Steganography Scheme Against RS Attack Enriched with Evolutionary Programming(AGA) and OPAP

Neha saxena
M. Tech scholar
Suresh Gyan Vihar University

Sandeep Bhargava
Assistant Professor
Suresh Gyan Vihar University

Abstract: **- Steganography refers to the technique of hiding secret messages into media such as text, audio, image and video without any suspicion, while steganalysis is the art and science of detection of the presence of steganography. It can be used for the benefit of the mankind to serve us as well as by terrorists and criminals for malicious purposes. Both steganography and steganalysis have received a lot of attention from law enforcement and media. In the past, different steganographic techniques with properties of imperceptibility, undetectability, robustness and capacity have been proposed. Newer and more sophisticated steganographic techniques for embedding secret message will require more powerful steganalysis methods for detection. The battle between steganography and steganalysis is never ending. In this paper, we are hiding data using evolutionary computing technique that is enriched with OPAP to enhance the picture quality. Evolutionary techniques are used to increase the robustness of the program and steganalysis techniques are proposed against RS attack.**

I. SYSTEM ARCHITECTURE

In this work the message has been embedded on Integer Wavelet Transform (IWT) coefficient using Evolutionay algorithm (EVOLUTIONAY ALGORITHM). Further, to obtain the embedded image OPAP algorithm is applied. In EVOLUTIONAY ALGORITHM method a chromosome is encoded by doing permutation from 1-64 that point to pixel numbers in each array. It is used to search for the best adjustment matrix. The main aim to apply OPAP is to minimize the error between cover and stego image.

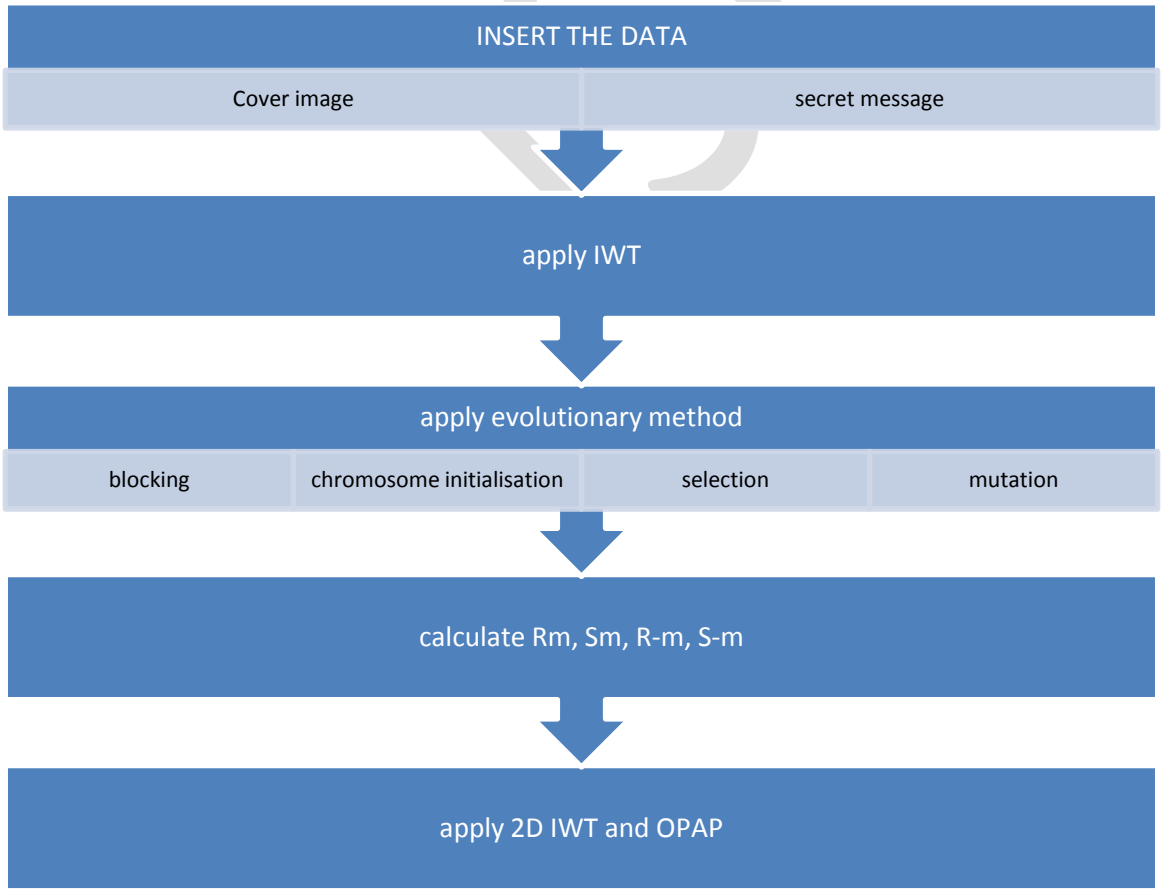


Fig (i) System Architecture of the proposed research

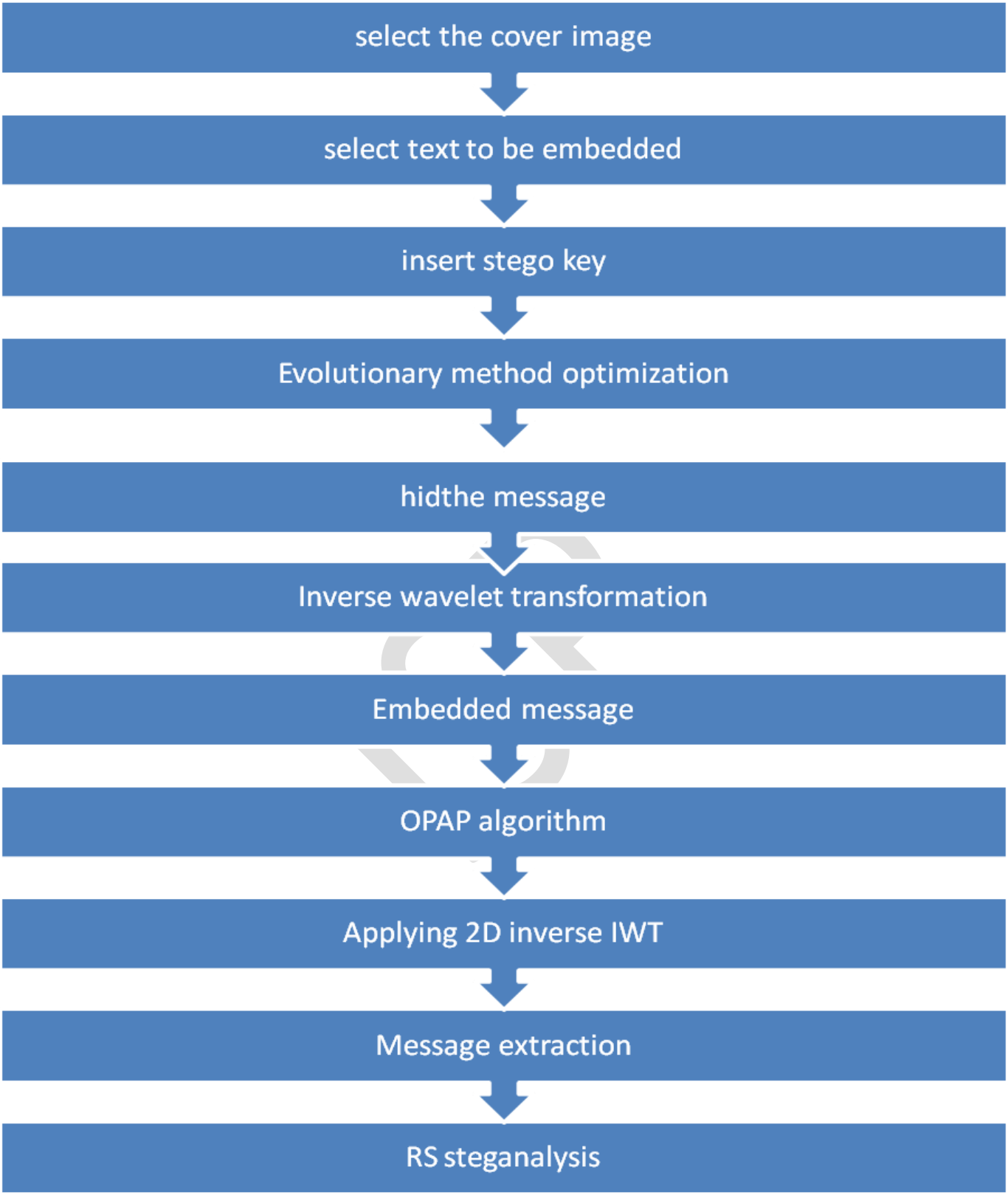


Fig (ii): The overall functional flow diagram

The above mentioned figure represents the overall system functionalities of the developed algorithm. The overall system function can be summarized by observing the figure mentioned above. The figure represents the real operative steps of the developed design. In the processing the user interface helps so as to

provide a user interface to handle the developed model and to access the developed module. At the inception, the cover image is selected where the data is to be embedded. Once the cover image has been selected then the text data or the message is to be selected and then in order to accomplish the motive of Steganography the stego key is assigned so that at the other terminal the data can be retrieved by putting the key. Once the Key has been provided, the real application development for the RS analysis will be started with the help of robust EVOLUTIONAY ALGORITHM optimization. In this technique initially the message is to be embedded. Here the EVOLUTIONAY ALGORITHM is playing a vital role for embedding more and more data to the image. In this developed system architecture the integer to integer wavelet transform has been done. Once the data has been embedded into the image file, then after embedding the image is evolutionay algorithmin recovered and then it is now ready to be transmitted over the communication channel. On the other hand at the receiver terminal or the extraction terminal with the accurate assignment of the stego key the data is retrieved accurately.

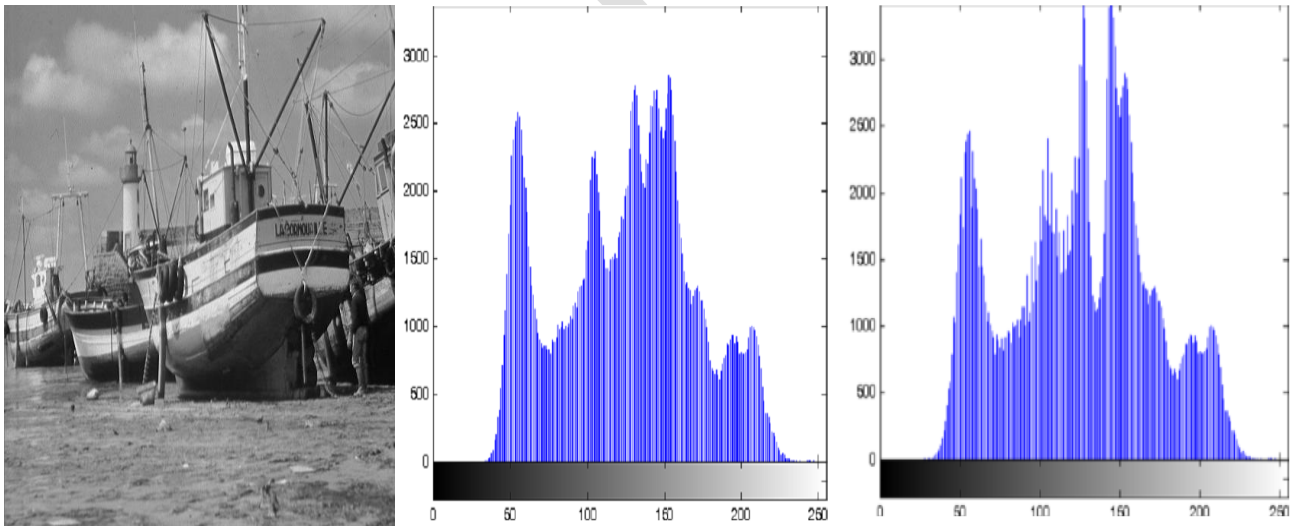
II. EXPERIMENTAL SCENARIO

The recommended method is applied on the images of 512x512 size and each of 8 bit in the format of grayscale, images that are used is “ship”, ”koala”, ”chrysanthemum” and ”penguins”. Then the generation of messages are started randomly and length is same of each message according to the maximum capacity of hiding. Table I represents the stego image quality with help of PSNR feature. To discriminate the images in grayscale format to the PSNR is impotent for the human visual system. In this project messages are projected in the K-LSBs, the k is lies between 3 to 6 and PSNR is received. The results represents highest message hiding capacity and visual quality for k value is 4 or 5, so value k is taken as 4.

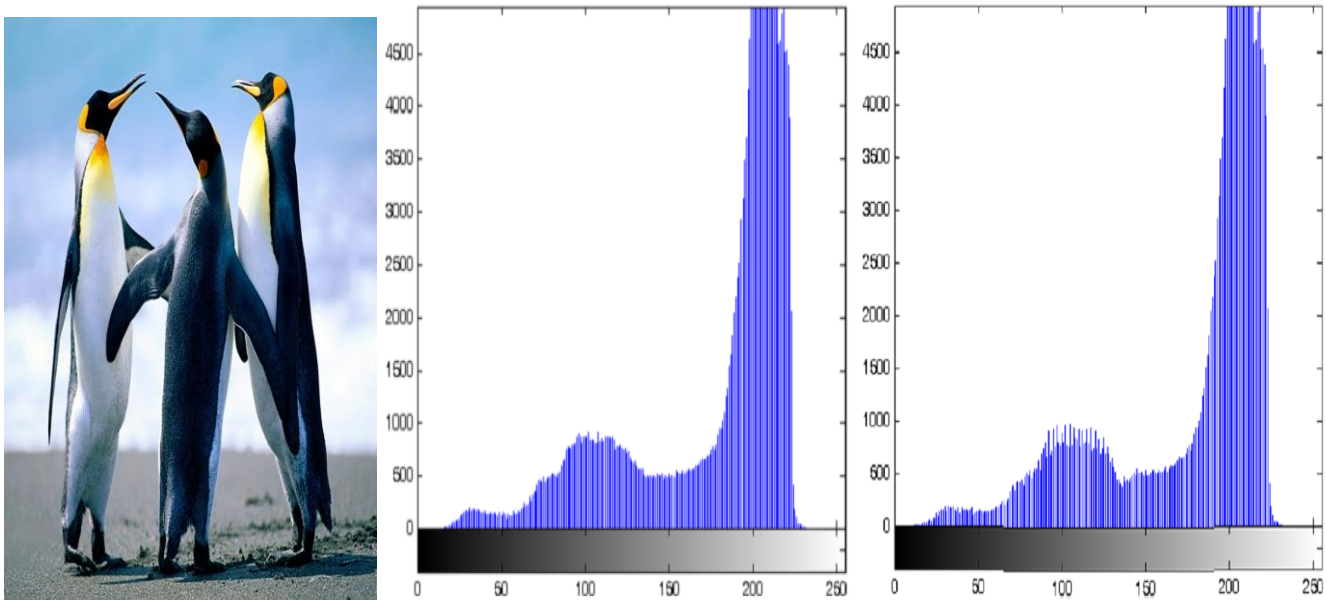
Table.6.1. Comparison of PSNR of Images for variant value of K

Cover Image	**PSNR**			
	K=3	**K=4**	**K=5**	**K=6**
Ship	46.83	39.94	32.04	24.69
Penguins	51.88	45.20	37.45	29.31
chrysanthemum	48.41	40.44	31.17	23.60
Koala	47.32	40.34	32.79	24.80

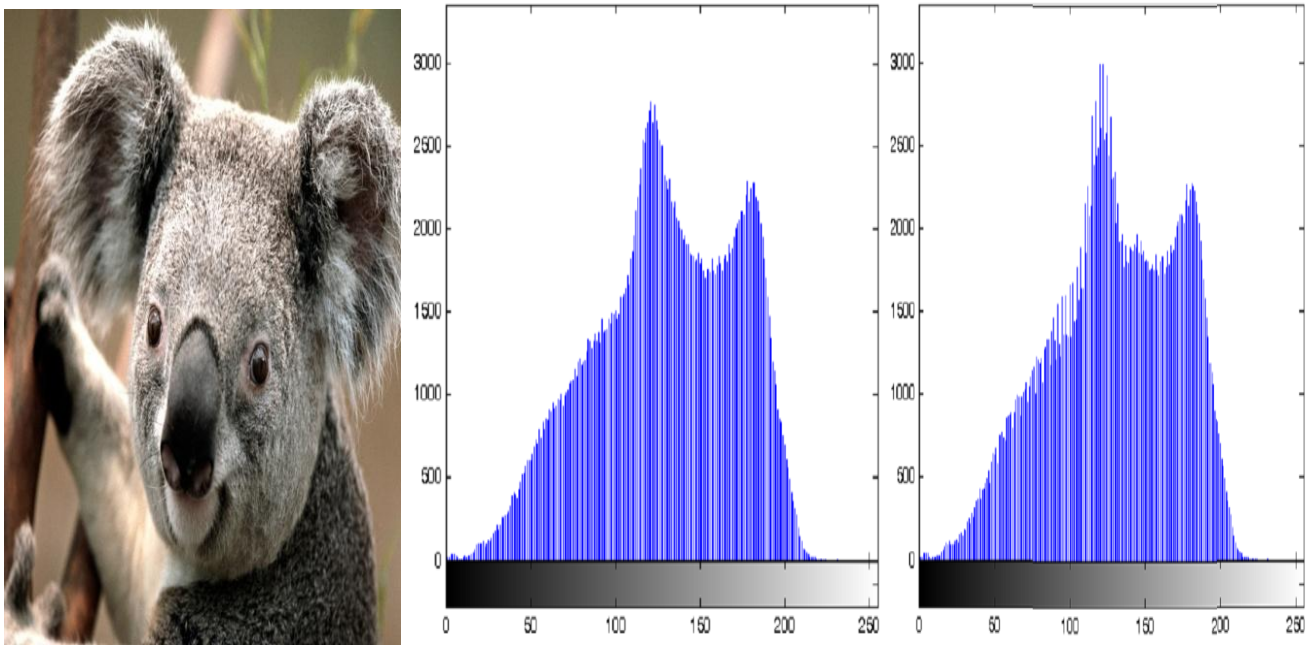
Fig.6.1 shows the original cover images along with their histogram and analyzed 4lsb histogram to compare it with the ones of the resulting stego image to test for imperceptibility.



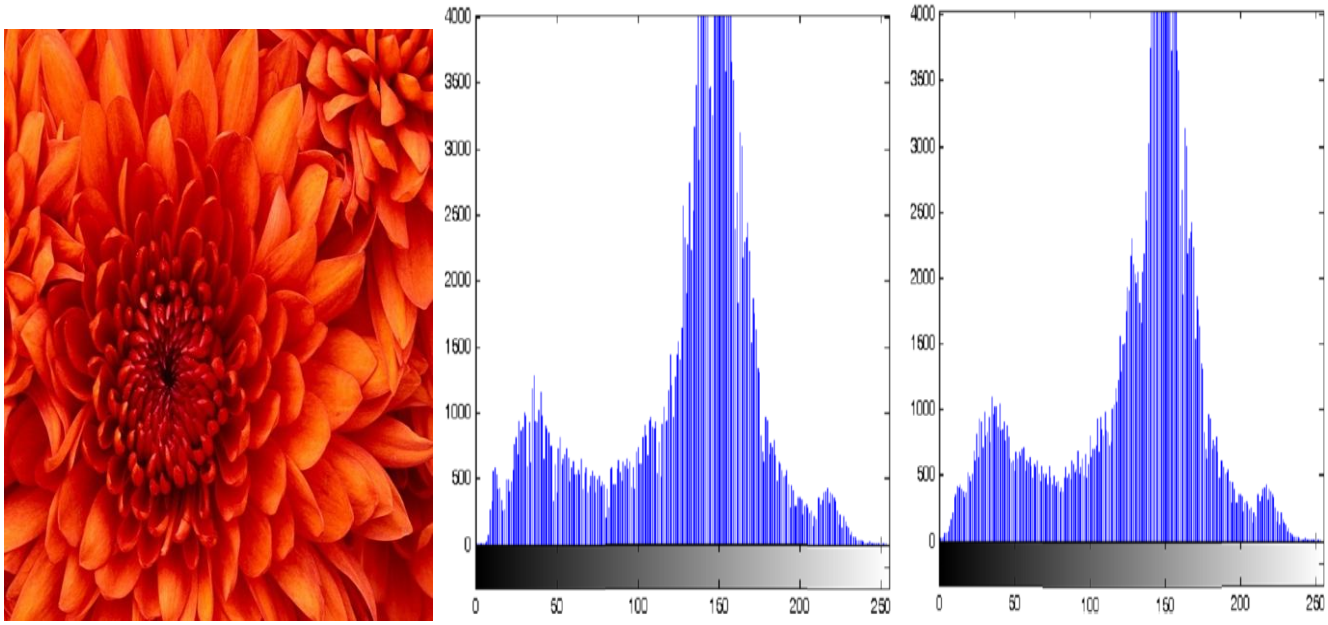
(a) (b) (c)


4500
4000
3500
3000
2500
2000
1500
1000
500
0
0
50
100
150
200
250

(d) (e) (f)


3000
2500
2000
1500
1000
500
0
0
50
100
150
200
250

(g) (h) (i)



(j) (k) (l)

Fig. Four Cover image used in system simulation and their corresponding histogram (a) Cover image Ship (b) ship histogram (c)stego histogram of ship (d) Cover image penguin (e) penguin histogram (f) stego histogram of penguin(g) cover image koala (h) koala histogram (i) stego histogram of koala(j) Cover image chrysanthemum (k) chrysanthemum histogram (l) stego histogram of chrysanthemum.

CONCLUSION

In this research work, the imperceptibility and capability of the input image has increased after embedding function with the use of innovative technique introduced as Steganography . evolutionay algorithm is very useful to minimizes the error differences between the stego and cover image to achieve the optimal mapping function and sustaining the local properties of image by using block mapping technique. This research also has another feature of increased hiding capacity of the secret messages by applying the OPAP method to the algorithms and it has the greater hiding capacity than the other existed systems. the results from the previously defined techniques provides increased capacity and imperceptibility of the input image, but on the other hand the complexity of the computations performed in this research are very high. at the same time we can deduct the cost of computation by selecting the finest block size. The optimization algorithms are also used for making increament in the PSNR and evolutionay algorithm is in the catagory of optimization techniques. .The experimental results show that this method works properly and is considered to give almost the optimum solution.

FUTURE ENHANCEMENT

A typical method for Steganalysis of the LSB substitution is the histogram attack that attempts to diagnose anomalies in the cover image's histogram. The future enhancement work would be in the direction to work on a new method for image Steganography which improves over the LSB image Steganography by decreasing the amount of changes made to the perceptual and statistical attributes of the cover image.

REFERENCE

[1] B. Norman, Secret Warfare, Acropolis Books, Washington D.C., 1973.

[2] W Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Systems Journal, Vol. 35, No. 3 and 4, pp. 313-336, 1996.

[3] M. Swanson, M. Kobayashi, and A. Tewfik, “Multimedia data embedding and watermarking technologies,” Proceedings of the IEEE, Vol. 86, No. 6, pp. 1064-1087, June 1998.

[4] R. Wolfgang, C. Podilchuk and E. Delp, “Perceptual watermarks for images and video,” to appear in the Proceedings of the IEEE, May, 1999. (A copy of this paper is availavle at: http://www.ece.purdue.edu/~ace).

[5] R. B. Wolfgang and E. J. Delp, “Fragile watermarking using the VW2D watermark,” Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents, SPIE Vol. 3657, San Jose, CA, January 1999.