidden information from the cover image. So now the main task is to protect the information from others this is very important to improve the steganography approach to high encryption for protecting the user's information.

II. IMAGE STEGNOGRAPHY PARAMETERS

When large information is embedded within the cover image then there is some major changes detected in the image and these change in image colours and its softness which is not good for the steganography process so there are some important parameters which should be considered in the image steganography process is done and these parameters are:

A. Capacity:

This parameter shows that how many number of bits embedded within the covering image without changes the image quality in the steganography method.

B. Mean Square Error :

Mean square error shows the quantity of change in the received image data (i.e. error) and between the cover image input data.The mean-squared error (MSE) between two images I1 (m,n) and I2(m,n) is [1]: Calculated as;

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(M,N)]^2}{M * N} \quad .....(1)$$

M and N are the number of rows and columns in the input images, respectively.

C. Peak Signal-to-Noise Ratio:

Peak Signal-to-Noise Ratio (PSNR) protect this problem by scaling the MSE according to the image file range [2]:

$$PSNR = 10\log_{10}\frac{256^2}{MSE} \quad ......(2)$$

PSNR is calculated in decibels (dB). Peak signal to noise ratio is an evaluating measurement for comparing for restoration of results for the same covering image.

III. THE CONVENTIONAL LSB STEGANOGRAPHY METHOD

The least significant bit (LSB) steganography method [3-4] is the most common spatial domain technique [5], in which consecutively replaces the least significant bit of cover image file with the information bits. The LSB method changes some or all the eighth bit of image's data so that the image's changes are not perceptible for any human eyes. When using a colour image file the LSB of each of the Blue, red, and green components can be used in this process.

Therefore, the capacity for hiding or embedded secret information within a colour image is triple of the same cover image size in the gray scale mode. When the data file is embedded subsequently to the all bytes of cover image file, it would be very easy to detect and identified and extract the message from the received image file. A moderately more secure method is improvised to have secret key between the transmitter and receiver to specify which bytes of image have been used for hiding data [6].

IV. PROPOSED STEGANOGRAPHY METHOD

In recent years so many methods and approaches are used to hide the information within the cover image is like LSB steganography, and using different transform functions like discrete cosine transform (DCT) and discrete wavelet transform (DWT) with LSB methods. In this proposed work to hide the text data within the cover image we used advance approach to create a stegno image file. In this process we first differentiate the red, green, and blue channel then after using one of the channel we perform the DWT and transform into the four frequencies low low(LL), low high(LH), high low(HL) and high high(HH) frequencies components.

The HH is less sensible to virtual eye so we can use this component to hide the data and after choosing this we perform the singular value decomposition (SVD) operation to increase the security and after the final step we used LSB steganography to create the stegno file. Figure 1 shows the block diagram of the proposed work.

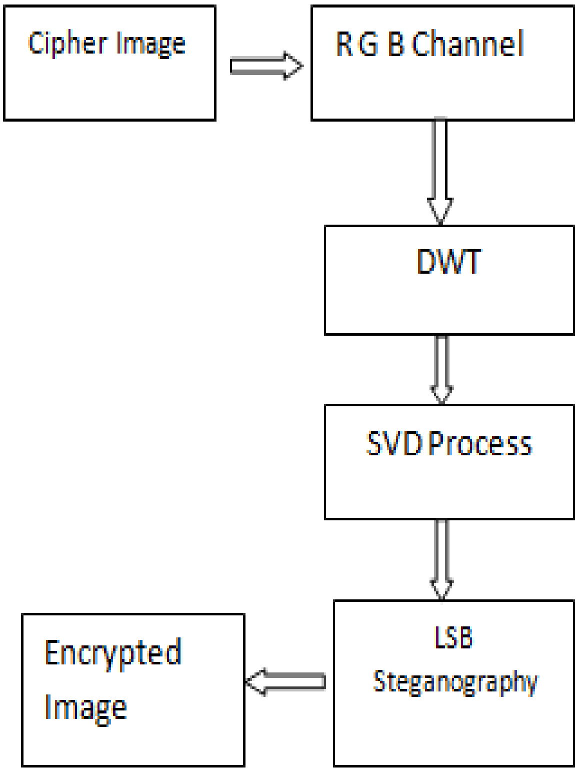

Figure.1. Block Diagram of proposed work

Same process will followed by the receiver end to recovering the original image and hiding information from the encrypted image. The encryption and decryption process is analysed with the help of MATLAB software through which we can simulate the code and process the steganography process and compare the results and calculated the MSE, PSNR, and its capacity of the cover image as well as the encrypted image data for the whole process.

V. EXPERIMENTAL RESULTS

The proposed method is implemented using the MATLAB software through which we used the Lena, Baboon, Peppers, and Sail Boat and tunnel image objects .All the cover images have .bmp image format and the same dimension of 512 × 512 and with the same size of 768 KB of 24 bit bit-maps.We encrypted the data in all these images and compare the results in term of MSE and PSNR to see how effective the proposed work. The Simulation results are mention in the figure 2 given below:

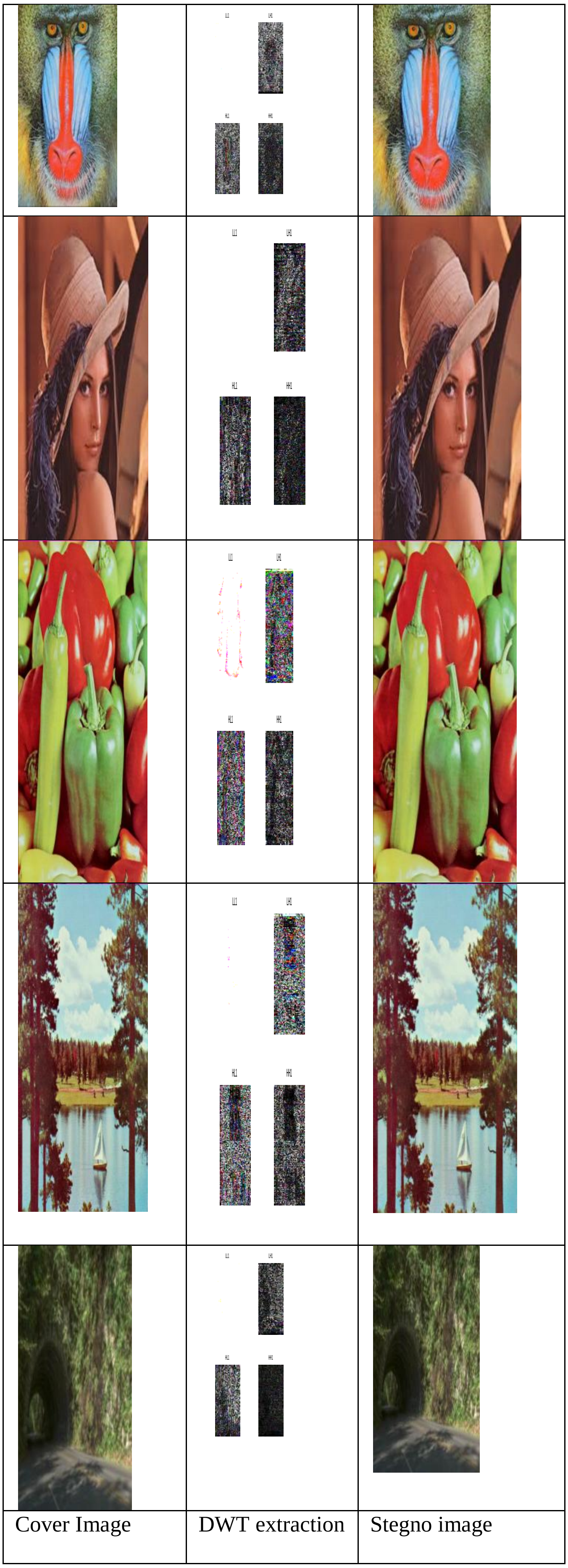

Figure.2. Column wise Cover images, DWT extraction and Stegno images of Baboon, Lena, Peppers, Sail boat and Tunnel

Table .I. Stastical Measurment

Image Name	MSE	PSNR	BER
Baboon	0.00025177	84.1548	0.00006676
Lena	0.00028992	83.5421	0.00014114
Peppers	0.00032806	83.0052	0.00008297
Sail Boat	0.00023270	84.4969	0.00004911
Tunnel	0.00024414	84.2884	0.00005865

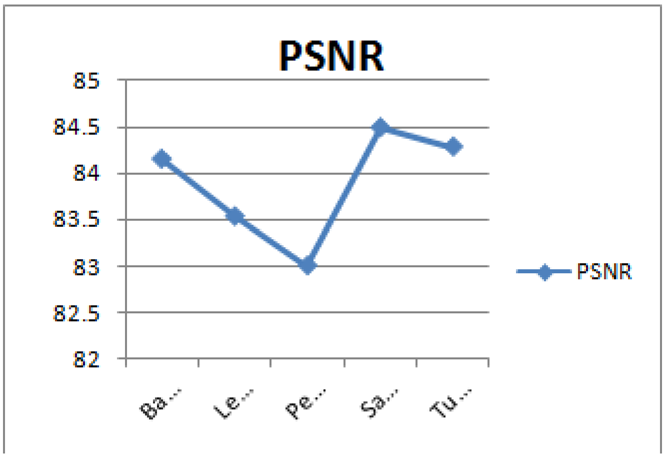

Figure.3. Comparison of PSNR

VI. CONCLUSION

In this work, we proposed the advance technique to hiding the data within the cover image file. This method gives the better results and shows the high order of security of message with the help of DWT and SVD before the LSB steganography and also we analysed the cover image and stegno image with respect to different parameters of MSE, PSNR and BER. The size of the stegno image and cover image is also which is the best for security and this proposed method provides the high security so that the hackers could not detected the hidden information.

VII.REFERENCES

[1].Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs, "Implementation of LSB Steganography and its Evaluation for Various Bits", 2004.

[2].Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.

[3].K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, pp. 469-474, 2004.

[4].S. Dey, et al., "An LSB Data Hiding Technique Using Prime Numbers," in Information Assurance and Security, 2007. IAS 2007. Third International Symposium on, 2007, pp. 101-108.

[5].Daneshkhah, et al., "A More Secure Steganography Method in Spatial Domain," in Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on, 2011, pp. 189-194.

[6].J. V. Anand and G. D. Dharaneetharan, "New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance security," presented at the Proceedings of the 2011 International Conference on Communication, Computing, Rourkela, Odisha, India 474-476, 2011.

[7].Aneesh Jain, Indranil Sen. Gupta, "A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images",IEEE-1-4244-1272-2/07©2007.

[8].Beenish Mehboob and Rashid Aziz Faruqui, "A Steganography Implementation", IEEE -4244-2427- 6/08/ $20.00 ©2008.

[9].Hassan Mathkour, Batool Al-Sadoon, Ameur Touir, "A New Image Steganography Technique", IEEE- 978-1-4244-2108-4/08/$25.00 © 2008.

[10]. Nageswara Rao Thota, Srinivasa Kumar Devireddy, "Image Compression Using Discrete Cosine Transform", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3(17), 2008.

[11].Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[12].Dr. Ekta Walia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[13].K.B. Shiva Kumar, K.B. Raja, R.K. Chhotaray, Sabyasachi Pattnaik, "Coherent Steganography using Segmentation and DCT", IEEE-978-1-4244- 5967-4/10/$26.00 ©2010.

[14]. K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, "Authentication of Secret Information in Image Steganography" .