International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 5, Volume 2 (May 2015) www.ijirae.com

Image To Image Hiding Using PSO

E Divya*
PG Student ,ECE Department
Nehru College Of Engineering And Research Centre

P Rajumar
Professor,ECE Department
Nehru College Of Engineering And Research Centre

Abstract— This paper describes the various steganographic techniques. It also compares the particle swarm optimisation algorithm with basic technique .Image to Image Hiding is possible using the steganographic techniques and improves the performance and capacity by the particle swarm optimisation.

Keywords— PSO,Image,PSNR,Zebra,Haar.

I. INTRODUCTION

The purpose of cryptography and steganography is to communicate information in a healthier and cleaner way. Then how both the cryptography and steganography differ from each other. In cryptography we feel the existence of the data whereas in steganography, we don't feel the existence of the data. So steganography is the art of hiding data. So it is derived from the greek word *stegano* and *graphia* meaning secret writing.

The technology is improving day by day we need powerful method to communicate from one place to other .More than the technology must be secure too. There are many steganographic techniques existing. Existing technique includes the spatial domain and transforms domain techniques. Spatial domain technique is having the highest payload capacity but is prone to more attack. The security is more for transform domain technique but has less payload capacity for DCT and little more for DWT.

Particle Swarm optimisation is the one of the evolutionary algorithm like the genetic algorithm. Here the particle swarm optimisation (PSO) increases the performance and thereby payload capacity. Particle Swarm optimisation is similar to fish schooling or bird flock. The particle swarm optimisation along with wavelet approach improves the performance.

II.LEAST SIGNIFICANT METHOD

Least significant Bit method (LSB) is one of the simplest and greatly used methods in steganography. Here the least bit is interchanged with a single bit of secret image. Here the message is stored in the LSB of each pixel value of cover image. When converting an analog image to digital format, we usually choose between three different ways of representing colors:

- 24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- 8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.
- 8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray

Let's see the pixels before the insertion for a 24 bit:

10000000,10100100,10110101,10110101,11110011 10110111,11100111 10110011 00110011

We need to hide a value say 30 whose binary is 11110 which after embedding becomes

10000001,10100101,101101001,10110101,11110010 10110111,11100111,10110011 ,00110011

Let's see the pixels before the insertion for a 8 bit:

10000000, 10100100, 10110101 10110101,11110011 10110111, 11100111, 10110011

We need to hide same value say 30 which after embedding becomes

10000001 10100101 10110101 10110101 11110010 10110111 11100111 10110011.

In both cases only three bits changed according to the message data, this small change is not visible to the normal human eye. So this method is more easy to implement but it is more vulnerable to attack.

But this is the method has good payload capacity and takes less time. Here the message can be protected by using two way key.LSB generally uses BMP images.

III. DISCRETE COSINE TRANSFORM

The secret data within the cover image is transformed into cosine transform using Discrete Cosine Transform (DCT). A cover image represented as image representation is transformed into a frequency representation. The DCT transforms a cover image by grouping the pixels into non-overlapping blocks of 8 × 8 pixels and transforming the pixel blocks into 64 DCT coefficients each. So even a slight modification in any one the pixel will affect the 64 image pixels in that block. If C(x,y) represents the cover image with x =12,.....M and y=1,2,....N. So the cover image is of MxN pixel which is dividing into 8x8 blocks.In this 8x8 block DCT is performed on the (MxN/64) blocks
The forward DCT is given by the following formula.

$$F(u,v) = C(u)C(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} Cos\left(\frac{(2x+1)M\pi}{2N}\right) Cos\left(\frac{(2x+1)N\pi}{2N}\right) f(x,y) \quad (1)$$

And inverse dct is

$$f(x,y) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(u)C(v)F(u,v)Cos\left(\frac{(2x+1)M\pi}{2N}\right) Cos\left(\frac{(2x+1)M\pi}{2N}\right) \quad (2)$$

IV. DISCRETE WAVELET TRANSFORM

Many practical tests propose to use the Wavelet transform domain for steganography because of a number of advantages that can be gained by using this approach. The use of such transform will mainly address the capacity and robustness of the Information-Hiding system features. It is shown that when subjected to distortion from compression, the corresponding hidden message can still be correctly identified at each resolution in the Discrete Wavelet Transform (DWT) domain. A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficient and functions. A two-parameter system is constructed such that one has a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal. In Wavelet transform, the original signal is transformed using predefined wavelets. The wavelets are orthogonal, orthonormal, or bi-orthogonal scalar or multiwavelets. The DWT used in this paper is implemented using the functions available with MATLAB with haar wavelet. The 2-D DWT leads to a decomposition of approximation coefficients at level *j* in four components which are, the approximation at level *j+1*, and the details in three orientations (horizontal, vertical, and diagonal).

Algorithm for Basic Steganographic Technique

Step1: Read the cover image and the secret message or image to hide
Step2: Convert the message into binary bit stream
Step3: Transform the cover image into spatial or transform domain.
Step4: Embedding the secret data.
Step5: Get the inverse transform
Step6: Write the stego image

V. PARTICLE SWARM OPTIMISATION

It is a optimisation technique proposed by Kennedy and Ebherhart in the year 1995 .The algorithm simulates the behaviour of bird flock flying in multidimensional space(like they fly in the sky for better food) search of food or for optimum place by adjusting their movements for a better place.The computation is similar to Genetic algorithm. Each particle or individual in the population (swarm) represents a potential solution. These particles are flying through a multidimensional search space, where the position of each particle is adjusted according to its own experience and that of its neighbours. The swarm or particles are initialised randomly and then search for optimal solution. All the particles have fitness values which are calculated by the objective function to be optimised and have velocities which direct the movement of the particles. Let $P_i(t)$ denote the position of the particle and this position is changed by adding a velocity component $V_i(t)$ to it.

$$P_i(t+1)=P_i(t)+V_i(t+1) \quad (3)$$

And its velocity is updated by

$V_i(t+1) = C*W*V_i(t)+c1*R1(t)*[P_{best} - P_i(t)] + c2*R2*[Gbest-Pi(t)$ (4)

The experiential knowledge of a particle is generally referred to as the cognitive component, which is proportional to the distance of the particle from its own best position found since the first time step. The socially exchanged information is referred to as the social component of the velocity equation. c1 and c2 are the cognitive and social components and c1+c2 can be maximum upto 4. The personal best position P_{best} associated with particle i is the best position the particle has visited since the first time step. G_{best} is the global best position for the PSO..R1 and R2 are the two random numbers in the range [0,1].C *W is the inertia weight introduced to control and balance the exploration and exploitation trade off. *W* changes according to the number of iteration and the maximum value of w achieved is 0.99.C is taken to be 1.
The personal best position at the next step can be calculated using:

$P_{best}(t+1) = P_{best}(t)$ if $f(Pi(t+1)) \geq f(P_i(t))$
$Pi(t+1)$ if $f(Pi(t+1)) < f(Pi(t))$ (5)

Where f is the fitness function and global best position is calculated as:

$G_{best}=\{P_1, P_2, \ldots\ldots\ldots\ldots, P_n\}=\min\{f(P_1(t)), \ldots\ldots f(P_n(t))\}$ (6)

Algorithm for Proposed Method

Step1: Read the cover image and the secret message or image to hide
Step2: Convert the message into binary bit stream
Step3: Transform the cover image into spatial or transform domain.
Step4: Embedding the secret data.
Step5: Get the inverse transform.
Step6: Calculate the fitness for each iteration.
Step7: Calculate the global and local best position.
Step8: Update particle velocity and position.
Step9: Write the stego image.

VI. RESULT AND ANALYSIS

The basic steganographic methods for image to image hiding are compared. Then the particle swarm optimization is applied to improve the performance. Matlab 2010 version software is used for compiling.The image zebra is used to hide in three image.The PSNR values and computation time before and after PSO is compared and tabulated .The histogram plots are also compared before and after hiding.The PSO is calculated for 100 of iterations.The wavelet approach using PSO gives the best result but the computation time is higher than LSB and DCT technique.The DCT gives less PSNR. The LSB gives better PSNR but is more prone to attacks.

Table 1: PSNR based Comparison of the Steganographic Techniques

Image	LSB	DCT	DWT	LSB PSO	DCT PSO	DWT PSO
Cameraman	56.1697	35.0425	47.9457	76.1697	71.8892	78.42
Baboon	55.4992	30.9343	48.5993	75.4992	73.7270	80.03
Lena	55.5698	36.4184	49.5953	75.5698	68.2608	77.80

Table 2: Computation Time (in seconds) for Steganographic Techniques

Image	LSB	DCT	DWT	LSB PSO	DCT PSO	DWT PSO
Cameraman	0.410230	4.196191	0.966922	49.024933	408.388462	416.124658
Baboon	0.323028	4.135997	0.879391	47.660984	416.062536	428.751503
Lena	0.414295	4.364761	0.909226	47.481568	424.223930	481.478607

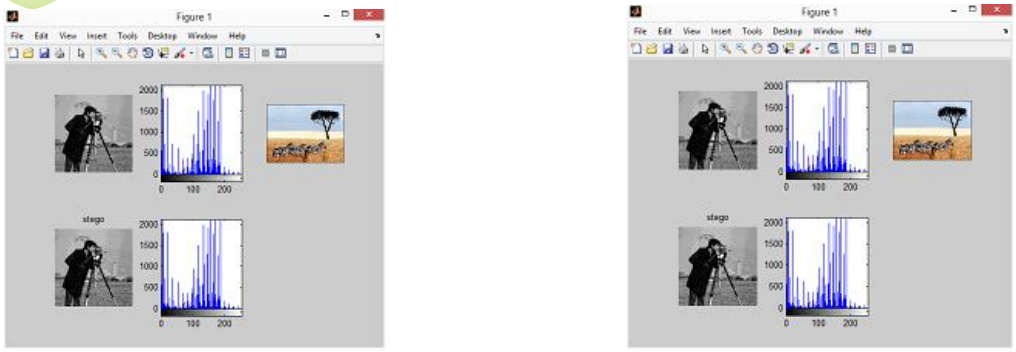

Figure1:Test Result Of Cameraman Hiding Zebra (a) based on LSB method (right) (b)based on PSO Method (left)

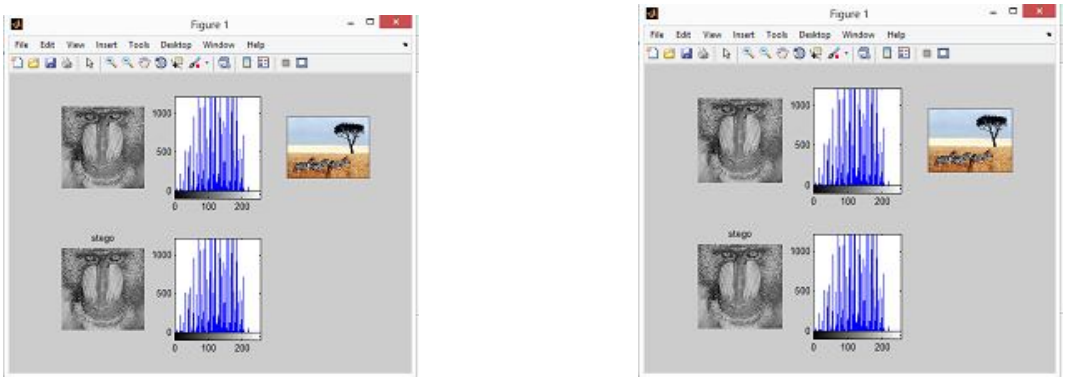

Figure2: Test Result of Baboon Hiding Zebra (a) based on LSB method (right) (b) based on PSO Method (left)

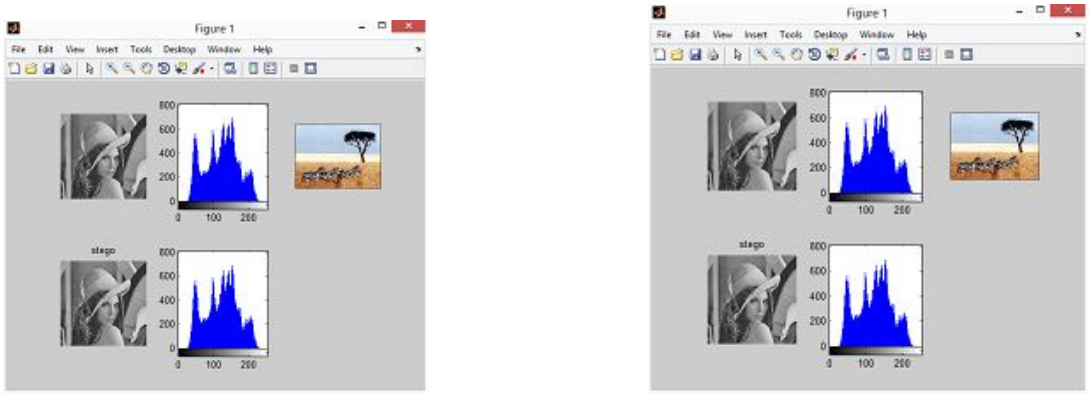

Figure3:Test Result Of Lena Hiding Zebra (a) based on LSB method (right) (b)based on PSO Method (left)

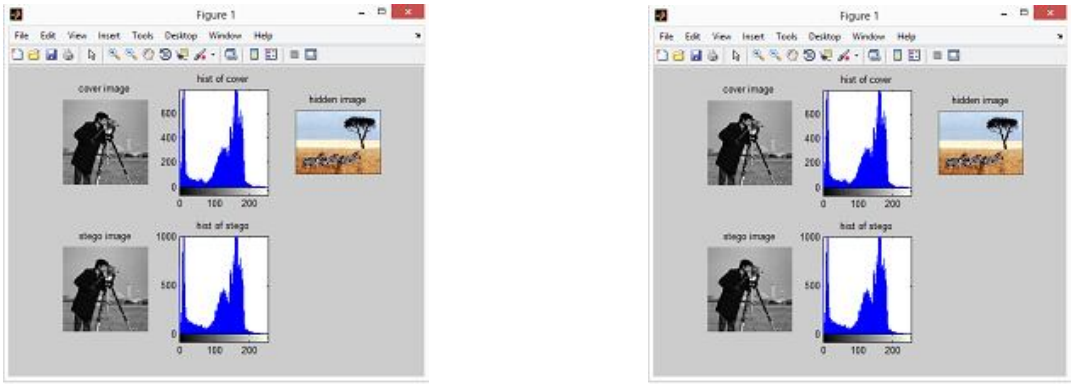

Figure 4:Test Result Of Cameraman Hiding Zebra (a) based on DCT method (right) (b)based on PSO Method (left)

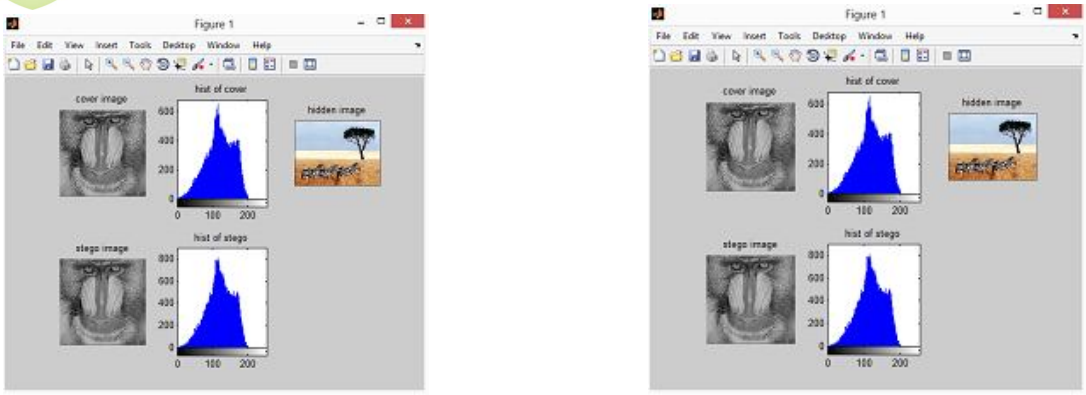

Figure5:Test Result Of Baboon Hiding Zebra (a) based on DCT method (right) (b)based on PSO Method (left)

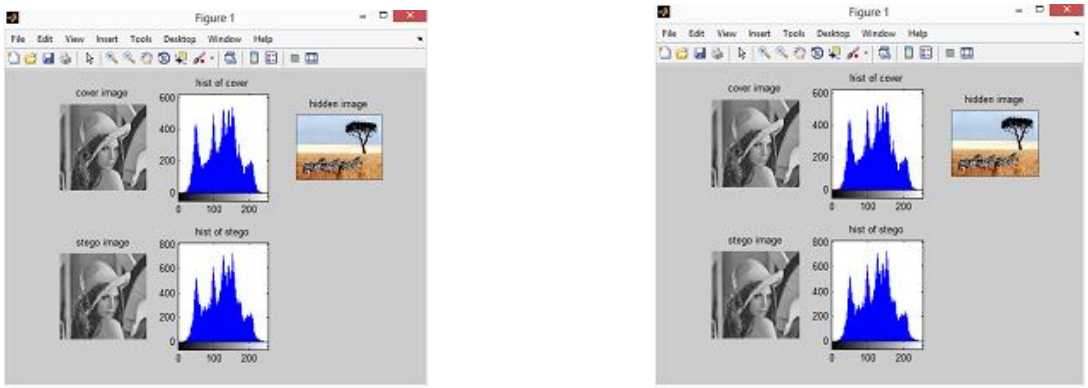

Figure6:Test Result Of Lena Hiding Zebra (a) based on DCT method (right) (b)based on PSO Method (left)

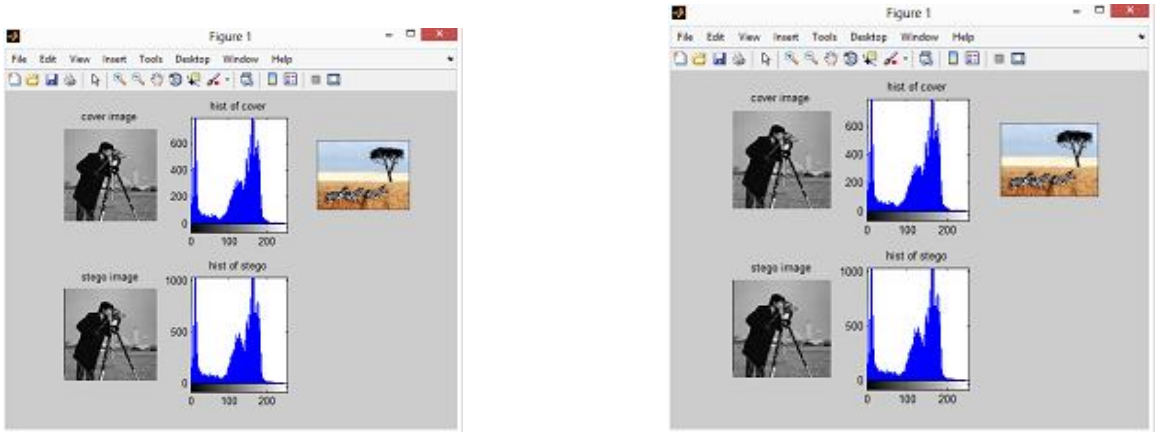

Figure7:Test Result Of Cameraman Hiding Zebra (a) based on DWT method (right) (b)based on PSO Method (left)

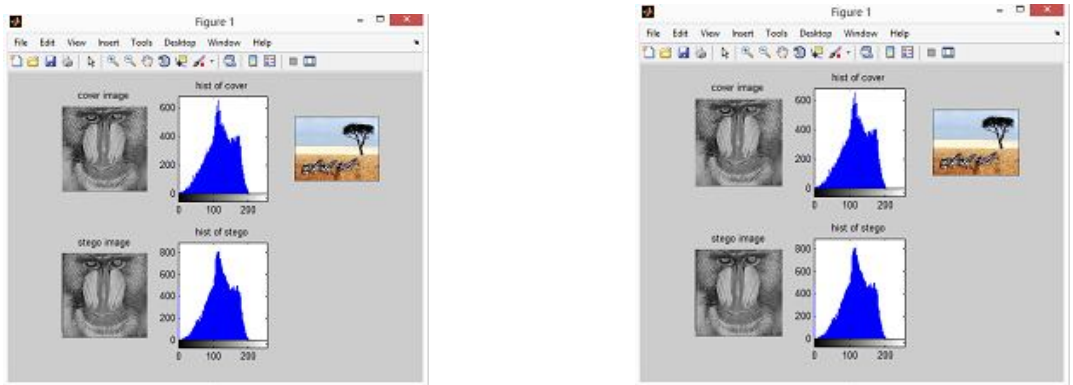

Figure8:Test Result Of Baboon Hiding Zebra (a) based on DWT method (right) (b)based on PSO Method (left)

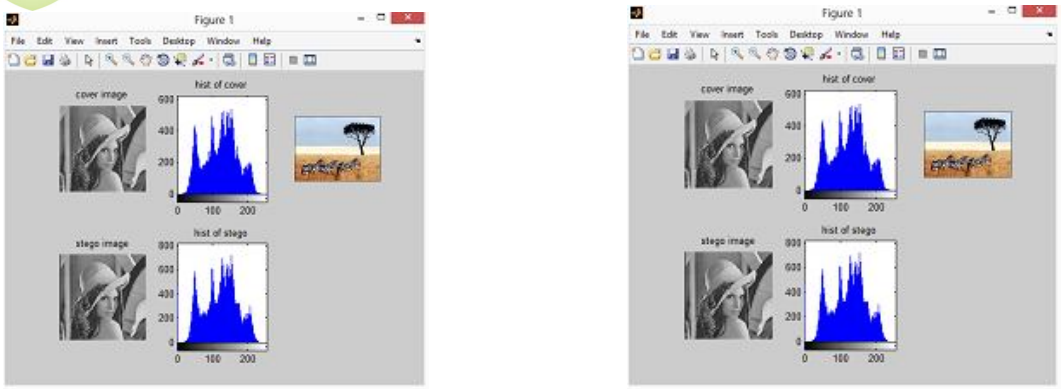

Figure9:Test Result Of Lena Hiding Zebra (a) based on DWT method (right) (b)based on PSO Method (left)

VII. CONCLUSION

This paper analysed the embedding procedure using PSO in spatial and transform domain.PSO was analysed for 100 iterations and obtained increase in efficiency. PSO finds pixel location for hiding the data. The performance of both techniques is compared and the PSO gives best stego images. Paper analysed the basic three techniques with PSO and without PSO.The PSNR value compared showed that the PSO gave good PSNR after 100 iterations.The DWT using PSO gives good PSNR but takes more computation compared to other two methods.

The future work would focus on decreasing the computation with improved performance and payload capacity.

REFERENCES

[1] Ratnakirti Roy1, Suvamoy Changder1, Anirban Sarkar1, Narayan C Debnath2**,** "Evaluating Image Steganography Techniques: Future Research Challenges " IEEE transaction 2013
[2] R. Amritharajan, R. Akila, P. Deepikachowdavarapu, "A ComparativeAnalysis of Image Steganography" International Journal Of Computer Applications, vol. 2,No 3, pp. 41–47, 2010.
[3] Punam Bedi, Roli Bansal , Priti Sehgal," Using PSO in a spatial domain based image hiding scheme with distortion tolerance" ,@ science direct Computers and Electrical Engineering 39 (2013) 640–654,
[4] Feno Heriniaina Rabevohitra and Jun Sang"Using PSO Algorithm for simple LSB Substitution Based Steganography Scheme in DCT Transformation Domain"@Springer-Verlag Berlin Heidelberg 2011,vol pp.212-220,2011.
[5] Mohd Afizi Mohd Shukran,et.al,"Image Classification Technique using modified Particle Swarm Optimisation" Modern Applied Science, Vol. 5, No. 5; October 2011.
[6] N. Lavanya , V.Manjula, N.V. Krishna Rao," Robust and Secure Data Hiding in Image UsingBiometric Technique, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5133 – 51 .
[7] Anjali A. Shejul, Umesh L. Kulkarni," A Secure Skin Tonebased Steganography Using Wavelet Transform"International Journal Of computer theory and engineering,Vol 3, No.1, pp. 16-22,February,2011 .
[8] P.Rajkumar, R.Kar, A.K.Bhattacharjee, H.Dharmasa "A comparative analysis of steganographic data hiding within digital Images" International Journal Of Computer Applications, Vol 53. N0-1, September 2012.
[9] Rafael C.Gonzalez, Richard E. Woods, Steven L.Eddins, "Digital Image Processing Using MATLAB' Pearson Education, 2004.

