ISSN 22773061

APPLICATION OF STEGANOGRAPHY IN SYMMETRIC KEY CRYPTOGRAPHY WITH GENETIC ALGORITHM

Sabyasachi Pramanik[1], Samir Kumar Bandopadhyay[2]
[1]Assistant Professor, Haldia Institute of Technology, India,
sabyalnt@gmail.com
[2]Professor, University of Calcutta, India,
skb1@vsnl.com

ABSTRACT

Embedding maximum information in a stego-image with minimum change in its appearance has been a major concern in image-based steganography techniques. In this paper, utilizing Genetic algorithm (GA) we have built up a competent optimal robust steganography technique. The watermarks are implanted into the HL and LH frequency coefficients in bi-orthogonal wavelet transform (BWT). In order to get better the quality of stego image and robustness of the steganography we have to develop an optimization technique using a model to explore for the optimal locations. We examine the presentation of the suggested technique in terms of Peak signal to Noise ratio (PSNR) and Normalized correlation (NC). The proposed technique is the application of steganography for confidential transmission of symmetric key generated using Genetic algorithm (GA) that can accomplish a good imperceptibility and robustness of the image

Key words: Steganography, Cryptography, Symmetric Key, Bi-Orthogonal Wavelet Transforms (BWT), Genetic Algorithm (GA), Robustness, PSNR, NC

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol 10, No.7
editor@cirworld.com
www.cirworld.com, member.cirworld.com

1. INTRODUCTION

Steganography is an art of transferring information in a way that the existence of information is concealed. It utilizes the various medium of a carrier information like video, audio, text, etc. [1]. With the development of internet technology, we can transfer the digital data over the network. Therefore how to protect the secret information during its transfer is an important issue [2]. Information hiding is one method to provide more security to transfer information. Many of the researchers utilize the cryptography, but nowadays steganography is the best method for hiding information. Suspicion factor is only difference between both of them [3].The three attributes which are used in the steganography method are imperceptibility, capacity and robustness [4]. Germans invented the Microdot technique during the Second World War. The information especially photographs, was sent over an insecure channel. Today steganography is used the most of the networks so it is high speed delivery channel [5]. The LSB planes replaces the least significant bits of the host image with secret data. For k-bit LSB substitution, the exhaustive search method would take a long period of time to find an optimal substitution matrix [6]. Based on image characteristic LSB insertion method is divided into fixed size and variable size. In first method same number of bits in each pixel of cover image and another one variable number of bits in each pixel are used for message [7].

The JPEG format uses discrete cosine transform (DCT) to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients. Here, LSBs of the quantized DCT coefficients are used as redundant bits [8]. DCT was extensively utilized in watermarking schemes. In DCT the image was divided into frequency bands, and the watermark was embedded in low and middle frequency bands [9]. The compressed data is stored as integers; however, if we need to quantize the data to encode a message, all the calculations required involve floating point data. Information is hidden in the JPEG image by modulating the rounding choices either up or down in the DCT coefficients [10].

For watermark embedding in the DCT domain, if we embed the watermark in the higher frequency bands, even though the watermarked image quality is good, it is vulnerable to the low pass filtering (LPF) attack. Thus, embedding into the higher frequency bands coefficients is not robust, although the watermarked image quality is assured [11]. In DCT method of hiding information of the image, the image coefficients are almost all zero and cannot hide messages. So, we utilize the DWT hiding technique. Wavelet transform has the capability to offer some information of frequency- time domain simultaneously. This transform utilize the time domain, it is passed through low-pass and high-pass filters to extract low and high frequencies respectively [12]. Discrete wavelet transform is applied to the original image and the watermark separately. Then separate the original image into 4 blocks [13]. Wavelets have their energy determined in time and are well suited for the analysis of the transient, time varying signals. The 2D wavelet transform decomposes an image into lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The two parameter system is constructed with two indices. The set of coefficients are called the DWT of a signal. 1D, 2D and 3D are the format of the image is transformed using predefined wavelets [14].

In use of DWT, embedding capacity is very low because we utilize the only one significant coefficient per block. In this Bi-orthogonal wavelet transform (BWT) [15] domain we use successive sub band quantization. DWT has single level decomposition whereas BWT has bi-level decomposition. Here we find the robust watermarking using BWT. In this scheme, the original image is decomposed into four frequency sub-band (LL, LH, HL and HH) using BWT and hidden information is embedded in to mid frequency range HL or LH sub band. Wavelets can be orthogonal or bi-orthogonal. The bi-orthogonal wavelet transform is an invertible transform.

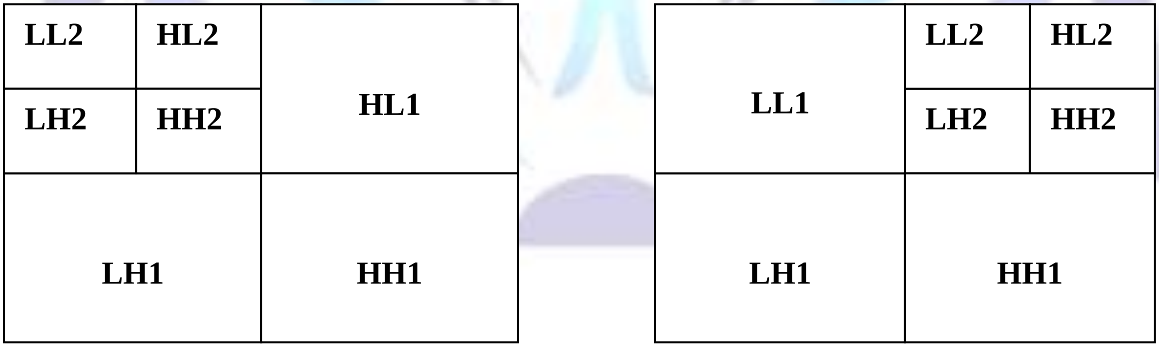


Fig 1: 1st level decomposition and 2nd level decomposition

In this paper we choose a most fit image based on Genetic algorithm as hidden object that would be sent through steganography from sender to receiver and this image's pixel information would produce the symmetric key. Symmetric key cryptography is based on sharing secrecy. The total process can also be handled by a Key Distribution Centre that would take the responsibility of symmetric key distribution between two negotiable parties on a session basis agreement.

2. CONSIDERABLE TECHNIQUES

2.1 BI-ORTHOGONAL WAVELET TRANSFORMS

By the properties of faultless reconstruction and decomposition functions the bi-orthogonal wavelet transforms are identified as invertible transforms. When compared with orthogonal wavelets, higher implanting capability while employed in the decomposition of the image into different channels is an extraordinary important characteristic of bi-orthogonal wavelets.

2.2 GENETIC ALGORITHM

Belonging to the field of evolutionary computation, Genetic algorithm is one of the most expansively utilized techniques. Several researches prepared using GA have showed that it was strong and steady in looking for global optimal solutions. An easy GA mainly contains three operations, i.e. selection, genetic operation, and replacement. GA varies from long-established optimization techniques in that:

1. They role on a group (population) of test solutions (individuals) and a positive number (fitness) is given to every individual denoting a measure of goodness.

2. They activate stochastic operators such as selection, crossover, and mutation in order to produce optimal solution.

3. PROPOSED ROBUST STEGANOGRAPHY TECHNIQUE USING GENETIC ALGORITHM :

Based on watermarking technique, our method may be very efficient against different low- frequency attacks, which will demolish the low frequency component of the image. DWT has the only level decomposition while BWT has the bilevel putrefaction.

3.1 Embedding algorithm

The embedding algorithm is described as follows, the initial process of the embedding algorithm, inputs are and Hidden Image image and output is Stego Image Procedure

1) Take the Cover Image

2) Decompose the Cover Image into different sub bands such as HH, HL, LH and LL using Biorthogonal wavelet transform for embedding the steganograph image.

3) Choose the HL and LH sub-bands for embedding the steganograph image from the four sub-bands. Since the approximation coefficients are supposed to be relatively stable and less sensitive to slight changes of the image pixel, they are the perfect embedding area. In order to achieve a balance between robustness and fidelity, the coefficients at widespread sub-bands HL and LH are selected for watermark embedding based on artificial intelligent technique.

In steganography, pixels are embedded into the HL and LH sub-band simultaneously with the aid of the following steps.

4) Compute the mean value and the maximum value of the chosen embedding parts in the HL sub-band. Similarly, the mean and maximum value of the LH sub-bands is computed.

5) The embedding process is carried out in two cases based on the embedded bit value of the Hidden Image that can be either 0 or 1. For embedding of each bit, we use HL and LH sub band one after another continuously until the total hidden image get embedded. At first we embed the height and width information i.e. two integer values into first 16 pixels then we embed pixel information of Hidden Image.

Case 1: for embedding the bit '1': For The values in the HL or LH sub-band is compared against the maximum value and modified as follows: If the values in the HL and LH sub-band are greater than mean value then take the absolute value and embed the same otherwise, if it is lesser than 1, add the corresponding pixel with the maximum value and embed the modified absolute value.

Case 2: for embedding the bit '0': If the values in the HL and LH sub-bands are lesser than mean value take the absolute value and embed the same. And, if it is greater than mean value, subtract the corresponding pixel with the maximum value and embed the modified absolute value. In the same way, embed the subsequent pixels into the LH sub-band.

The block diagram for the watermark embedding process is shown in figure 2.

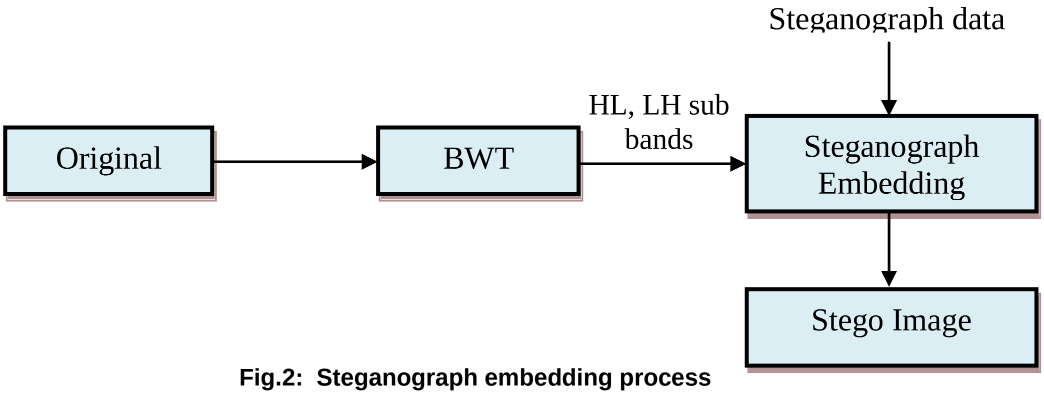


Fig.2: Steganograph embedding process

3.2 Extracting algorithm

The steganograph extraction algorithm is described as follows: Here the inputs are stego image, an output is extracted Hidden Image

Procedure

1)Decompose the obtained stego image into HH, HL, LH and LL sub-bands using Inverse biorthogonal wavelet transform for extracting the steganograph image.

2)Select the HL and LH sub-bands for extracting the steganograph image.

3) Extract the Hidden Images bit information from the Stego Image from the HL and LH sub-bands one after another. First 16 pixel would provide the height and width of the Hiden Image, after that carry on the extraction process for height*width times . If the embedded pixel value is greater than the mean value of Cover Image then the extracted bitl value as 1. If it is lesser than the extracted bit is 0.

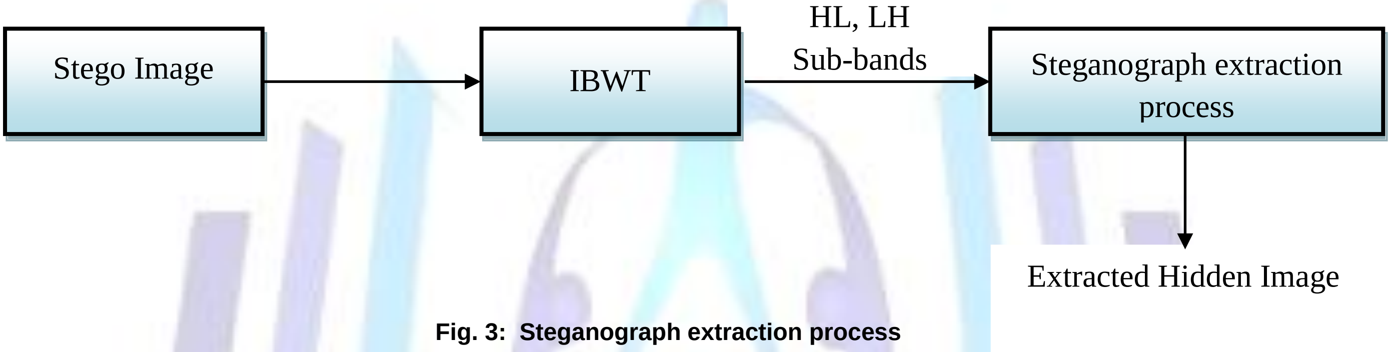


Fig. 3: Steganograph extraction process

3.3 Optimization based on GA:

We make use of the Genetic algorithm for producing the chromosome.

We test the chromosome image one by one through embedding and extraction process and find out the fitness value based on PSNR and NCC value. Thus we select the most fit Chromosome image as our Hidden Image

$$Fitness = PSNR + NCC \qquad - (1)$$

Below mentioned formula for computing the value for PSNR and Normalised correlation coefficient (NCC) is,

$$PSNR = 10\log_{10}\frac{E_{\max}^{2} \times S_w \times S_h}{\sum \left(S_{ab} - S_{ab}^{*}\right)} \qquad - (2)$$

$$NCC = \frac{\sum_{a=0}^{q}\sum_{b=0}^{p} I_S(a,b) \times E_S(a,b)}{\sum_{a=0}^{q}\sum_{b=0}^{p} I_S(a,b)^2}$$

Where,

S_w and S_h - width and height of the Hidden Image,

S_{ab} - Cover Image pixel value at coordinate (a, b)

S_{ab}^{*} - Hidden Image pixel value at coordinate (a, b)

$E_{\max}^{2}$ - Largest energy of the image pixels (i.e., $E_{\max}$ = 255 for 256 gray-level images)

$I_S(a,b)$ - Original stego image, $E_S(a,b)$ - Extracted image

p and q - width and height of the stego image

Here Selection ,Crossover and Mutation has been performed

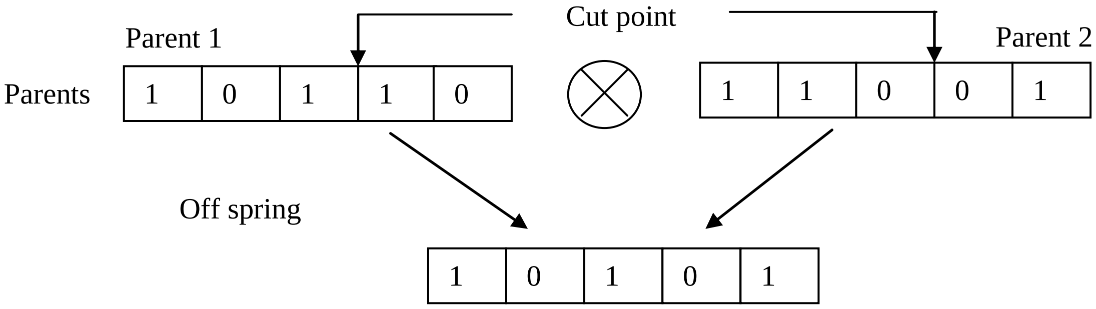
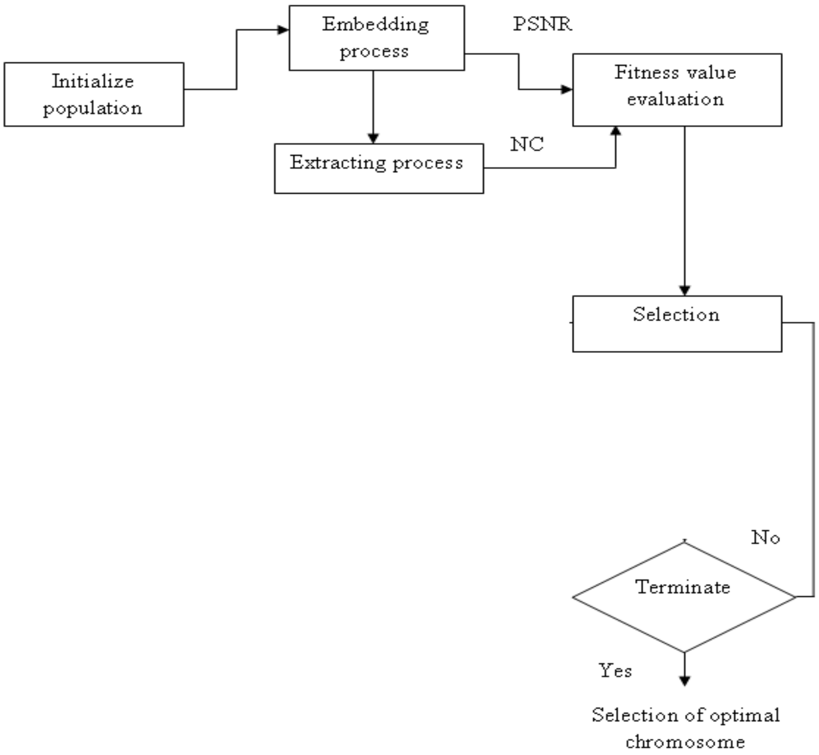


Fig 4: crossover operation

3.4 Steps:

Symmetric Key is also referred as Session Key. It is the key between two parties and it is dynamic in nature. It is created for each session and destroyed when the session is over. Here we take a set of images of chromosomes and then we produce another set of images of chromosomes using genetic algorithm. We select the most fit image out of them based on fitness value that depends on the values of PSNR and NC. This selected image's pixels information would generate the symmetric key that would be sent through steganography from sender to receiver i.e., the distribution of key between two negotiable parties. A third party also can work as Key Distribution Centre and can send the image to two negotiable parties for generation of key for one session only.

1) Take a set of chromosomes' images say n numbers of images as they are unique in nature so that we can get diversity in images.
2) Make crossover for x times where x is a random integer variable. Cut point of each pair would also be variable in nature. Thus finally we get the set of p no of images of mutated chromosomes.
3) Take each image of mutated chromosome as hidden image and run embedding algorithm and calculate PSNR values using genetic algorithm.
4) Thus through extraction algorithm use embedded image as input and calculate NC values.
5) Add PSNR and NC values to calculate fitness values
6) Repeat step 3 to 5 until the p^{th} image
7) Find out maximum fitness value based on PSNR and NC values
8) Calculate row sum value of the pixels of the selected image and finally add them to get the value of symmetric key
9) Transmit the finally selected most fitted mutated chromosome's image as hidden image to the receiver using steganography approach
10) Receiver would extract the sender's hidden image from his received stegano image and by calculating row sum of the pixel values of the hidden image followed by the calculation of adding those row sum values, he can retrieve the value of the symmetric key.



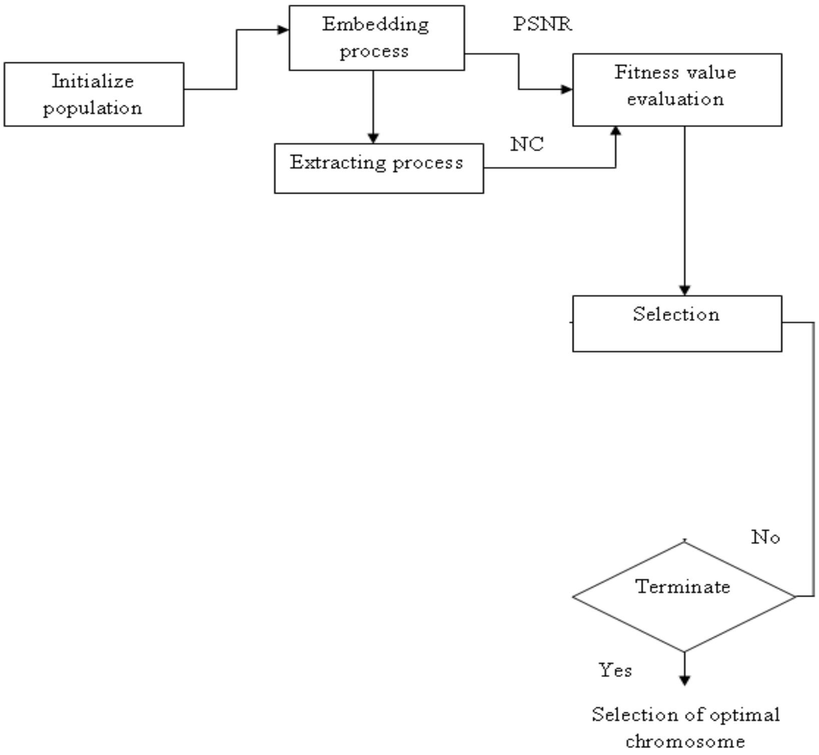


Fig 5: Proposed steganograph technique based on GA

4. EXPERIMENTAL RESULTS AND DISCUSSION

In MATLAB our suggested method is executed. Using the paradigm image developing we have experimented our offered approach. We have taken a Cover Image,”Lena”, and sample mutated chromosomes’ images as Hidden Images, these are Chromosome 1”, “Chromosome 2”, “Chromosome 3” and “Chromosome 4” generated through GA. We run the embedding and extraction algorithm and find out the PSNR and NC values respectively and calculate the FITNESS value to choose the most fit Chromosome Image as selected Hidden Image. Here, Chromosome 1 is selected as the most fit image i.e. the chosen Hidden Image.

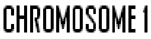
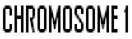
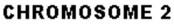
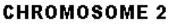
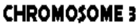
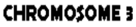
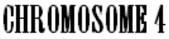
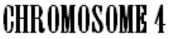
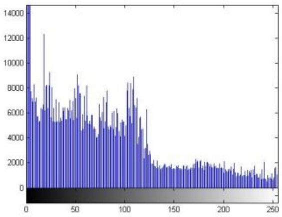
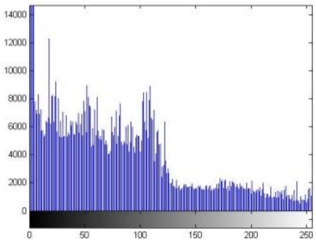
Sl. No	Original Image	Hidden image	Stego image	Extracted image	Proposed	
					PSNR	NC
1		 CHROMOSOME 1		 CHROMOSOME 1	54.3153	0.96391
2		 CHROMOSOME 2		 CHROMOSOME 2	53.9238	0.96622
3		 CHROMOSOME 3		 CHROMOSOME 3	53.5513	0.99893
4		 CHROMOSOME 4		 CHROMOSOME 4	53.5599	0.9808

Table 1: Experimental results for proposed steganography technique

Sl. No	Original image	Corresponding Histogram image	Stego Image	Corresponding Histogram image
1				

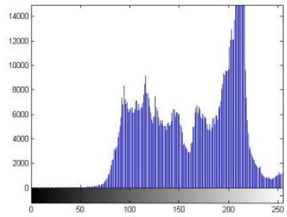
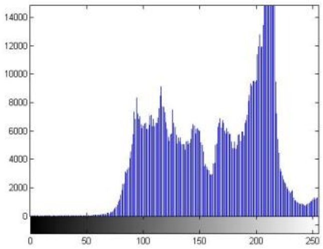
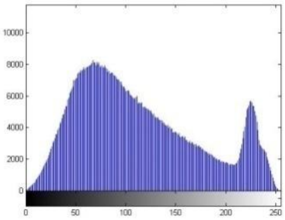
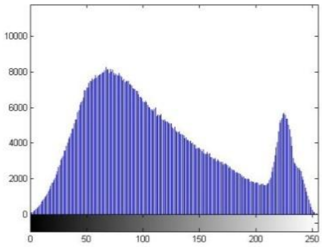
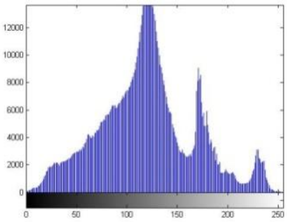
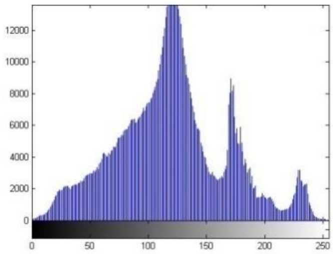
2				
3				
4				

Table 2: Histogram image of original image and stegano image

5. COMPARISON AND ROBUSTNESS ANALYSIS

Our recommended steganography technique is compared with the present DWT based steaganography technique as illustrated in the literature [9]. With the assistance of PSNR and NC values of the stegano image the strength of our planned steganography technique can be analysed.

Cover image	Proposed technique PSNR	
	DWT	Our model
Lena	44.90	**54.3153**

Table 5: Comparison results

The variation between the present technique and proposed technique PSNR values are shown in the above mentioned graph. The above illustrated table obviously explains that our offered technique is superior than DWT .This gives improved results than that algorithms and this shows that our offered technique is superior than the present work.

6. CONCLUSION

Thus we have successfully implemented above technique of steganography using BWT for confidential transmission of symmetric key generated using Genetic algorithm (GA) that can accomplish a good imperceptibility and robustness of the image that was shown by the experimental result. As improvement of work is a continuous process, we would eagerly look for further improved technique for contributing more potential security in the world of global networking.

Reference paper:

[1] Mahwish Bano, Tasneem MShah and Shaheryar Malik, “Improving Embedding Capacity with Minimum Degradation of Stego-image”, International Journal of Basic & Applied Sciences, Vol. 10, No. 06, pp. 30-35, 2010

[2] Yeuan Kuen Lee and Ling Hwei Chen, “High capacity image steganographic model”, Image signal process, Vol. 147, No.3, pp. 1-15, 2000

[3] H S Manjunatha Reddy and K B Raja, “High Capacity and Security Steganography Using Discrete Wavelet Transform”, International Journal of Computer Science and Security (IJCSS), Vol. 3, No. 6, pp. 462-472, xxxx

[4] G. Brisbane, R. Safavi-Naini and P. Ogunbona, “High-capacity steganography using a shared colour palette”, Image Signal Process, Vol. 152, No. 6, pp. 787-792, December 2005

[5] T. Morkel, J.H.P. Eloff and M.S. Olivier, “An Overview of Image Steganography”, Information and Computer Security Architecture (ICSA) Research Group

[6] Marghny Mohamed, Fadwa Al-Afari and Mohamed Bamatraf, “Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation”, International Arab Journal of e-Technology, Vol. 2, No. 1, pp. 11-17, January 2011

[7] Elham Ghasemi, Jamshid Shanbehzadeh, and Nima Fassihi, “High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform”, Intelligent Control and Innovative Computing, Vol. 10, pp. 395-402, 2012

[8] Amin Milani Fard, Mohammad-R. Akbarzadeh-T and Farshad Varasteh -A, “A New Genetic Algorithm Approach for Secure JPEG Steganography”

[9] Alimohammad Latif and Ahmad reza Naghsh-Nilchi, “Digital Image Watermarking Based On Parameters Amelioration of Parametric Slant-Hadamard Transform Using Genetic Algorithm”, International Journal of Innovative Computing, Information And Control, Vol. 8, No. 2, pp.1205-1220, 2012

[10] Usha B.A, N K Srinath and N K Cauvery, “Analysis of Image Steganalysis Techniques to Defend Against Statistical Attacks – A SURVEY”, IJRET, Vol. 1, No. 2, pp. 148-151, 2012

[11] Chin-Shiuh Shieh, Hsiang-Cheh Huang, Feng-Hsing Wang and Jeng-Shyang Pan, “Genetic watermarking based on transform-domain techniques”, Pattern Recognition, Vol. 37, pp. 555 – 565, 2004

[12] Patrizio Campisi, Alessandro Neri and Marco Visconti, “A wavelet based method for high frequency subbands watermark Embedding”, Multimedia Systems and Applications III, Vol. 4209, pp. 344-353, 2001

[13] Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering, Vol.4, No. 3, pp. 275-290, 2006

[14] Akhil Pratap Singh and Agya Mishra, “Wavelet Based Watermarking On Digital Image”, Indian Journal of Computer Science and Engineering, Vol. 1, No. 2, pp. 86-91, 2004

[15] Weimin WEI and Yan ZHAO, “Lapped-Biorthogonal-Transform-Based Robust Image Watermarking”, Journal of Computational Information Systems, Vol.6, No.9, pp.2991-2996