Empirical Computation Of Rs-Analysis For Building Robust Steganography Using Integer Wavelet Transform And Genetic Algorithm

Shamimunnisabi[#1], Cauvery N.K[*2]
Shamimunnisabi
Department of CSE, R.V.C.E., Bangalore, India
Cauvery N.K
Department of CSE, R.V.C.E., Bangalore, India

***Abstract*— The proposed system presents a novel approach of building a secure data hiding technique of Steganography using Integer Wavelet Transform along with Genetic Algorithm. The prominent focus of the proposed work is to develop Resistant Secure-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, Peak Signal to Noise Ratio, image histogram, and parameters of RS analysis. The implementation 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-component; Steganography, Genetic Algorithm, Resistant Secure-Analysus, Optimal Pixel Adjustment Process, Peak Signal to Noise Ratio.

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 researches 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, 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 the 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 an overview of related work which identifies all the major research work being done in this area. Section III highlights the proposed system along with the system architecture and algorithm description. Implementation and result analysis is discussed in Section IV followed by conclusion in Section V.

II. RELATED WORK

Taras Holotyak e.t. al [13] propose a new method for estimation of the number of embedding changes for non-adaptive ±k embedding in images. The similar author [14] has also advocate a new approach to blind steganalysis based on classifying higher-order statistical features derived from an estimation of the stego signal in the wavelet domain.

Agaian and Perez [15] propose a new steganographic approach for palette-based images. This new method has the advantage of embedding secure data, within the index, or the palette or both, using special sorting scheme. The presented technique also incorporates the use of color model and cover image measures in order to select the best of the candidates for the insertion of the stego information.

Chen and Lin [16] propose a new steganography technique which embeds the secret messages in frequency domain to show that the PSNR is still a satisfactory value even the highest capacity case is applied. According to the simulation results, the PSNR is still a satisfactory value even the highest capacity case is applied. This is due to the different characteristics of Discrete Wavelet Transform (DWT) coefficients in different sub-bands. Since the most essential portion (the low frequency part) is kept unchanged while the secret messages are embedded in the high frequency sub-bands (corresponding to the edges portion of the original image), better PSNR is not a surprising result. Furthermore, respectable security is maintained as well since no message can be extracted without the "Key matrix" and decoding rules.

Kathryn Hempstalk [17] investigates using the cover's original information to avoid making marks on the stego-object, by hiding raw electronic files inside digital colour images. This paper has introduced two new techniques for image steganography, FilterFirst and BattleSteg. These two techniques attempt to improve on the effectiveness of the hiding by using edge detection filters to produce better steganography.

Wang and Moulin [18] showed that the independently and identically distributed unit exponential distribution model is not a sufficiently accurate description of the statistics of the normalized periodogram of the full-frame 2-D image Discrete Fourier Transform (DFT) coefficients.

Park e.t. al [19] propose a new image steganography method to verify whether the secret information had been deleted, forged or changed by attackers. The proposed method hides secret information into spatial domain of digital image. In this paper, the integrity is verified from extracted secret information using the approximate coefficients of the Discrete Cosine Transform (DCT) domain.

Ramani, Prasad, and Varadarajan [20] propose an image steganography system, in which the data hiding (embedding) is realized in bit planes of subband wavelets coefficients obtained by using the Integer Wavelet Transform (IWT) and Bit-Plane Complexity Segmentation Steganography (BPCS).

Farhan and Abdul [21] has presented their work in message concealment techniques using image based steganography. Anindya e.t. al [22] present further extensions of yet another steganographic scheme (YASS), a method based on embedding data in randomized locations so as to resist blind steganalysis. YASS is a JPEG steganographic technique that hides data in the Discrete Cosine Transform (DCT) coefficients of randomly chosen image blocks.

Adnan Gutub e.t. al. [23] merge between the ideas from the random pixel manipulation methods and the stego-key ones to propose our work, which uses the least two significant bits of one of the channels to indicate existence of data in the other two channels. This work showed attractive results especially in the capacity of the data-bits to be hidden with relation to the RGB image pixels.

Mohammed and Aman [24] uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. Aasma Ghani Memon e.t. al. [25] provides a new horizon for safe communication through XML steganography on Internet.

Zaidan e.t. a.l. [26] has presented a model for protection of executable files by securing cover-file without limitation of hidden data size using computation between cryptography and steganography.

Vinay Kumar and Muttoo [27] has discussed that graph theoretic approach to steganography in an image as cover object helps in retaining all bits that participate in the color palette of image.

Wang e.t. al. [28] presents a new steganography based on Genetic Algorithm and LSB. Souvik Bhattacharyya and Gautam Sanyal [29] propose a novel steganographic method for hiding

information in the transform domain of the gray scale image. The proposed approach works by converting the gray level image in transform domain using Discrete Integer Wavelet technique through lifting scheme.

Nadia M. Mohammed [30] has presented four new methods in steganography systems to embed secret data in compressed images. Two methods are working in spatial domain, known as moving window and odd/even LSB, others are working in transform domain, known as odd/even DCT and DCT+DWT.

Zaidan e.t. al.[31] has proposed a multi-cover steganography using remote sensing image. Shaamala e.t. al. [32] has studied the effect DCT and DWT domains on the imperceptibility and robustness of Genetic watermarking. Results of watermark image quality and attacks based on Peak Signal-to-Noise Ratio (PSNR) Numerical Correlation (NC) is analyzed, and the DWT results showed more robustness high imperceptibility than DCT in watermarking based on GA. Shiva Kumar e.t. al [33] propose Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques (PCRSMT). The cover image is divided into 64 blocks of 4*4 each and DWT is applied to each block. The resulting 64 blocks of vertical band of 2x2 each are isolated and IWT is applied to get 1x1 blocks. The DWT and IWT are applied to payload and IWT coefficients of payload are embedded with that of cover image. IDWT and IIWT are applied to derive stego image. In addition error detection and correction technique is also applied to ensure more secured communication. It is observed that the robustness and capacity are improved with very little tradeoffs in PSNR.

III. 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 Integer Wavelet Transform coefficients based on Genetic Algorithm and Optimal Pixel Adjustment Process algorithm and then applied on the obtained embedded image. The system architecture of the proposed work is as shown in Fig.1 below:

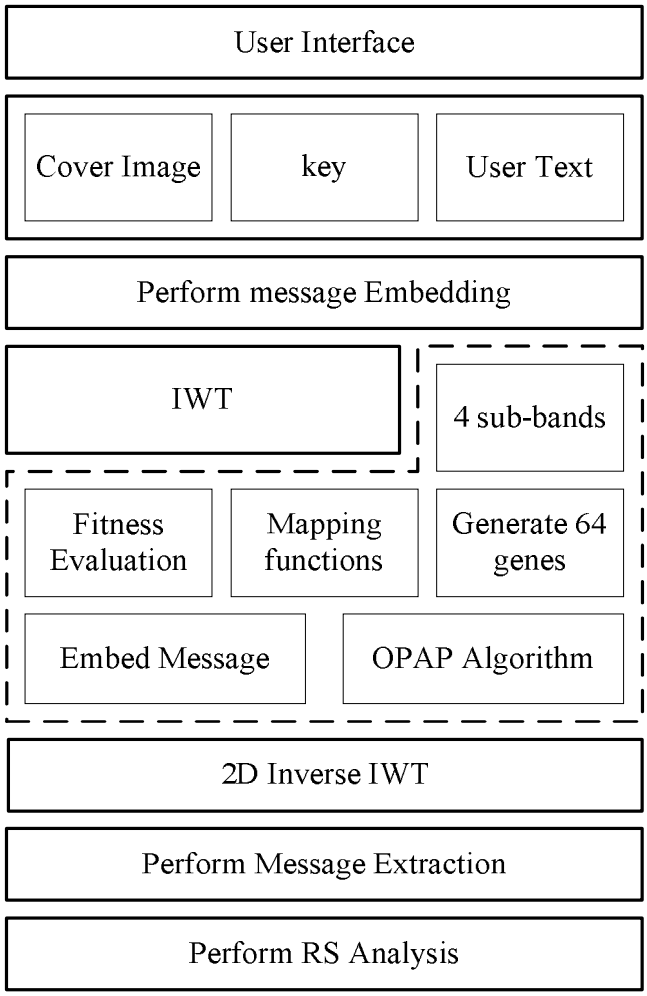


Fig.1 Proposed System Architecture

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. 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 subbands of two dimensional wavelet transform. To avoid problems with floating point precision of the wavelet filters, the proposed system uses Integer Wavelet Transform. The proposed method 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 uses 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 embedding process of the proposed system is shown in Fig.2.

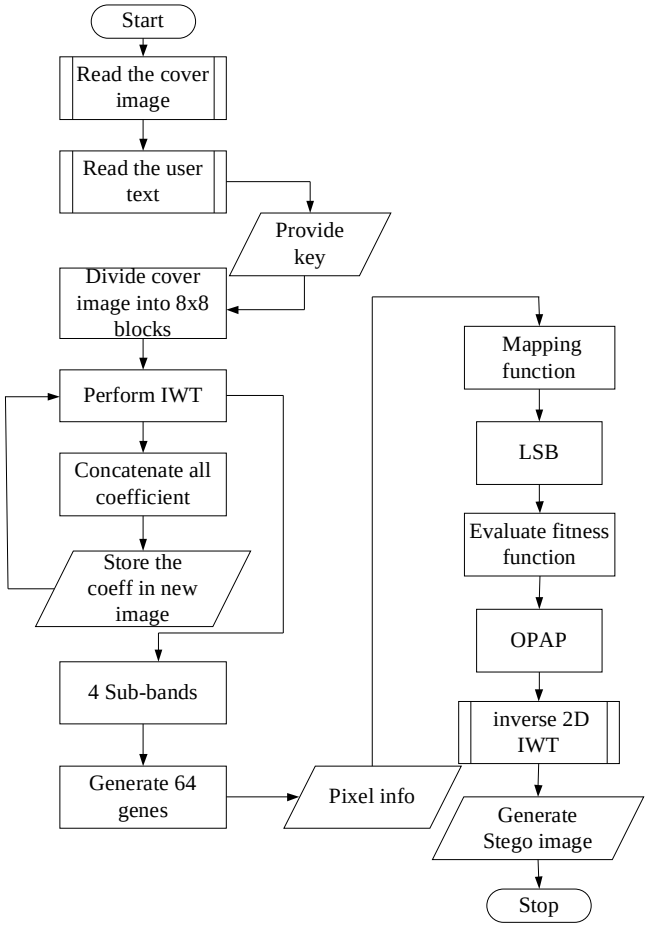


Fig.2 Proposed Message Embedding Scheme

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 pixel numbers of each 8x8 blocks as the mapping function. The message bits in 4-LSBs IWT coefficients of 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 Intercomponent Relationship: This module interacts with all the components of the application responsible for selection of parameters for performing encryption. The extraction process is as shown in Fig.3.

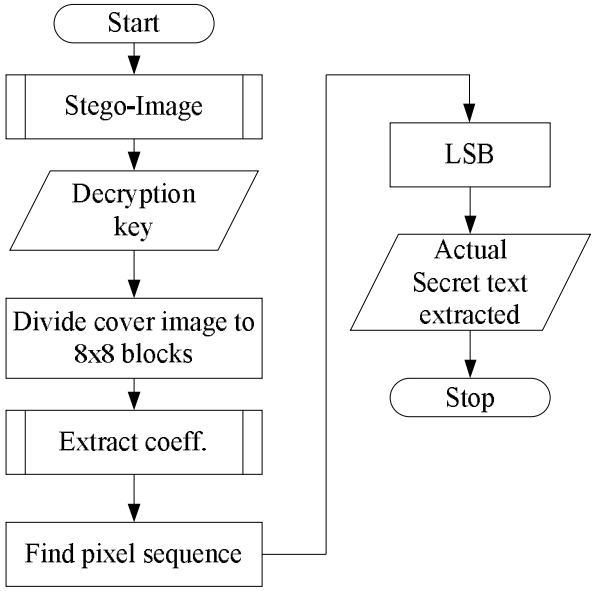


Fig.3 Proposed Message Extraction Scheme

The respective algorithm descriptions are as follows:

Algorithm: Message Embedding

Input: Colored Image, User Plain Text, key

Output: Stego-Image

Steps:

Step1. *Perform Integer wavelet transform using lifting scheme*

Step2. *Start from the Haar wavelet and get the corresponding lifting scheme*

Step3. *Add primal ELS to the lifting scheme.*

Step4. *Perform integer LWT of the same image.*

Step5. *Divide image in 8 x 8 blocks and perform IWT on each block.*

Step6. *Find the frequency domain representation of blocks by 2D Integer Wavelet Transform.*

Step7. *Obtain the size of the image.*

Step8. *Generate 64 genes containing the pixels numbers of each 8x8 blocks as the mapping function.*

Step9. *Initialize empty matrix to store the wavelet values.*

Step10. *Obtain 8 x 8 blocks for R G B*

Step11. *Perform IWT*

Step12. *Concatenate all coefficients together*

Step13. *Store the coefficients in new image*

Step14. *Embed in 4-LSBs IWT coefficients of each pixel according to mapping function.*

Step15. *Save the transformed image*

Step16. *Fitness evaluation is performed to select the best mapping function.*

Step17. *Calculate embedded capacity.*

Step18. *Apply Optimal Pixel Adjustment Process on the image.*

Step19. *Convert image to binary.*

Step20. *Calculate inverse 2D-IWT on each 8x8 block.*

Algorithm: Message Extraction

Input: Stego-Image, key

Output: Original Secret Message

Steps:

Step1. *Divide the cover image into 8x8 blocks.*

Step2. *Extract the transform domain coefficient by 2D IWT of each 8x8 block.*

Step3. *Employ the obtained mapping function in the embedding phase.*

Step4. *Fmd the pixel sequences for extracting.*

Step5. *Extract 4-LSBs in each pixel.*

Algorithm: RS-Analysis

Input: Stego- Image

Output: Perform comparative RS-Analysis

Steps:

Step1. *Create function for non-positive flipping*

Step2. *Create function for non-negative flipping*

Step3. *Change LSB as per flipping*

Step4. *Initialize Relative number of regular block after positive flipping (Rm) = 0;*

Step5. *Initialize Relative number of Singular block after positive flipping (Sm) = 0;*

Step6. *Divide Stego Image into 8 x 8 blocks*

Step7. *Apply the non-positive flipping (Fn)*

Step8. *Apply the non-negative flipping (Fp)*

Step9. *Calculate cumulative correlation (c)*

Step10. *Calculate correlation for non-positive flipping (Cn)*

Step11. *Calculate correlation for non-negative flipping (Cp)*

Step12. *Iterate the step 7 to step10 to 1000 times.*

Step13. *Compute the count of occurrence for block is regular under non-negative flipping (ppr)*

Step14. *Compute the count of occurrence for block is singular under non-negative flipping (pps)*

Step15. *Compute the count of occurrence for block is regular under non-positive flipping (pnr)*

Step16. *Compute the count of occurrence for block is singular under non-positive flipping (pns)*

Step17. *If Cn>C*

Pnr = Pnr +1

Else

Pns = Pns+1

Step18. If Cp>C

Ppr = Ppr+1

Else

Pps = Pps+1

Step19. *If Ppr/Pps>1.8*

str = 'R+';

Rp = Rp+1;

Step20. *If Pps/Ppr>1.8*

str = 'S+'

Sp = Sp+1;

Step21. *If Pnr/Pns>1.8*

str = 'R-'

Rm = Rm+1

Step22. *If Pns/Pnr>1.8*

str = 'S-'

Sm = Sm+1

Step23. *Classify the blocks into 4 groups (R+R-), (R+S-), (S+R-), and (S+S-)*

Step24. *Reject the block which doesn't fall in Step 23.*

Step25. *Use genetic Algorithm for minimizing R- block.*

[NOTE: Compared with the original image, the amounts of R + R- and S + R- blocks are increased in the steg-images. This phenomenon can be detected by the RS analysis. The target of our algorithm is to decrease the amount of R- blocks. Genetic Algorithm will be used to adjust them]

Algorithm: Minimizing R- blocks using Genetic Algorithm

Input: Stego-Image, Alpha value

Output: Minimization of R- block

Steps:

Step1. *Perform Chromosome Initialization Steps.*

Step2.*Select every 3 adjacent pixels in the block*

Step3. *Initialize maximum Fitness as 0*

Step4. *Initialize Alpha as 0.88*

//The factor alpha is used to control the weights of the visual quality of the steg-image and the secrecy of the embedded message.

Step5. *Flip second lowest bit randomly for number of time*

Step6. *For kk = 1: length (Block)-2*

Chrom = Block (kk: kk+2);

Cp = non_negative_flipping(Chrom);

Cn = non_positive_flipping(Chrom);

Step7. *Initialize e1 and e2 as 0*

Step8. *Compute Correlation (C, Cn, and Cp)*

Step9. *If Cn<C*

e1 = 1;

End

Step10. *If Cp > C*

e2 = 1;

End

Step11. *Apply PSNR = SNR (Chrom-Cn);* // See step6

Step12. *Apply FITNESS = alpha*(e1+e2) +PSNR*

Step13. *If fitness>maxfitness*

maxfitness = fitness;

Chrommax = Cp;

crossover = crossover+1;

End

Step14. *Replace chromosome with new one*

Step15. *Compute pns and pnr*

Step16. *If Pns>Pnr* //See Step15-16 of previous algorithm

Block is successfully adjusted

End

Step17. *If crossover < 2*

Shift the chromosome one pixel and repeat step 5 to 16

End

Step18. *Compute difference, diff1 = Ppr-Pnr*

Step19. *Compute difference, diff2 = Pps - Pns*

Step20. *If diff1>0.05*diff2*

Adjust the next block

End

IV. Implementation and Result Analysis

The proposed method is applied on 512x512 24-bit color images "Jet", "Boat", "Baboon" and "Lena". The messages are generated randomly with the same length as the maximum hiding capacity. Table I shows the stego image quality by PSNR. The proposed system embedded the messages in the k-LSBs, from k=3 to k=6 and received a reasonable PSNR. Table I shows PSNR for variant value of k. Table I 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, the proposed method takes k equal to 4 as the number of bits per pixel.

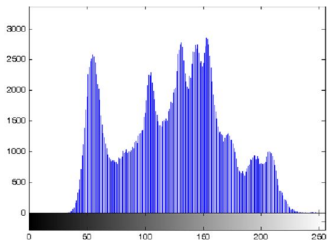
TABLE I

COMPARISON OF PSNR OF IMAGES FOR VARIANT VALUE OF K

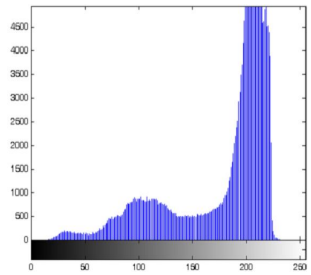
Cover	PSNR (dB)

Image	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

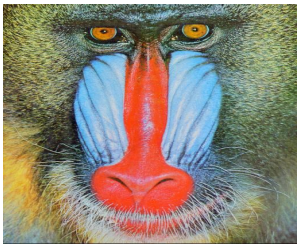
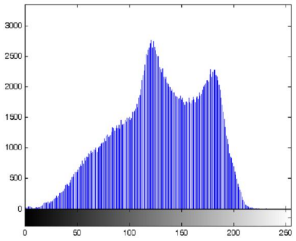
The results are as followings:

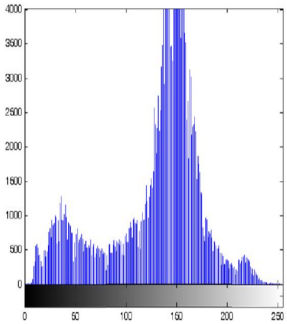
a) Lena Cover image b) Lena Histogram

c) Jet Cover image d) Jet Histogram

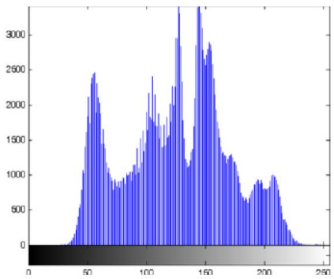
e) Baboon Cover image f) Baboon Histogram

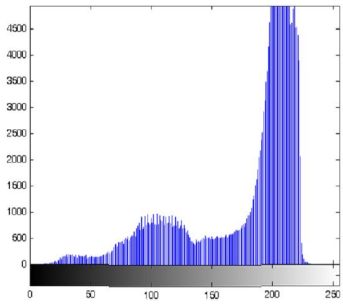
g) Boat Cover image b) Boat Histogram

Fig.4. Four Cover images used in system implementation testing and their corresponding histogram

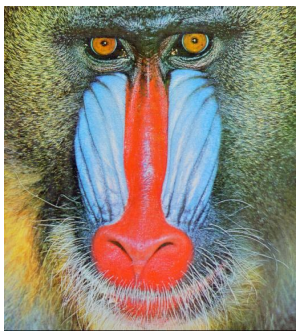
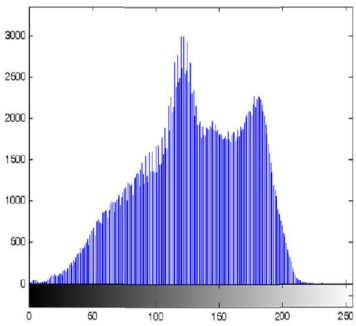
Fig.4 shows that images for k equal to 4 that there is no significant change in the stego image histogram for 4-LSBs images, thus it is robust against any statistic attack.

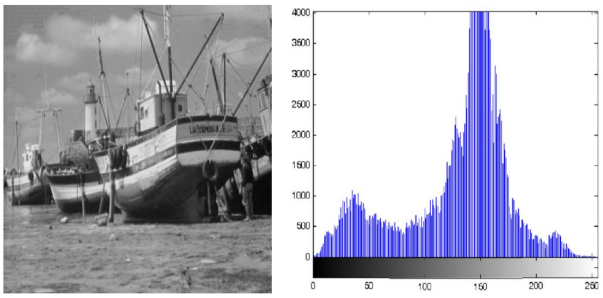
a) Lena Cover image b) Lena Histogram

c) Jet Cover image d) Jet Histogram

e) Baboon Cover image f) Baboon Histogram



g) Boat Cover image b) Boat Histogram

Fig.5. Output Stego image of k=4 for embedding data and their corresponding histograms.

TABLE II

COMPARISON OF HIDING CAPACITY ACHIEVED AND THE OBTAINED PSNR BETWEEN PROPOSED METHOD AND METHODS IN [34], [16] AND [35]

Cover image	Method Used	Hiding Capacity (bits)	Hiding Capacity (%)	PSNR (dB)
Lena	Proposed Method	1048576	50%	39.94
	Adaptive [34]	986408	47%	31.8
	HDWT[35]	801842	38%	33.58
	DWT [16]	573550	27.34%	44.90
Baboon	Proposed Method	1048576	50%	40.34
	Adaptive [34]	1008593	48%	30.89
	HDWT[35]	883220	42%	32.69
	DWT [16]	573392	27.34%	44.96
Jet	Proposed Method	1048576	50%	45.20
	DWT [16]	573206	27.33%	44.76
Boat	Proposed Method	1048576	50%	40.44
	DWT [16]	573318	27.33%	44.92

Hence, it can be seen that the proposed system has better performance in comparison to majority of the steganography techniques using wavelets or any evolutionary algorithms such as Adaptive, HDWT, and DWT. The most important aspect of the proposed method is that during RS-analysis the detect-ability of hiding capacity is not identified irrespective of having higher PSNR value.

V. CONCLUSION

The proposed system has highlighted a novel technique of data hiding on images using Integer Wavelet Transform as well as Genetic Algorithm. The proposed system has shown an optimal result by conducting RS-analysis and minimizing R. blocks using Genetic Algorithm. However, there are certain limitations to the proposed system also. The proposed 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.

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

[13] Taras Holotyak, Jessica Fridrich, and David Soukal, Stochastic Approach to Secret Message Length Estimation in ±k Embedding Steganography, Communications and Multimedia Security 2005

[14] Taras Holotyak, Jessica Fridrich, Sviatoslav Voloshynovskiy, Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics, Communications and Multimedia Security 2005

[15] Sos S. Agaian and Juan P. Perez, New Pixel Sorting Method For Palette Based Steganography And Color Model Selection, 2004

[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] Kathryn Hempstalk, Hiding Behind Corners: Using Edges in Images for Better Steganography, 2006

[18] Ying Wang and Pierre Moulin, Statistical Modelling and Steganalysis of DFT-Based Image Steganography, Proc. of SPIE Electronic Imaging, 2006

[19] Youngran Park, Hyunho Kang, Kazuhiko Yamaguchi, and Kingo Kobayashi, Integrity Verification of Secret Information in Image Steganography, The 29th Symposium on Information Theory and its Applications (SITA2006), Hakodate, Hokkaido, Japan, Nov. 28 { Dec. 1, 2006

[20] Ms. K. Ramani Dr. E. V. Prasad Dr. S. Varadarajan, Steganography using bpcs to the integer wavelet transformed image, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7, July 2007

[21] Farhan Khan and Adnan Abdul-Aziz Gutub, Message Concealment Techniques using Image based Steganography, *The 4th IEEE GCC Conference and Exhibition*, Gulf International Convention Centre, Manamah, Bahrain, 11-14 November 2007.

[22] Anindya Sarkary, Kaushal Solankiyy and B. S. Manjunathy, Further Study on YASS: Steganography Based on Randomized Embedding to Resist Blind Steganalysis, Proc. SPIE - Security, Steganography, and Watermarking of Multimedia Contents (X), San Jose, California, Jan. 2008.

[23] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi, Pixel indicator high capacity technique for RGB image based steganography, WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008

[24] Mohammad Ali Bani Younes and Aman Jantan, A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008

[25] Aasma Ghani Memon, Sumbul Khawaja and Asadullah Shah, STEGANOGRAPHY: A new horizon for safe communication through XML, Journal of Theoretical and Applied Information Technology, 2008

[26] A.A.Zaidan, Fazidah.Othman, B.B.Zaidan , R.Z.Raji, Ahmed.K.Hasan, and A.W.Naji, Securing Cover-File Without Limitation of Hidden Data Size Using Computation Between Cryptography and Steganography, Proceedings of the World Congress on Engineering 2009 Vol I WCE 2009, July 1 - 3, 2009, London, U.K.

[27] Vinay Kumar, S. K. Muttoo, Principle of Graph Theoretic Approach to Digital Steganography, Proceedings of the 3rd National Conference; INDIACom-2009

[28] Shen Wang, Bian Yang and Xiamu Niu, A Secure Steganography Method based on Genetic Algorithm, Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 1, January 2010

[29] Souvik Bhattacharyya and Gautam Sanyal, Data Hiding in Images in Discrete Wavelet Domain Using PMM, World Academy of Science, Engineering and Technology 68 2010

[30] Nadia M. Mohammed, Multistage Hiding Image Techniques, Raf. J. of Comp. & Math's. , Vol. 7, No. 2, 2010

[31] A. A. Zaidan, B. B. Zaidan, Y. Alaa Taqa, M. Kanar Sami, Gazi Mahabubul Alam and A. Hamid Jalab, Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem, International Journal of the Physical Sciences Vol. 5(11), pp. 1776-1786, 18 September, 2010

[32] Abduljabbar Shaamala, Shahidan M. Abdullah and Azizah A. Manaf, Study of the effect DCT and DWT domains on the imperceptibility and robustness of Genetic watermarking, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011

[33] K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattnaik, Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques, Int. J. Comp. Tech. Appl., Vol 2 (4), 1035-1047, IJCTA | July-August 2011

[34] 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

[35] 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