RESEARCH PAPER | Engineering | Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

Information Hiding Scheme For Digital Images Based on Genetic Algorithms

KEYWORDS: Steganography, Message concealment, Information hiding, Region selection, Genetic algorithms.

P.M.Siva Raja
Research Scholar, Sathyabama University, Chennai, Tamil Nadu, India.

E.Baburaj
Professor, Department of Computer Science and Engineering, Sun College of Engineering and Technology, Nagercoil,

ABSTRACT *Modern information hiding technology plays a vital role in information security. Hiding capacity is very much essential for efficient secret communication. The redundancies of digital media as well as the features of human visual system create hiding technology an important one. Steganography is the art and Science of scripting hidden messages in such a manner that no one, except the sender and directed receiver realize the existence of the message. Images are the generally secret objects used for information hiding schemes. Image steganography is the most well-liked method for message cover up. Numerous special carrier file designs are used, but digital images are the most familiar, because of their frequency in the Internet. In LSBMR, two covert bits is fixed into each embedding unit and the threshold value for region selection is determined. The major disadvantage of this scheme is the total difference is taken as the threshold value. In this paper LSB Matching Revisited (LSBMR) image steganography using Genetic Algorithm (GA) is proposed, in which Genetic algorithm is used to select the embedding regions according to the size of the secret message and to optimize the threshold value of the selected image regions. Experimental analysis shows that the proposed algorithm outperforms the existing methods in terms of capacity and security.*

I. INTRODUCTION

As an important component of multimedia information security, information hiding has received wide attention in recent years. In fact, intellectual properties are becoming harder to protect and so are original contents, leading to requirement of image Steganography techniques. Steganography is a technique for information hiding [1]. Steganography intends to insert secret data in to digital wrap media, such as Images, Audio, and Video without being suspicious. During insecure communication between two parties, a high possibility of causing attack is feasible by the intruder in interrupting and reading secret information. The characteristic Invisibility, Storage capacity, Resilience against attack makes Steganography a significant concept in hiding technology. On the other hand the users of digital representation are under risk due to the increasing concern of copyright intrusion, criminal sharing, illegal interfering and inferior security in communication [10]. Data hiding manages an invisible embedding of an supplementary data in the digital media becomes a potential solution to the latter class of troubles over the last decade (Vleeschouwer et al. 2002; Wu and Liu 2002). Several data hiding methods are urbanized for audio, image, video and graphics etc., and are also detailed in literature (Special issue on copyright and privacy protection 1998; Special issue on enabling security technologies for digital right management 2004; Pan et al. 2004) [6] [22]. Even though data hiding is a general term, steganography and digital watermarking are the two admired terms where the former establishes an enclosed information channel in point-to-point link, later does not essentially cover the detail of secret communication to third party [15]. Based on various applications the degree of requirements varies. But the important necessities of image data hiding normally are visual undetectability of the hidden data, security against arithmetical investigation and robustness to unmalicious operations that a transmission channel is to face. The processing contains compression for proficient storage and transmission, mean/median filtering for the use of noise cleaning [12] [23]. However, the quantity or strength of the signal processing operations is limited to a level so that the stego/watermarked-object necessity preserves its commercial value.

In data hiding crisis, GA is utilized for optimizing the basically inconsistent requirements of security and robustness [8] [10]. A report on data hiding research in digital media presents several tradeoff relations. The majority of the data hiding algorithms urbanized so far concentrates on single need or offer suboptimal results to meet a group of needs based on the applications [3][7]. On one hand the digital media revolution and the successful growth in network transmissions provides benefits of approximately noise free transmission, the no difficulty of editing and the internet sharing of digital multimedia information. In this paper LSB Matching Revisited (LSBMR) image steganography using Genetic Algorithm (GA) is proposed, in which Genetic algorithm is used to select the embedding regions according to the size of the secret message and to optimize the threshold value of the selected image regions. The rest of the paper is arranged as follows. Section 2 analyzes the limitations of the relevant steganographic schemes with the other techniques. Section 3 shows the details of data embedding and data extraction in the proposed scheme. Section 4 presents experimental results and discussions. Finally, conclusion and future enhancement are given in section 5.

II. RELATED WORKS

a Data hiding scheme is vastly discussed in this section in order to emphasize the usefulness of this class of tools for performance improvement in data hiding. The idea of this review is to argue advantages and disadvantages of the relevant works. LSB based techniques pose a tricky challenge to a steganalysis in the inactive warden model as it is complex to distinguish cover images from stego images with small alters made. Obviously with an active warden, such techniques are effortlessly beaten by randomizing the LSB. In this LSB replacement and LSBM approaches [7] [11], the embedding process is extremely alike. Given a secret bit stream to be implanted, a travelling order in the secret image is first produced by a PRNG, and then each pixel along the travelling order is treated individually. For LSB replacement, the secret bit simply overwrites the LSB of the pixel. For LSBM scheme, if the secret bit is not equal to the LSB of the given pixel, then plus or minus one is added randomly to the pixel while keeping the altered pixel in the range of [0,255]. In such a manner,

Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

the LSB of pixels along the traveling order couple the covert bit stream after data hiding both LSB replacement and LSBM [16][17]. As a result, the data extraction method is accurately the same for the two approaches. It initially produces the similar traveling order according to a public key, and then the secrete message is extracted correctly by authenticating the parity bit pixel values.

According to the method of LSBMR, two covert bits is fixed into each embedding unit and the threshold T for region selection is determined [18] [14]. After data hiding, the image outcome is separated into non-overlapping blocks. The blocks are then turned around by a random number of degrees. In data extraction, the method initially extracts the side information from the stego image [19]. Based on the side information, data extraction does some parameter recognition process and identifies the regions that have been used for data hiding [4] [5]. At last, it obtains the secret message M with respect to the matching extraction algorithm. The main drawback of LSBM scheme is the absolute difference is taken as the threshold value T and the threshold for region selection is also varied. Additional regions are discharged flexibly for data hiding by reducing the threshold when the embedding rate increases [13] [9].

III. SECRET DATA HIDING-ISSUES

In the data embedding stage, the method initially digitize some parameters in utilizing consequent data preprocessing and region selection. In addition the threshold value is optimized for the selected regions. If the regions are enough for hiding the given secret message M, then data hiding is performed on the selected regions and then repeats the region selection process using Genetic Algorithms and optimize the threshold value of selected regions until the secret message M is embedded completely. In data extraction, the method initially extracts the side information from the stego image. Based on the side information, Algorithms does some post processing and recognizes the regions that have been used for data hiding. At last, the method obtains the secret message M according to the precise extraction algorithm. This paper proposes an embedding method based on LSBMR with Genetic Algorithms. Genetic Algorithms are used for optimizing the threshold value and the selection of embedding regions.

3.1 Data Embedding

The process of data hiding method in digital images is discussed in this section. The choice of cover images is significant and influences the security in a most important way. Gray scale image is considered as cover and the related type image like content data is considered as message signal as it preserves related data even after different signal processing operations. Algorithms for embedding process are as follows.

Step 1: The cover image of size h x w is first divided into non-overlapping blocks of BS × BS. For each small block turn around it by an arbitrary degree in the range of {0, 90,180,270} as determined by a secret key k1.Two benefits are obtained by the arbitrary rotation. First, it checks the detector from receiving the correct embedding regions without the secret key k1and thus the security is increased much more.

Step 2: The developed image is reorganized as a row vector RV by raster scanning and then the vector is separated non overlapping embedding units with every two successive pixels (x_i,x_{i+1}).

Step 3: According to the LSMBR method, two secret bits are implanted into each embedding unit. Therefore, for a given secret message M, the threshold T for region selection is determined by using genetic algorithm.

GA operations

In LSMBR proposal, to find the perfect position for data embedding, the approach based on new genetic algorithm is used. In case of optimization, four goals to be handled are: lengthy secret message, superior image quality, enhanced

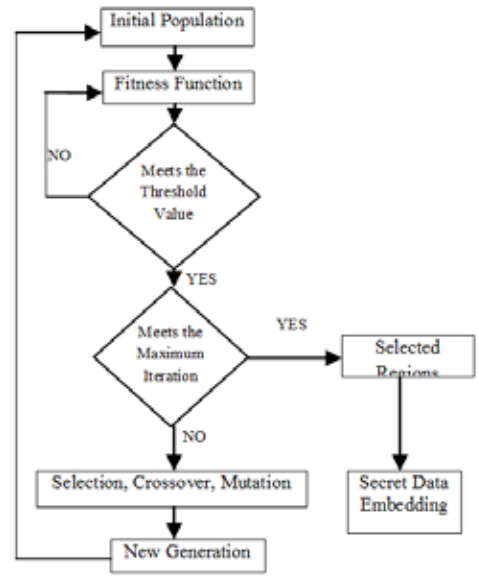

Fig. 2. Flowchart for the main module of the problem statement.

robustness and better data capacity. The first and the main step to model a Genetic Algorithm is to find the chromosomes, operators and fitness function. The chromosome is encrypted as an array of 64 genes enclosing quantized DCT coefficients of each 8*8 pixel block of the image. The purpose of utilizing genetic algorithm in LSMBR is to identify the finest position for data embedding. In addition genetic algorithm optimizes the quality of the steganographic image. The optimization process in genetic algorithm handles four conflicting objective such as lengthy secret message, superior image quality, enhanced robustness and better data capacity. The first step to model this problem as a GA problem, is determining the chromosome, GA operators and fitness function. The procedure for the selection of embedding regions and optimization of threshold value of selected regions are as follows

1. Initialization of Population

Chromosomal representation of the parameter values is defined in string of bits. The initial population is formed by taking BS×BS pixel blocks and Binary Encoding is used for forming the initial population. Binary encoding is the most common and simplest one. Every chromosome is represented in strings of bits as 0 or 1 for binary encoding.

2. Selection

Most excellent embedded pair of individuals is selected by roulette-wheel selection procedure by summing robustness values of the individuals to get robustness. Then arbitrarily choose individuals to cross 50% of the robustness value in the aggregative way. The exacting individual which crosses 50% condition in the aggregation process is chosen to be one of the matching pool pair. This process is again carried on to find another individual pool matching pair.

3. Crossover

Locate the crossover site and execute crossover between the selected pixel pair in order to obtain the new pair of more embedded individuals using sums crossover. The selected matching pool is taken as input and finds the crossover site using arithmetic crossover. Exchange the positions lying on one side of crossover site of those matching pool pair resulting in a new pair of individuals.

Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

4. Mutation
To mutate or modify a specific bit in a pixel block with very small probability is defined as mutation. Uniform mutation is used for the mutation process. A very small mutation probability is chosen, depending upon the probability value; change a bit from 1 to 0 or 0 to 1.

5. Objective Function
To estimate the fitness or robustness value of an individual, the initial population is taken as input. On each population 2D interpolation technique is used to estimate the original matrix. The mean square error is evaluated by subtracting the interpolated matrix from the original matrix. The square of that MSE is considered to be the fitness value of that particular individual. The fitness function is evaluated using the equation 1 as

$$\left[f(x) = \left(\frac{1}{hxw} \right) \sum_{i}^{H} \sum_{j}^{W} (I_{ij} - I'_{ij})^2 \right] \quad (1)$$

Where hxw is the height and width of the cover image, I_{ij} is the pixel value of coordinate (x,y) in cover image, I'_{ij} is the corresponding pixel value in the rotated image.

Step 4: According to LSMBR, two secret bits are embedded into each embedding unit. Therefore for a given secret message M, the threshold T for region selection is determined by using the optimization technique in eqn (1). The embedding regions in a pseudorandom order determined by a secret key k_2. The secret key is the difference between the two pixel values. That value is greater than or equal to the threshold value.
Performing data hiding on the selected embedding regions are as follows. In the LSB matching revisited, the choice of either to insert or delete one from the cover image pixel is arbitrary. This method employs the option to set a binary function of two cover image pixels to the preferred value in eqn (2). The embedding is achieved by a pair of pixels as a unit, where the LSB of the initial pixel holds one bit of information, and a function of the two pixel values holds another bit of information.

$$f(l, w) = LSB\left(\left[\frac{l}{2} \right] + w \right) \quad (2)$$

Data hiding is performed according to the following two properties:

Property 1: $f(l-1, w) \neq f(l+1, w)$

Property 2: $f(l, w) \neq f(l, w+1)$

Where h_i and h_{i+1} denote two secret bits to be embedded. The function f (l, w) is a random value in {-1, +1} and (x, xi_{+1}) in the cover image pixel and (x^l, x^l_{i+1}) = $h_{i+1,}$(x^l, x^l_{i+1}) = (x, xi_{+1})

Step 5: After data hiding, the developed image is partitioned into non overlapping BS×BS blocks. The blocks are then rotated by a random number of degrees based on key k_1.

3.2 Data Extraction
The final stage of the algorithm is the retrieval process of the secret message M. To mine the secret message, first extract the side information as the block size BS and the threshold T from the stego image. For that the stego image is divided into BS*BS non overlapping blocks and the blocks are then rotated by random degree based on the secret key k_1. The resulting image is rearranged as a row vector RV_i. Finally to get the embedding units by dividing row vector RV_i into non-overlapping blocks with two consecutive pixels. The travel through the embedding regions whose mean values are greater than or equal to the threshold T according to a pseudorandom order based on the secret key k_2 until all the hidden bits (secret message) are extracted completely based on eqn(3). To extract the two secret bits h_i, h_{i+1} as follows

M_i = LSB (x_i^{ll}), hi_{+1} = LSB ([I^{ll}/2] +w_{i+1}) (3)

IV. RESULTS AND DISCUSSIONS
This section presents simulation results to demonstrate the effectiveness of the proposed data hiding method compared with existing relevant methods as mentioned in section II. The above programs are implemented using Mat LAB 7.04 and runs in PC I5 with 512 MB RAM, Windows 7 Operating system. Experiment focus on the two measures stego image quality and the message capacity which is used for evaluating steganographic method. 8 bit gray level images like Lena, Baboon, Fover, Deer, and Lichtenstein are utilized in experimental evaluation as shown in figure 3(a). The Cover Image With 256* 256 Pixels and 256 gray levels is used. In LSBMR method, one block hides two secret messages, thus each block blinds up to 26*2=52 bit secret messages. In LSBMR with genetic algorithm experiment, a quantized DCT coefficient blinds up to k secret bits. In order to compare LSBMR - GA method with LSBMR method using the above said circumstance, k is set to 2 i.e., a quantized DCT coefficient hides up to two secret bit. Thus, each block blinds 36*2 =72 bit messages. The message capacity for different methods are shown in Table-I.

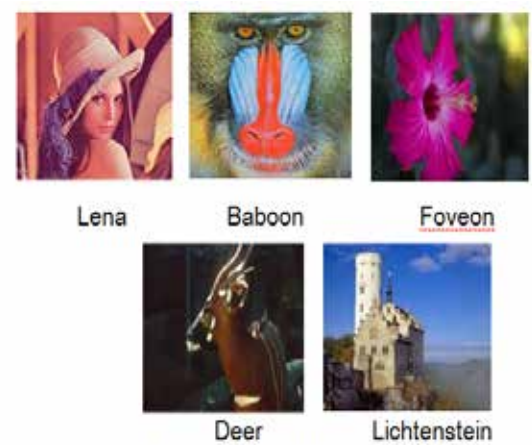

Fig 3. (a) Cover Images

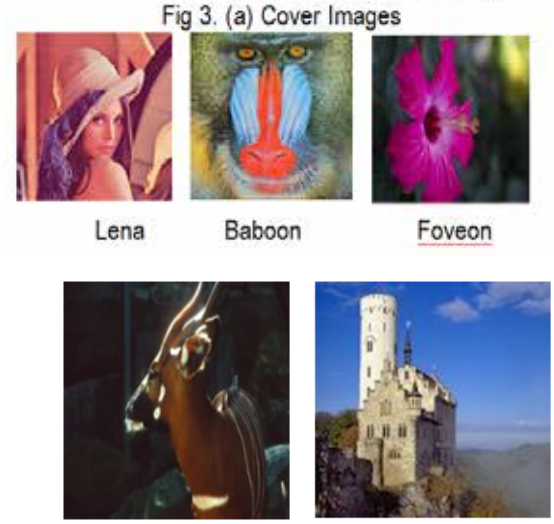

Fig 3. (b) Stego Images

LSBMR uses the image size of 104*64 pixels. But LSBMR with GA uses the image size of 128*72 pixels. Along with the optimal substitution strategy, LSBMR-GA method achieves better

Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

quality when compared to LSBMR. The LSBMR-GA utilizes five cover images specified in Figure 3(a) to compare the visual quality of the LSBMR method with LSBMR-GA method. Figure 3(b) shows the stego images of LSBMR-GA method. On comparing the cover image in figures 3(a) with the resultant stego image in figure 3(b) are more or less similar and highly difficult to detect the embedded secret images. LSBMR-GA method provides larger PSNRs in contrast to LSBMR. The larger PSNRs value reduces degradation in image increasing the quality of the cover image. Final conclusion is that the message capacity of LSBMR-GA proposal is larger and facilitates better image quality when compared to LSBMR.

The Peak Signal to Noise Ratio (PSNR) is used to evaluate qualities of the stego images. Experimental results of few stego images are shown in figure 3(b). In addition, other noticeable image quality measures, such as Mean Square Error (MSE) and Receiver Optimization Curve (ROC) are also applied to LSBMR-GA method indicating the significance to the contribution of this paper. Besides, from MSE values, it shows that the changed value of each pixel is almost same in stego images. Experiments demonstrates the accomplished performance of LSBMR-GA approach in terms of capacity and security for hiding secret data in the stegoimage.The analysis of selection technique is based on a comparison as the number of function evaluations. Population size, Crossover, Mutation, criteria for termination, Fitness function and number of generations are the parameters used for analysis.

4.1 Histogram Analysis

A histogram proceeds with graphical depiction of the tonal distribution in a digital image is defined as image histogram. The number of pixels is plotted for each tonal value. By observing histogram a viewer finds all the tonal distribution. Since the information present in a graph is a depiction of pixel sharing as a task of tonal variation, the image histogram acts as a useful tool in case of thresholding. Most of the histograms are identical because of embedding message bits in a noisy region of an image.

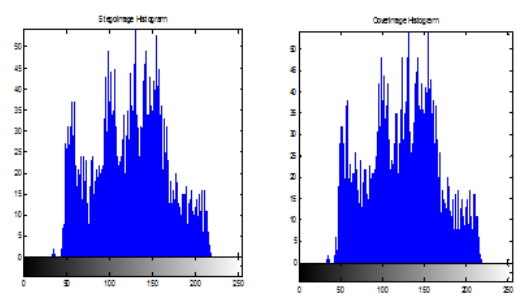

Fig.4 (a) Histogram of Cover Images

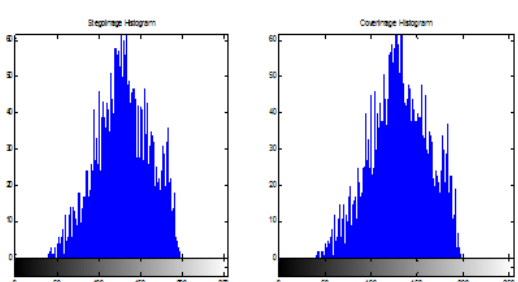

Fig.4 (b) Histogram of Stego Images

Figure 4(a) and 4(b) shows the histograms of cover and stego images respectively. The resulting histograms are almost identical. The identical similarity histogram is caused by embedding the message bits in noisy regions of the image. The results of PSNRs and the MSE values obtained from LSBMR-GA technique is depicted in Table 3.

4.2 .Optimization of Threshold Value

To evaluate the performance of the LSBMR-GA selection methods, the experiment analysis of selection techniques based on a comparison of their respective performance is estimated as the number of function evaluations. The raw data obtained from the optimization comprised the average, mean and best of 100 generations for each function of the set of functions under consecration.

The parameters used in experiments are Population size as 100, Selection Methods as Roulette Wheel selection, Simple Arithmetic Crossover with the probability of 0.08 per generations, the Multi Non Uniform mutation with Probability 5% and objective value of fitness function. A criterion for termination is defined as the executions stops on reaching the number of generations. The average, mean and best values for each function is evaluated for each number of generations.

4.3. ROC Curve Analysis

For comparing the embedding security of LSBMR-GA method to that of LSBMR methods, Receive Operating Characteristic (ROC) curves are used. ROC curves are utilized to embed image databases with the minimum value of the maximum capacity of the LSBMR-GA method and the LSBMR method.

Table 1. ROC Curve (Embedding)

False Positives	True Negative	
	LSBMR	LSBMR-GA
0.2	0.17	0.19
0.4	0.35	0.37
0.6	0.51	0.56
0.8	0.70	0.77
1.0	0.98	0.99

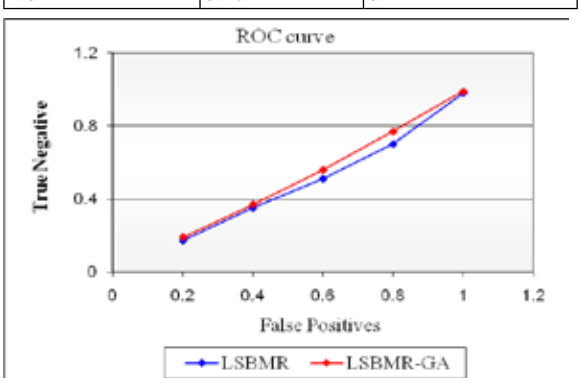

Fig. 5. ROC Curve (Embedding)

The Receiver Operating Characteristics (ROC) curves are shown in above Figure.5. The ROC curves clearly shows that both specific steganalytic algorithms would fail in detecting the LSBMR-GA method even when the embedding rate is as high as 25%, while they obtain satisfactory results for detecting stego image using LSBMR and LSBMR-GA methods. As observed from figure the detection accuracy, shown as the area under the ROC curve, is lower for LSBMR-GA algorithm as compared to the LSBMR algorithms.

4.4. Comparing Capacity

Figure 6 shows the results of computing capacity for LSBMR-GA algorithm and the LSBMR method in 35 images. It is clear that the capacity of the LSBMR-GA method is higher in most images. The mean capacity of the LSBMR-BA method is about 1024 bits higher than the mean capacity given by the LSBMR method.

Volume : 4 | Issue : 6 | June 2014 | ISSN - 2249-555X

Table 2. Embedding Capacities

Numberof Images	Capacity (MB)	
	LSBMR	LSBMR-GA
5	4.60	3.94
10	4.13	3.40
15	3.78	2.78
20	3.20	2.13
25	2.33	1.78
30	1.56	1.33
35	0.98	0.65

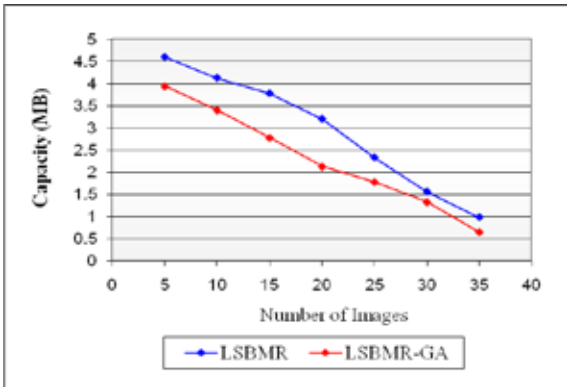

Fig. 6. Embedding Capacities of the LSBMR-GA method (Red) and LSBMR method (Blue).

The embedding capacities are shown in above Figure.6. The LSBMR-GA facilitates a high capacity of about 20-25% compared to LSBMR. The performances of the methods are evaluated and compared on the basics of two measures which are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) .The equations 4 and 5 of these two measures are

$$MSE = \left(\frac{1}{m \times n}\right) \sum_{i=1}^{m-1} \sum_{j=1}^{n-1} (I_{ij} - I'_{ij})^2 \quad (4)$$

$$PSNR = 10 \log_{10} \left(\sum_{i=1}^{M} \sum_{j=1}^{N} (S_{ij})^2 / MSE \right) \quad (5)$$

Table 3. Results of PSNRS and MSE Values for the LSBMR-GA algorithm

Image	PSNR		MSE	
	LSBMR	LSBMR-GA	LSBMR	LSBMR-GA
Lena	47.34	48.55	0.00098	0.00082
Baboon	47.91	48.63	0.00087	0.00079
Foveon	46.54	47.89	0.00095	0.00081
Deer	46,71	47.91	0.00097	0.00089
Lichtenstein	47.82	48.92	0.00099	0.00082

V. CONCLUSION

Image Steganography systems scale up and become increasingly complex in their optimization techniques facing new challenges. Conventional image steganography methods become fragile and show poor performance. Lot of optimization techniques have long been proposed to improve the hiding capacity of the stego images. This paper designs the idea of optimizing the region using Genetic Algorithm which is a conventional bio-inspired optimization technique used in engineering problems. The task of optimization technique is to regions the message to embed on the cover image. This paper designs LSBMR-GA systems, with detailed design that meets all requirements. The results of LSBMR-GA evaluation suggest that when the exact regions with correct threshold value are selected, the method offer high embedding capacity of about 20-25%. Decrypting trustworthiness is enhanced with the increase in number of iterations, when set of parameter values are fixed. The algorithm is verified to be secured against stego test based on high order statistics. Other steganography methods such as audio/video steganography in the spatial or frequency domains in providing the less embedding rate than the maximal amount is considered as a future work.

REFERENCE

[1] C.H.Yang, C.Y Weng, S.J.Wang et al., "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, Vol.3, No.3, pp488-497,2008. | [2] Weiqi Luo, Fangjun Huang, Jiwu Huang,"Edge Adaptive Image Steganography Based on LSB Matching Revisited" IEEE Transactions on Information Forensics and Security, Vol.5 No.2, pp 201-214,June 2010. | [3] Mahdi Ramezani, Shahrokh, "Adaptive Image Steganoraphy with Mod-4 Embedding using Image Contrast",IEEE CCNC 2010 Proceedings. | [4] M.Ramezani and S.Ghaemmaghami, "Towards Genetic Feature Selection in Image Steganalysis," in 6th IEEE International Workshop on Digital Rights Management, Las Vegas, SA, 2010, PPT. | [5] Mielkainen, "LSB matching revisited,"IEEE Signal process Lett., vol. 13no. p. 285 – 287, May 2006 | [6] S. Dumitrscu, X. Wu . and Z. Wang, Detection of LSB steganography via Sample pair analysis,"IEEE Trans. Signal process., Vol. 51. no. 7. pp.1995 – 2007, Jul. 2003. | [7] Weiqi Luo,Fanggjun Hunang and Jiwu Huang,"Edge Adaptive Image Steganoraphy Based on LSB Matching Revisited"IEEE Transactions on Information Forensics and Security,vol.5, No 2,June 2010 | [8] Ran-Zan Wang,Chi-Fang Lin,Ja-Chen Lin "Image Hiding by optimal LSB substitution and genetic algoritm",Pattern Recognition Society, Published by Elsevier Science Ltd. pp.671-683,2001. | [9] R.Z. Wang and C.F. Lin: ImageHiding by Optimal LSB Substituition and Genetic Algorithm, Pattern Recognition, ELSEVIER, Vol. 34, (2001)671-883. | [10] T. Zhang and X. Ping: A New Approach to Reliable Detection of LSB Steganography in Natural Image, Signal Processing Journal, ELSEVIER, Vol.83 May(2003) 2085- 2093. | [11] Information Hiding Techniques for steganography and Digital Watermarking. S. Katzenbeizzer and F.A.Petticolas, eds. Artech House, 2000. | [12] R.J. Anderson, "Stretching the Limits of Steganography," proc. First International workshop Information Hiding (IH '96), pp. 39 – 48, 1996. | [13] R.J. Anderson, " Stretching the Limits of Steganography," proc. First International workshop Information Hiding (IH '96), pp. 39 – 48, 1996. | [14] C. Cachin,"An Information-Theoratic Model for Steganography", proc. Second InInt'l Workshop Information Hiding (IH '98), pp. 306 -318, 1998. | [15] J.Zollner,H.Federrath, H.Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G.Wicke, and G.Wolf, "Modelling the security of steganographic Systems," proc. Second Int'l Workshop Information Hiding (IH '98), pp. 344 – 354, 1998. | [16] C.T.Hsu,J.L.Wu,Hidden digital watermarking in images,IEEE Transactions on Image Processing,vol 8,pp 58-68,1999. | [17] C.K.Chan and L.M. Chen " Hiding data in images by simple LSB substituition,"Pattern Recognit., vol. 37, no. 3 pp 469-474, 2004. | [18] C.C.Chang and H.W.Tseng ,"A steganographic method for digital images using side match,"Pattern Recognit. Lett. vol 25, no, 12 pp. 1431-1437, 2004. | [19] H.C.Wu aN.I. Wu C. S Tsai and M.S. Hwang,"Image Steganographic scheme based on pixel- value differencing and LSB replacement methods", proc. Inst. Elect. Eng. vis Image Digital Process. vol. 152. no. 5, pp. 611-615, 2005. | [20] Y.R.Park , H. H. Kang , S. U. Shin and K. R. Kwon, A steganographic scheme in digital Images Using Informatio of Neighbouring Pixels. Berlin, Germany: Springer-Verlag, 2005, vol. 3612, pp/ 962-968. | [21] X. Li. T.Zeng. and B.ang,"Detecting LSB matching by applying calibration technique for difference image", in proc. 10th ACM Workshop on multimedia and security, Oxford, UK., 2008. pp. 133-138. | [22] Y.Q. Shi et al. " Image Steganalysis based on moments of characteristic functions using Wavelet decompostitions prediction-error image. and neural metwork." in proc. IEEE Int. Conf. Multimedia and Expo. Jul. 6-8, 2005. pp. 269-272. | [23] K. Hempstalk ,"Hiding Behind corners: Using edges in images for better steganography", in proc. Computing Women's Congress. Hamilton, New Zealand. 2006. |