Kautilya International Journal of Engineering, Science and Management
Volume - 1 July 2019

High Capacity Embedding And Secured Steganography Model By Using GA And Integer Wavelet Transform

Er. R.L. Yadav[1], Er. Chetan Kumar[2], Er. Raj Yadav[3]
[1] *Associate Professor, Deptt of Computer Science & Engineering, Kautilya Institute of Technolog & Engineering y,Jaipur*
[2] *Associate Professor, Deptt of Computer Science & Engineering, Kautilya Institute of Technolog & Engineering y,Jaipur*
[3] *Software Engineer, Deptt of Computer Science & Engineering, Kautilya Institute of Technolog & Engineering y,Jaipur*

***Abstract*— The proposed system presents a novel approach of building a secure data hiding technique of Steganography using inverse wavelet transform along with Genetic algorithm. The prominent focus of the proposed work is to develop RS-analysis proof design with highest imperceptibility. Optimal Pixel Adjustment process is also adopted to minimize the difference error between the input cover image and the embedded-image and in order to maximize the hiding capacity with low distortions respectively. The analysis is done for mapping function, PSNR, image histogram, and parameters of RS analysis. The simulation results highlights that the proposed security measure basically gives better and optimal results in comparison to prior research work conducted using wavelets and genetic algorithm.**

Keywords- Steganography, Genetic Algorithm, RS-Analysus, Optimal Pixel Adjustment process, PSNR.

I. INTRODUCTION

Steganography is the art of hiding secret information in the form of cover which can be image [1], complex audio[2], video or any sophisticated biometrics formats [3]. Clearly, the goal of cryptography is to protect the content of messages [4], steganography is to hide the existence of messages. An advantage of steganography is that it can be employed to secretly transmit messages without the fact of the transmission being discovered. Generically, the steganography process is classified into two phases in majority of the prior research work e.g. message embedding and extraction. In the embedding operation, a secret message is transformed into a bit stream of bits, which is embedded into the least significant bits (LSBs) [5] of the image pixels. The embedding overwrites the pixel LSB with the message bit if the pixel LSB and message bit do not match. Otherwise, no changes are necessary. For the extraction operation, message bits are retrieved from pixel LSBs and combined to form the secret message. There are two main selection algorithms that can be employed to embed secret message bits: sequential and random. For sequential selection, the locations of pixels used for embedding are selected sequentially—one after another. For instance, pixels are selected from left to right and top to bottom until all message bits are embedded. With random selection, the locations of the pixels used for embedding are permuted and distributed over the whole image. The distribution of the message bits is controlled by a pseudorandom number generator whose seed is a secret shared by the sender and the receiver. This seed is also called the stego-key. The latter selection method provides better security than the former because random selection scatters the image distortion over the whole image, which makes it less perceptible. In addition, the complexity of tracing the selection path for an adversary is increased when random selection is applied. Apart from this, steganographic security can be enhanced by encrypting the secret message before embedding it.

Although there are couple of research being conducted in past [6][7] in the area of steganography, but majority of the prior research work has some or other limitation in terms of imperceptibility. However, the researches conducted in wavelet transform [8][9] and Genetic Algorithm [10] can be considered as benchmark for further extensibility of the existing system. Another research gap in the similar issue is majority of the prior work do not consider robust RS-analysis [11], which is one of the most prominent success factor for steganography application. RS analysis is a special case of Sample pair analysis, which also uses least significant bit modification in order to help calculate an estimated embedding rate. Sample pair analysis [12] deploys finite state machines to classify groups of pixels modified by a given pattern.

In the proposed research paper, we highlight a secure steganography framework is designed where the secret plain text user message is embedded on Integer Wavelet Transform coefficient which is purely based on robust design of genetic algorithm. Then, optimal pixel adjustment process is applied on the obtained embedded image. Every analysis is associated with generation of image histogram and PSNR. Majority of the prior work has used gray scale cover image, whereas the proposed work has considered exclusive colored image from standard image datasets of "*Lena*", "*Baboon*", "*Jet*", and "*Boat.*" Section II highlights about the proposed system along with system architecture and algorithm description. Implementation and result analysis is discussed Section III followed by conclusion in Section IV.

II. PROPOSED SYSTEM

The main purpose of the project work is to establish a highly RS-resistant secure model with novel stegano-algorithm along with implementation of Genetic algorithm and Integer Wavelet Transform to ensure image security and maintain

image quality. The proposed method embeds the message in Discrete Wavelet Transform coefficients based on genetic algorithm and optimal pixel adjustment process algorithm and then applied on the obtained embedded image. As already known, the wavelet transform has the potential to present some information on frequency-time domain simultaneously, where Haar wavelet operates on data by calculating the sums and differences of adjacent elements. The system architecture of the proposed work is as shown in Figure 1 below:

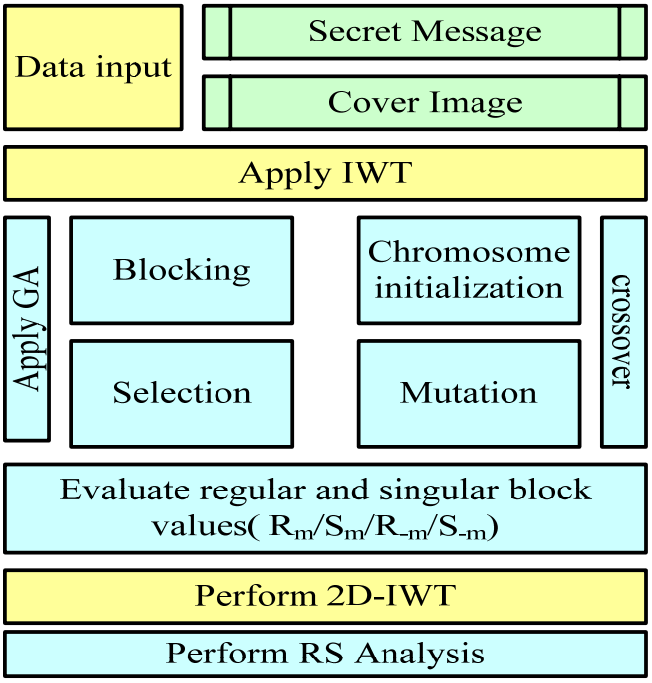


Figure 1: Proposed System Architecture

This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. One nice feature of the Haar wavelet transform is that the transform is equal to its inverse. Each transform computes the data energy in relocated to the top left hand corner.The proposed algorithm employs the wavelet transform coefficients to embed messages into four sub-bands of two dimensional wavelet transform. To avoid problems with floating point precision of the wavelet filters, the proposed system uses Integer Wavelet Transform. This paper embeds the message inside the cover with the least distortion therefore we have to use a mapping function to LSBs of the cover image according to the content of the message. The proposed system also use Genetic Algorithm to find a mapping function for all the image blocks, where various block based techniques can be used to retain local image property and minimize the algorithm complexity compared to single pixel substitution.

The frequency domain representation of the respective created blocks is projected by two dimensional Integer wavelet transform in order to accomplish 4 sub bands LL1, HL1, LH1, and HH1, where 64 genes are generated containing the pixels numbers of each 8x8 blocks as the mapping function. The message bits in 4-LSBs IWT coefficients each pixel according to mapping function are embedded. Based on fitness evaluation, Optimal Pixel Adjustment Process on the Image is applied. Finally, inverse two dimensional integer wavelet transform is computed in this module in order to generate the stego image. Input: The input for this processing is basically a user text message and cover image for embedding purpose. Output: Generation of stego image Inter-component Relationship: This module interacts with all the components of the application responsible for selection of parameters for performing encryption

After embedding the secret message in cover image by LSB. The adjustment is as follows:

Initially, the stego-image is divided into 8 × 8 blocks. Secondly, the blocks are classified and labeled by follow steps:

1. For a modified block B, apply the non-positive flipping F_- and the non-negative flipping F_+ on the block. The flipping mask M_+ and M_- are generated randomly. The result is B'_+ and B'_-.
2. Estimate $f(B'_+)$, $f(B'_-)$ and $f(B)$.
3. Iterate step 1 and 2 1000 times. Define four variables to categorize the blocks by comparison of $f(B'_+)$, $f(B'_-)$ and $f(B)$.

• Estimate P_{+R}, the count of the occurrence when the block is regular under the non-negative flipping.
• Estimate P_{+S}, the count of the occurrence when the block is singular under the nonnegative flipping.
• Estimate P_{-R}, the count of the occurrence when the block is regular under the non-positive flipping.
• Estimate P_{-S}, the count of the occurrence when the block is singular under the non-positive flipping.

4. Compare P_{+R} to P_{+S} and P_{-R} to P_{-S}, and the labels of the block are determined:

• R+, if $P_{+R}/P_{+S} > 1.8$.
• S+, if $P_{+S}/P_{+R} > 1.8$.
• R−, if $P_{-R}/P_{-S} > 1.8$.
• S−, if $P_{-S}/P_{-R} > 1.8$.

5. At last, the blocks are categorized into 4 groups R+R−, R+S−, S +R−, S +S−.

The blocks, which are not included in the 4 categories, are not processed in following steps.

Compared with the original image, the amounts of R + R− and S+R− blocks are increased in the stego-images. This phenomenon can be detected by the RS analysis. The target of the proposed algorithm is to decrease the amount of R− blocks. Therefore genetic algorithm is deployed to adjust them in follow steps:

1. *Initialization*. From the first pixel, select every 3 adjacent pixels in the block as the initial chromosomes C.

2. *Mutation*. Flip the second lowest bits in the chromosomes randomly; the several second generation chromosomes C_i are generated.

3. Selection. Select the best chromosome, which maximize the fitness function (Equation 5), to replace its corresponding initial chromosome.

$Fitness = \alpha(e_1 + e_2) + \text{PNSR}$ α . . . weight

e_1 is the probability of $f(F_{-}(C_i)) < f(C_i)$ and e_2 is the probability of $f(F_{+}(C_i)) > f(C_i)$. PSNR is the peak signal-to-noise ratio of the chromosome. α is the weight decided empirically. The factor α is used to control the weights of the visual quality of the steg-image and the secrecy of the embedded message. For a given α, higher e_1 and e_2 demonstrate a higher security of the stego algorithm. Therefore, we aim at maximizing the value of fitness function. In this step, e_1 and e_2 must be larger than threshold T, which is a decided by the user. The minimum of T is 50%.

4. Calculate P_{-R} and P_{-S} of the adjusted image block. If $P_{-S} > P_{-R}$, the block is successfully adjusted.

5. Crossover. Shift the chromosomes one pixel, go to step 2. If crossover has been applied two times, stop the cycle.

After a block is adjusted, calculate R_m, R_{-m}, S_m and S_{-m} of the image. If the difference between R_m and R_{-m} is more than 5%, or the difference between S_m and S_{-m} is more than 5%, adjust the next block. In the proposed technique, the blocks are labeled before the adjustment. Thus, the computational complexity is reduced. The usage of the genetic method avoids the exhausting searching and the algorithm is easy to be implemented.

III. PERFORMANCE ANALYSIS

The proposed implementation of RS-analysis using genetic algorithm for the robust security in Steganographic application is done on standard 32-bit windows OS with minimum of 1.84 GHz processor and 2 GB RAM. The proposed method is applied on 512x512 8-bit grayscale images "Jet", "Boat", "Baboon" and "Lena" as shown in Figure 2.

a) Jet(JPG, 512x512)

b)Boat(JPG, 512x512)

c) Baboon (JPG, 512x512)

d) Lena (JPG, 512x512)

Figure 2: Datasets of Jet, Boat, Baboon, and Lena

As the proposed work is done on 4 set of data image, therefore their respective accomplished results of RS-analysis are as follows:

Table 1: RS-analysis for Jet

For Jet	Initial Value	After Embedding	OPAP
R_m-R_{-m}	0.0017043	0.026925	0.00078363
S_m-S_{-m}	0.0044596	0.025877	0.0070058

Table 2: RS-analysis for Boat

For Boat	Initial Value	After Embedding	OPAP
R_m-R_{-m}	0.0035762	0.030281	0.0034139
S_m-S_{-m}	0.006262	0.033195	0.0032035

Table 3: RS-analysis for Baboon

For Baboon	Initial Value	After Embedding	OPAP
R_m-R_{-m}	0.0073893	0.028737	0.0043453
S_m-S_{-m}	0.0047449	0.030666	0.0016398

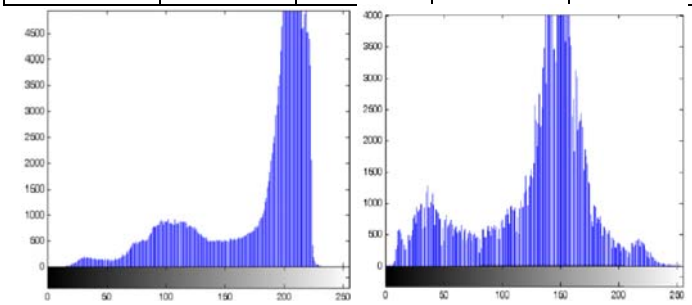
Table 4: RS-analysis for Lena

For Lena	Initial Value	After Embedding	OPAP
R_m-R_{-m}	0.0036152	0.026464	0.0029631
S_m-S_{-m}	0.0055441	0.03023	0.0084601

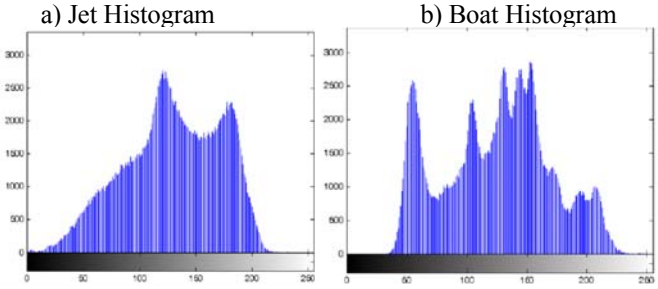
The tables 1-4 are shown for the values of $|R_m\text{-}R_{-m}|$ and $|S_m\text{-}S_{-m}|$ that represents the RS-steganalysis on regular and singular block. It can be easily seen that the value of $|R_m\text{-}R_{-m}|$ and $|S_m\text{-}S_{-m}|$ increases from initial value before embedding and after embedding that exhibits a strong correlation in potential of RS-analysis and designed module. Table 5 shows the stego image quality by PSNR. Human visual system is unable to distinguish the grayscale images with PSNR more than 36 dB. This project embedded the messages in the k-LSBs, from k=3 to k=6 and received a reasonable PSNR. Table 5 shows PSNR for variant value of k. Table 5 presents the results and we can see that for k equal to 4 or 5, we obtain the highest hiding capacity and reasonable visual quality. Therefore, we take k equal to 4 as the number of bits per pixel.

Table 5: Comparison of PSNR of Images for variant value of K

Cover Image	PSNR			
	K=3	K=4	K=5	K=6
Lena	46.83	39.94	32.04	24.69
Jet	51.88	45.20	37.45	29.31
Boat	48.41	40.44	31.17	23.60
Baboon	47.32	40.34	32.79	24.80



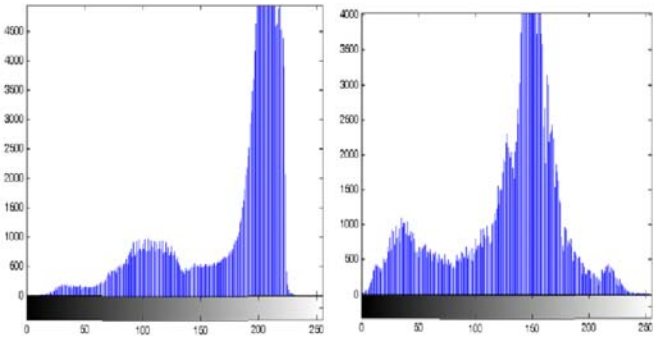
a) Jet Histogram b) Boat Histogram



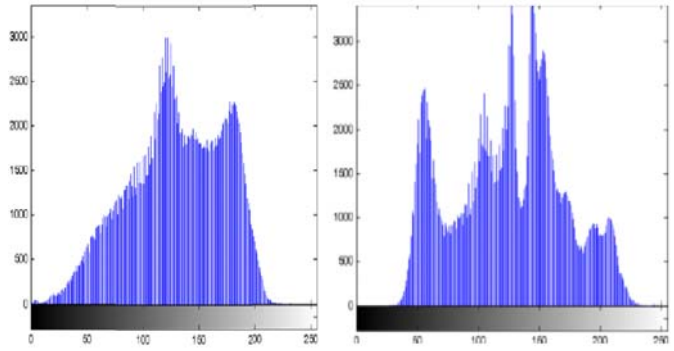
c) Baboon Histogram d) Lena Histogram

Figure 3: Histograms of the Cover Images

Figure 3 shows that images for k equal to 4 that there is no significant change in the stego-image histogram for 4-LSBs images, thus it is robust against any statistic attack.

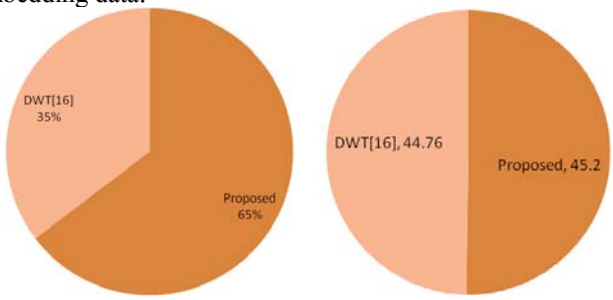


a) Jet Histogram b) Boat Histogram



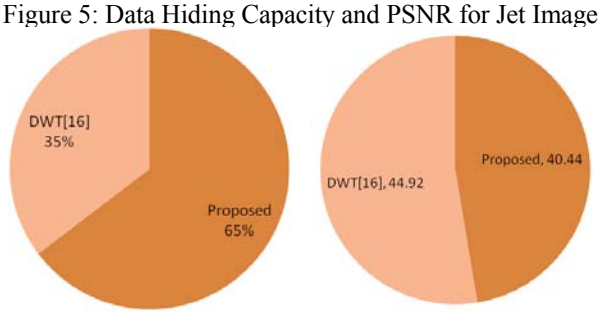
c) Baboon Histogram d) Lena Histogram

Figure 4: Output Histogram for Stego image of k=4 for embedding data.



Data Hiding Capacity PSNR (dB)

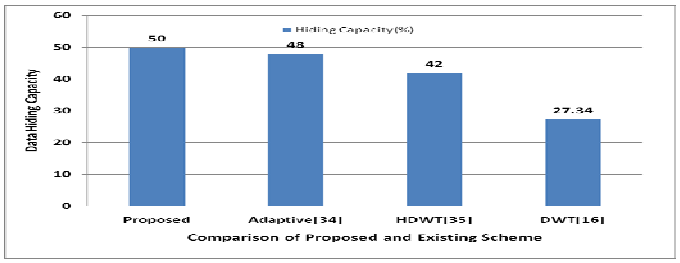
Figure 5: Data Hiding Capacity and PSNR for Jet Image



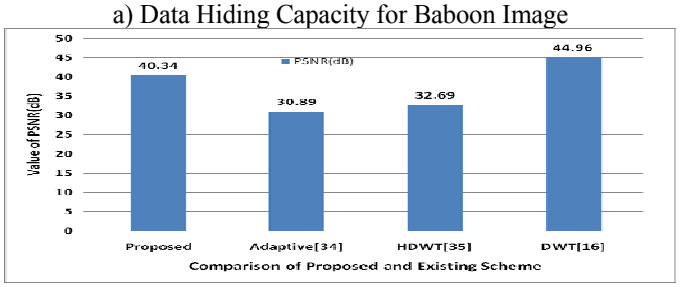
Data Hiding Capacity PSNR(dB)

Figure 6: Data Hiding Capacity and PSNR for Boat Image

It can be seen that the proposed work considering Jet Image and Boat image is only compared with work done by DWT [16]. The basic reason behind this is that other comparative techniques that use adaptive [17] and HDWT [18] is already tested in many prior research works. Hence the past research work is missing for the evaluation of work done in [16] when it is applicable in the current study. It can be obviously seen that proposed research work has better data hiding scheme and better accomplishment of PSNR value when experimented with Jet and Boat images. The other results are as follows:

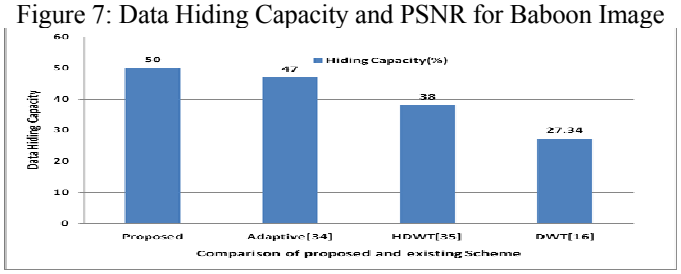


a) Data Hiding Capacity for Baboon Image

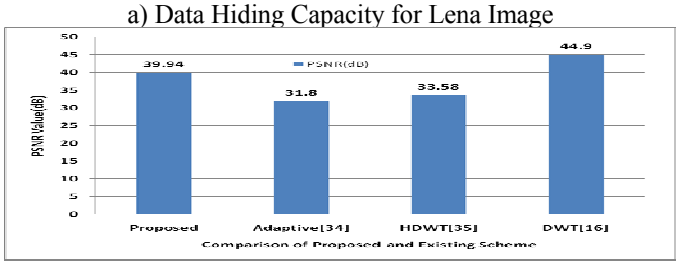


b) PSNR (dB) for Baboon Image

Figure 7: Data Hiding Capacity and PSNR for Baboon Image



a) Data Hiding Capacity for Lena Image



b) PSNR(dB) for Lena Image

Figure 8: Data Hiding Capacity and PSNR for Lena Image

Figure 5 and 6 highlights the comparison for proposed scheme and work done on DWT [16] using Jet and Boat Image. Figure 7 and 8 highlights the comparison of hiding capacity achieved and the obtained PSNR between our proposed method and methods in [17], [16] and [18]. Hence, it can be seen that the proposed system has better performance in compared to majority of the Steganographic techniques using wavelets or any evolutionary algorithms.

IV. CONCLUSION

The proposed system has highlighted a novel technique of data hiding up to 65% on images using Inverse Wavelet Transform as well as genetic algorithm. Conducting RS-analysis and minimizing R_ blocks using genetic algorithm has shown an optimal result for our proposed system. However, there are certain limitations to the proposed system also. The proposed project work is a semantic oriented security design which is experimented on single computer system. Real time deployment on computer network will be the first constraint thereafter. The data hiding technique is restricted to only image, whereas video, speech and other biometrics are out of scope. Bulk Steganographic is not performed. However, our future work will be on addressing the above mentioned issues.

V. REFERENCES

[1] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in HS Venter, JHP Eloff, L Labuschagne and MM Eloff (eds), *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, June/July 2005 (Published electronically)

[2] R Sridevi, Dr. A Damodaram, Dr. SVL.NARASIMHAM, efficient method of audio steganography by modified lsb algorithm and strong encryption key with enhanced security, Journal of Theoretical and Applied Information Technology, 2009

[3] Chander Kant, Rajender Nath, Sheetal Chaudhary, Biometrics Security using Steganography, International Journal of Security, Volume (2) : Issue (1), 2008

[4] Domenico Bloisi and Luca Iocchi, Image based steganography and cryptography, International Journal of Computer Applications, 2010

[5] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy, Implementation of LSB Steganography and its Evaluation for Various File Formats, Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05, Pages: 868-872 (2011)

[6] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, A Survey on Image Steganography and Steganalysis, Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 2, April 2011

[7] A. Joseph Raphael, Dr. V. Sundaram, Cryptography and Steganography – A Survey, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630, ISSN:2229- 6093, 2010

[8] Amitava Nag, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, A Novel Technique for Image Steganography Based on DWT and Huffman Encoding, International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6), 2011

[9] H S Manjunatha Reddy, K B Raja, High capacity and security steganography using discrete wavelet transform, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6), 2011

[10] Amin Milani Fard, Mohammad-R. Akbarzadeh, Farshad Varasteh, A New Genetic Algorithm Approach for Secure JPEG Steganography, Engineering of Intelligent Systems, IEEE International Conference, 2006

[11] Yun Q. Shi, Hyoung Joong Kim, Digital Watermarking, 6th International Workshop, IWDW 2007 Guangzhou, China, December 3-5, 2007, Proceedings Springer, 2008

[12] Shreelekshmi R, M Wilscy and M Wilscy, Preprocessing Cover Images for More Secure LSB Steganography, International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010

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

[17] El Safy, R.O. Zayed, H.H. El Dessouki, A. , An adaptive steganographic technique based on integer wavelet transform, Networking and Media Convergence, 2009. ICNM. International Conference, 2009

[18] Bo-Luen Lai and Long-Wen Chang, Adaptive Data Hiding for Images Based on Harr Discrete Wavelet Transform, Lecture Notes in Computer Science, 2006, Volume 4319/2006, 1085-1093, DOI: 10.1007/11949534_109