INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

INCREASING PSNR AFTER EMBEDDING SECRET INFORMATION IN THE IMAGE USING THE GENETIC ALGORITHM

Mehdi EffatParvar[1], Sina Bageri[2], Davar eslampanah[3]

[1]Islamic Azad University Ardabil branch, Ardabil, Iran, me.effatparvar@gmail.com
Author Correspondence: [2] Islamic Azad University bilehsavar branch, bilehsavar, Iran, Sina.bagery@gmail.com
[3] Islamic Azad University bilehsavar branch, bilehsavar, Iran, valiasr_216steganography@yahoo.com

Abstract: - This paper proposes an image embedding method using the genetic algorithm. The proposed method ensures high quality for image steganography. We employ the genetic algorithm to find the best position in the host image to embed secret data. The proposed approach can achieve high embedding capacity, increase the quality of steganography, and increase the PSNR of the output image in comparison to that of other methods. The proposed approach has a better performance in embedding confidential data in other media, including sound, image, text, or video. Accordingly, simulation results indicate that the proposed method outperforms previous approaches and provides better quality.

Keywords: PSNR; LSB; storage capacity; attack

1. Introduction

Today, with the advance and expansion of computers and global networks, as well as the increase in the efficiency of this technology in all dimensions of human life, there has been an interest in using computers as work offices of people, organizations, and remote communications. However, one of the most important concerns and challenges of this domain is security and preventing unauthorized access to private personal information of different people and organizations. Steganography, which is known as a technology related to embedding secret and hidden data into objects or subjects that arouse no suspicion, has been emerged as a considerable interdisciplinary approach in data embedding methods. Although, this phenomenon has been mostly used for fixed images in the past, it is currently known for its application in video frames [1].

When steganography is used in digital video streams, it is vital to select target pixels to store secret or hidden data and particularly, achieve a successful and desirable embedding process. If these pixels are not carefully selected in this type of video steganography, problems may arise regarding undesirable spatial and temporal understanding. Steganography belongs to the cryptography family in information security and aims to hide the

existence of a message and deny its existence. Whereas, cryptography aims to preserve the confidentiality and integrity of a message, which is achieved by encrypting it, and make it impossible for unauthorized individuals to access the content of that message [2]. First, it is necessary to have a general view of the domain of steganography. Steganography is one of the subsets of security systems. Therefore, it seems that it is essential for better understanding to present a brief explanation of security systems. In order to create a better view about the subject, Fig 1 is presented from reference [3] and each field of security systems are investigated separately.

Information hiding preserves the copy right of software applications and electronic products, including music, artworks, electronic books, etc. there are different methods to hide the information, including text, sound, image, and video. LSB is a common method and JPEG images provide the best format in networks and the internet with high quality and compression. Regarding sound, LWT wavelet transformation is a new method, whose advantages include eliminating the need for the original sound for data recovery, high hiding capacity, full recovery, and high audio quality of the hidden sound. Different steganography methods have been proposed, which try to provide better quality and increase the efficiency of images and different applications. These methods replace a certain number of bits in image pixels or wavelet transformation coefficients [4]. However, using the genetic algorithm in a steganography scenario allows better performance for embedding confidential data into other media, including sound, image, text, or video. Therefore, this paper proposes a novel secure steganography approach using the genetic algorithm.

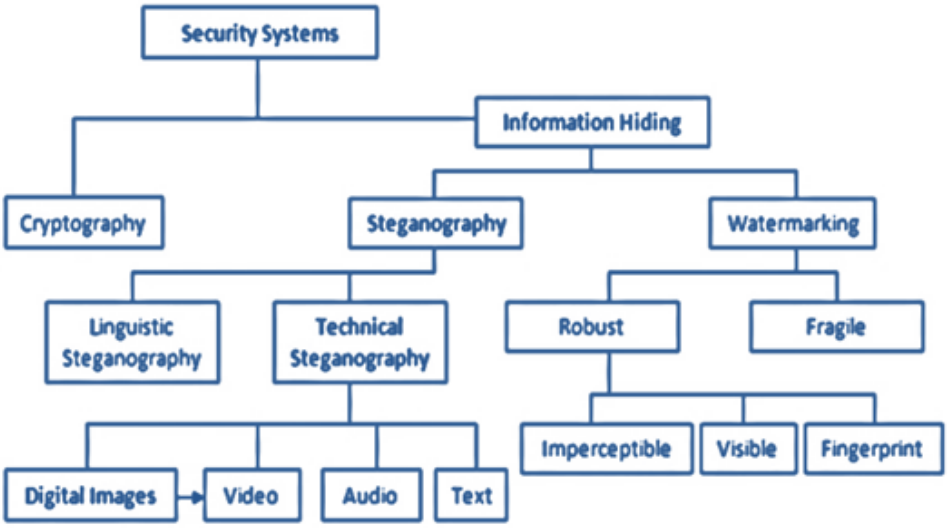

Figure 1: an overall view of security systems

2. BODY PREVIOUS WORKS

Genetic algorithms are inspired by the nature and have vast applications in different sciences. These algorithms are inspired by the natural evolution system, which is based on Darwin`s natural selection theory. This theory observes the nature and announces that the fitter creature or chromosome has a better chance of surviving and proliferating. This principle is used to design genetic algorithms. These algorithms usually include an initial random population of creatures or chromosomes. Using a crossover operator, two genes can be combined. Using a mutation operator, a gene can be mutated to find characteristics, which were no present in his parents. Genetic algorithms have a fitness function, which specifies the fitness of chromosomes. In order to apply genetic operators, chromosomes should be first selected, which can produce better offspring. In fact, parent chromosomes should possess high fitness, which indicates the survival of the fittest. There are different algorithms to select parent chromosomes. We do not go into the details, but only note that they all apply a policy in selecting parent chromosomes to increase the chance of selecting fitter chromosomes.

Steganography is one of the domains, which uses genetic algorithms, e.g. [5]. In this method, whose creators are Iranian, a safe Jpeg steganography method is proposed, which uses the genetic algorithm to evolve the optimal solution. First, chromosomes should be designed so that each chromosome can represent a (optimal or non-optimal) solution. Before that, we should take a look at the Jpeg structure. In Jpeg files, cosine transformation is used to map the image into the frequency domain, which is applied to 8x8 pixel blocks [6]. Another paper proposes a method, which can insert secret information in the host image, such that it is resistant

to RS attacks. This method also uses the genetic algorithm. At first, it applies the simple LSB approach and embeds secret bits in the host image. Next, using the genetic algorithm, pixel values are adjusted, such that RS parameter values satisfy the conditions of an ordinary image [7]. In order to insure security against RS analysis, after hiding the secret message in the cover image by LSB, pixel values are determined by the genetic algorithm. Therefore, the existence of a secret message is hardly detectable by RS analysis. The proposed method provides a higher quality image and empiric results also indicate that the resistance of the proposed algorithm against steganalysis provides higher quality and a desirable trade-off between security and image quality [8].

Another paper proposes a steganography method based on the genetic algorithm to increase the embedding capacity and security. Embedding is a method to provide communications between the sender and the receiver by means of hiding a message in an image. This paper proposes a secure embedding method in color images using the genetic algorithm, which is resistant against RS attacks. In the proposed steganography scheme, the image is embedded into the integer of wavelet transformation coefficient using a mapping function. This function is based on the genetic algorithm with 8x8 blocks on the input color image. After embedding the message optimally, the pixel adjustment process is applied. Using OPAP, the error difference between the cover and steganography images is minimized. The frequency domain method is used to increase the robustness of the proposed approach [9]. Steganography is a safe communication system, which can be simply known as hidden objects or subjects in multimedia files. This paper proposes an embedding scheme using the genetic algorithm. The optimal pixel adjustment process is performed after separating the message. More specifically, separation is performed by applying a mapping function based on the genetic algorithm with 8x8 blocks to the cover image. This method employs the genetic algorithm to achieve the optimal capacity for reducing the error difference between the cover and the image [10] [11].

3. THE PROPOSED STEGANOGRAPHY METHOD

The method proposed in this section can embed messages in color images resulting in high quality and high capacity cover media after embedding. After image segmentation, the proposed method uses the genetic algorithm to find the best part (chromosome) and maximize PSNR. Selecting the best part prevents reducing image quality after embedding. Fig 2 presents the overall scheme of the proposed method.

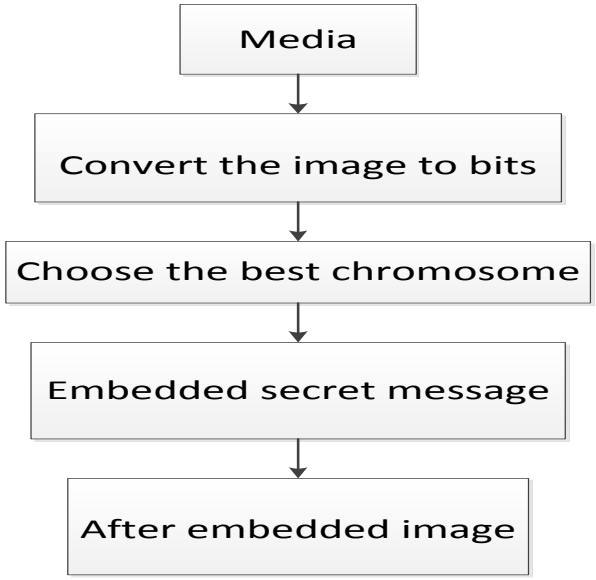

Figure 2: the overall scheme of the proposed method

3.1. Converting Sequential Images to Arrays

The host image has 512 bits and the sequential image has 256 bytes, where each pixel of the host image consists of 8 bits. The sequential image is converted into an array of bits, which includes 1014 rows and 512 bits. More specifically, there are 512 bits at each row. Operator XOR is applied to each two rows of the array of sequential bits and the chromosome and it is inserted in its LSB with a row of the host mage. When inserting bits in the LSB of the host mage, the first row of the sequential bit array is inserted into the LSB1 of the host image and the second row is inserted into LSB2. The insertion procedure for the rest of the rows is performed similarly until all bits of the array are inserted into the pixels of the host image. Fig 3 presents the conversion of a sequence to a bit array.

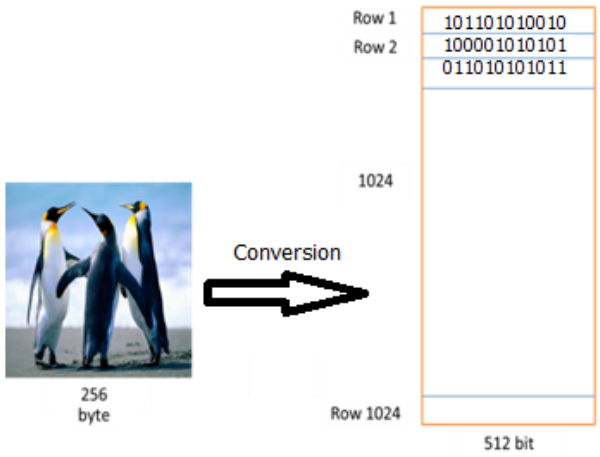

Figure 3: converting a sequential image to an array

3.2. The Overall Optimization and Problem Solution Process in the genetic algorithm

This section presents the genetic algorithm employed in the proposed method. The genetic algorithm is one of the subsets of soft computing, which has currently attracted a lot of interest. An optimization problem can be solved using the genetic algorithm. More specifically, the genetic algorithm is used to evolve the optimal solution. First, chromosome representation should be determined so that each chromosome represents an (optimal or non-optimal) solution. The proposed method employs the genetic algorithm to find the best chromosome, such that PSNR is maximized. Fig 4 presents an overall scheme of the genetic algorithm in the proposed method. The genetic algorithm exploits an initial population. Future generations are generated with optimization capabilities using mutation and crossover operations. We can say that the most sensitive and key part of the genetic algorithm is its chromosome evaluation, since it can alter the direction of the search. The following equation (1) is used to measure the fitness of each chromosome. PSNR is calculated in decibels (dB).

$$PSNR = 10\log_{10}\frac{(N^2)}{MSE} \tag{1}$$

Where, N shows the dimensions of the host image and x and y are the value of pixel (i, j) in the host image before and after inserting secret information.

$$MSE = \sum_{i=1}^{X}\sum_{j=1}^{Y}\frac{(|A_{ij} - B_{ij}|)^2}{X \times Y} \tag{2}$$

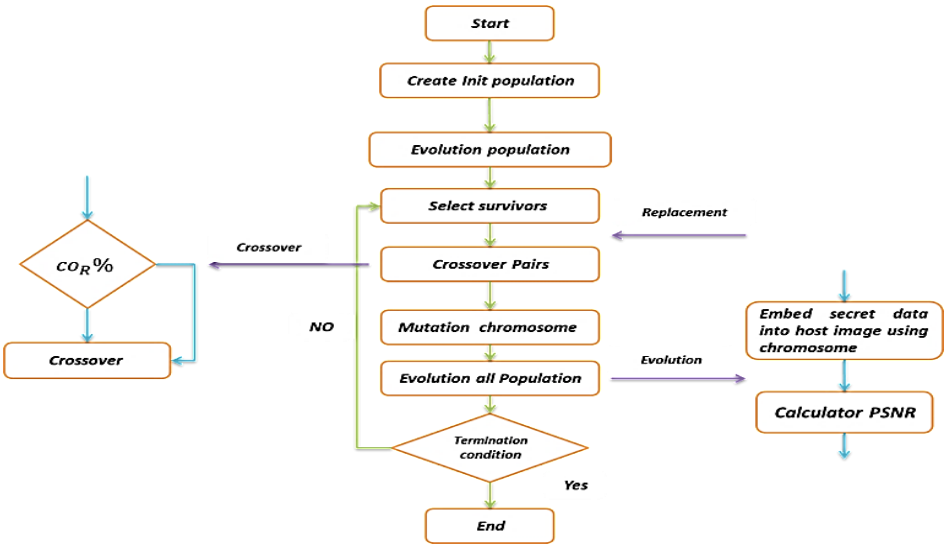

Figure 4: an overall scheme of the genetic algorithm for the proposed method

Selecting a fitness function is one of the most important stages in designing a method based on the genetic algorithm. In the proposed the genetic algorithm with the goal of improving the image quality, selecting Peak Signal to Noise Ratio (PSNR) can be an appropriate evaluation test. At the replacement stage, the best chromosome is selected so that the best result is not removed and the fitter chromosome is selected. Accordingly, tournament selection algorithm is used to select the best chromosome. In the tournament selection method, first a subset of the population of the previous generation is selected and an appropriate roulette wheel is developed according to the ranks of its members. Subsequently, using this roulette wheel, several members of the population are selected. At the Evolution All Population stage, this stage is applied to the entire population. At this stage, secret information is embedded into the host image using chromosome. More specifically, the XOR operator is applied to array bits and the chromosome and PSNR is computed. Fig 5 presents the information embedding into the host image.

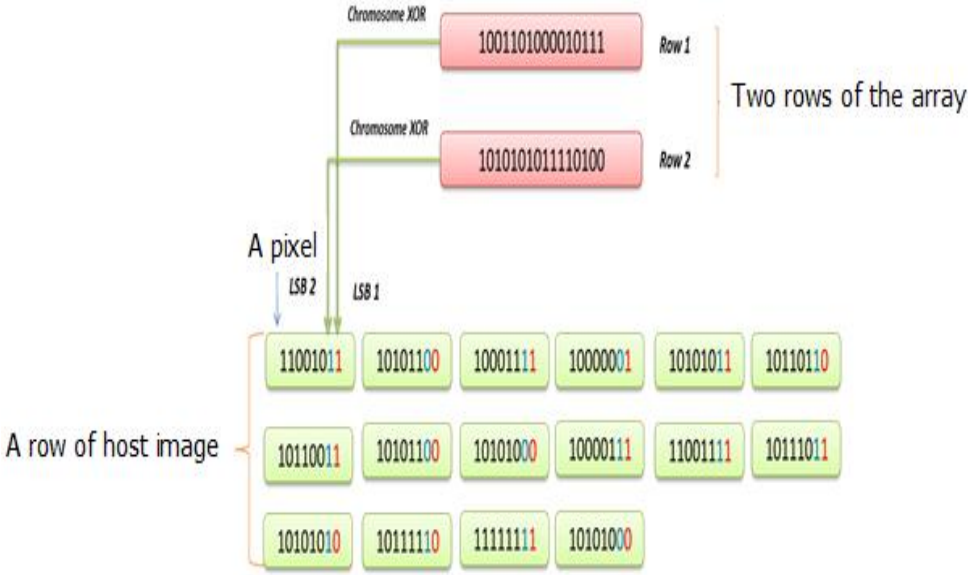

Figure 5: information embedding in the host image

3.3. Information Extraction

The stages of secret information retrieval are also very simple.

- Segmentation of the host image
- Using the order obtained by the chromosome
- Extracting the two least significant bits of each pixel in the host image (extracting the considered chromosome from the pixel bit and separating its gene).
- According to the chromosome`s gene, a set of pixel bits and then raw sequential bits are achieved

4. SIMULATION AND EVALUATION

The proposed scheme was tested using different images and its performance and efficiency were compared with those of previous works. Moreover, in order to evaluate the proposed method in MATLAB software, different images were used in embedding. Comparison results show that the output image of the proposed method is better than that of other previous algorithms.

For our experiments, Lena's image was used as a host image with a 256x256 size. Moreover, jet, pepper, and baboon images were used as sequential images as Fig 6. The dimensions of sequential images were changed in different experiments. Table I presents the results of different storage capacities. The proposed method considers the tournament selection mechanism and as it was mentioned, PSNR of the embedded images are used as the fitness function of the genetic algorithm. The genetic algorithm is stopped when maximum numbers of generations have been produced or there is an insignificant chance of achieving significant changes in the next

generation. We must note that the maximum number of generations is considered 200. Table 2 presents the parameters of the genetic algorithm.

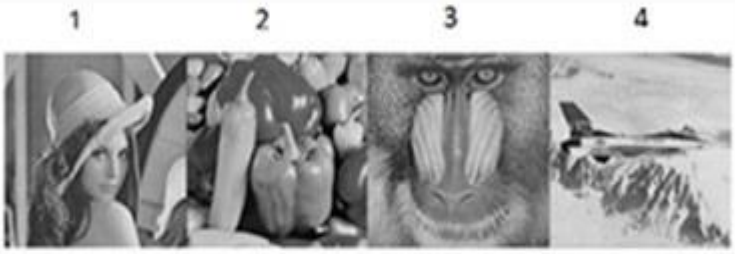

Figure 6: Sequential and Host Images: 1: Host Image, 2, 3, and 4: Sequential Images

Table 1: Experimental Results of the Proposed Method for Different Images

Capacity		PSNR (%)		
%	Bpp (bits / pixel)	Jet	Pepper	Baboon
6.25	0.50	54.30	54.28	54.25
10.0	0.80	52.20	52.19	52.16
20.1	1.61	46.52	46.53	46.60
24.6	1.96	45.66	45.61	45.61
29.9	2.39	41.73	41.71	41.68
40.0	3.20	35.70	35.81	36.51
49.4	3.95	34.67	34.93	35.42

Table 2: Parameters Used to Implement a Genetic Algorithm

Parameter	Value
Population Size	300
Crossover Rate	0.7
Mutation Rate	0.04
Replacement Rate	0.8

Table 1 show that even when the capacity of the embedded hidden image is increased, the PSNR value of the embedded image is almost acceptable. In order to evaluate the performance of the proposed algorithm in comparison to that of other algorithms, the visual quality (i.e. PSNR) of the embedded images is compared with previous steganography schemes. Table 3 presents the PSNR of the proposed method and compared algorithms. Experimental results of the proposed algorithm are compared with those of other methods. In the reference paper [12], a novel approach is proposed to share the sequential image based on the threshold scheme (K, n) with additional steganography and authentication capabilities. Moreover, paper [13] proposes a scheme to improve the authentication capability, which prevents imposter participants. The proposed scheme defines the order of embedding bits to improve the quality of the embedded image. Chang et al. [14] propose an image sharing scheme, which is a combination of embedding and authentication based on the Chinese remainder theorem (CRT). The proposed scheme not only improves the authentication capability, but also increases the visual quality of the embedded images. Wu et al. [15] propose an image sharing scheme using the optimal pixel adjustment process to increase image quality and different authentication bit conditions.

Table 3: performance comparison of the proposed method and different embedding algorithms

PSNR (%)					
The Proposed Method	Wu et al.'s method	Chang et al's method	Yang et al.'s method	Stego Image (512×512)	Secret Image (256×256)
(General test Pattern)	44.50	43.54	40.37	41.60	**Lena**
	44.52	43.53	40.73	41.66	**Jet**
	44.56	43.56	39.30	41.56	**Pepper**
	44.55	43.55	38.86	41.51	**Sailboat**
	44.52	43.54	39.94	41.55	**Baboon**
	44.57	43.54	39.84	41.58	**Average**

As we can see, the proposed algorithm outperforms all compared methods. In order to investigate the visual quality of the embedded images produced by the proposed algorithm, original cover and embedded images are presented, which show that the distortion between the original cover and embedded images is visually and perceptively undetectable Fig 7.

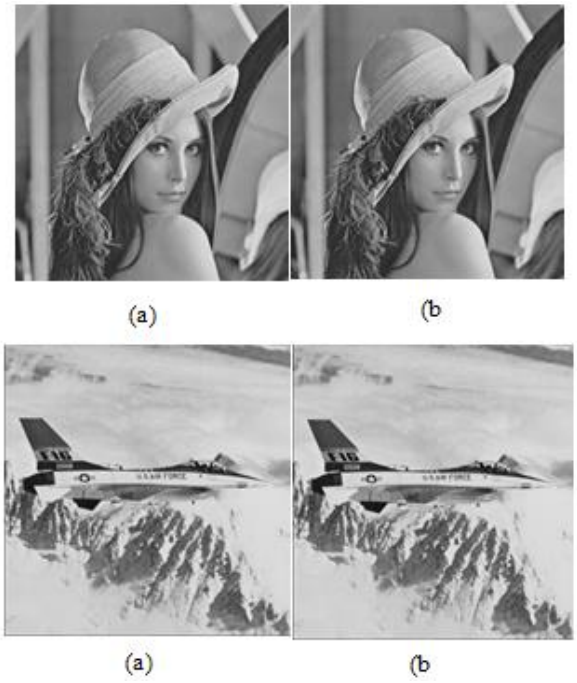

Figure 7: original cover and embedded images

5. CONCLUSIONS

This paper proposed an image embedding method using the genetic algorithm. The proposed method provides high quality for embedding images. Moreover, the genetic algorithm is used to locate the best position in the host image to embed secret data. The proposed method can achieve high embedding capacity and increase the quality of image embedding, which is clear from the PSNR value of the proposed approach.

The embedding process is performed in two stages. At the first stage, secret bits are modified and the second stage embeds it in the host image. The proposed method was compared with previous works regarding the hiding effectiveness and the quality of image embedding. Empiric results indicate that the proposed method increases the embedding capacity of the secret image. The embedding image is visually indistinguishable from its corresponding host image. We conclude that the proposed algorithm can create a high quality hidden image, which satisfies embedding capacity demands of the users. The proposed plan is simple and practical for embedding applications. Our future work focuses on improving the efficiency of the proposed method, particularly, suing efficient meta-heuristic algorithms.

REFERENCES

[1] T. Bhattacharya, S. Bhowmik and S. R. B. Chaudhuri, 2008, "A Steganographic Approach by using Session Based Stego-Key, Genetic Algorithm and Variable Bit Replacement Technique", 2008 International Conference on Computer and Electrical Engineering.

[2] L.Y. Tseng, Y.K. Chan, Y.A. Ho, Y.P. Chu, 2008, "Image hiding with an improved genetic algorithm and an optimal pixel adjustment process", Eighth International Conference on Intelligent Systems Design and Applications, IEEE, pp. 239-253.

[3] Abbas Cheddad et al., Digital image steganography, 2010, "Survey and analysis of current methods", Signal Processing, ELSEVIER.

[4] M. Nosrati and R. Karimi, 2012, "A Survey on Usage of Genetic Algorithms in Recent Steganography Researches", World Applied Programming, Vol (2), No (3), March 2012. PP- 206-210.

[5] Krishna Bhowal et al, 2010, "Audio Steganography using GA", 2010 International Conference on Computational Intelligence and Communication Networks, IEEE.

[6] Amin Milani Fard et al, 2006, "A New Genetic Algorithm Approach for Secure JPEG Steganography", IEEE.

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

[8] Shen Wang et al, 2010, "A Secure Steganography Method based on Genetic Algorithm", Journal of Information Hiding and Multimedia Signal Processing, IEEE.

[9] Jyoti, Md. Sabir, 2013, "More Secured Steganography Model with High Concealing Capacity by using Genetic Algorithm, Integer Wavelet Transform and OPAP", International Journal on Recent and Innovation Trends in Computing and Communication, IJRITCC, MAR 2013, Volume: 1 Issue: 4, pp. 394 – 408.

[10] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang and Te-Ming Tu, 2008, "A novel image steganographic method using tri-way pixelvalue differencing", Journal of Multimedia, Vol 3, No 2, pp 37-44.

[11] Lee, Y.K.; Chen, L.H. 2000, "High capacity image steganographic model", IEE Proceedings Image and Signal Processing, Vol 147, pp. 288-294.

[12] Lin, Chang Ch, Wen H. T. 2004, "Secret image sharing with steganography and authentication", Journal of Systems and Software 73.3, pp. 405-414.

[13] Yang, Ching N. 2007, "Improvements of image sharing with steganography and authentication", Journal of Systems and Software 80.7, pp. 1070-1076.

[14] Chang, Chin-Chen, Yi-Pei Hsieh, and Chia-Hsuan Lin. 2008, "Sharing secrets in stego images with authentication Pattern Recognition", 41.10, pp. 3130-3137.

[15] Wu, ChiaCh, Shang J.K, Min Sh.H. 2011, "A high quality image sharing with steganography and adaptive authentication scheme", Journal of Systems and Software 84.12, pp. 2196-2207.