

Steganographic Data Hiding using Modified APSO

E Divya

Nehru College of Engineering and Research Centre/Electronics and Communication, Thirissur, India
E-mail: eddivs@gmail.com

P Raj Kumar

Nehru College of Engineering and Research Centre/Electronics and Communication, Thirissur, India
E-mail: qraj2014@gmail.com

Abstract—In this paper we are analyzing the steganographic data hiding using the least significant bit technique. This paper describes the particle swarm optimisation. The particle swarm optimisation algorithm is applied to the spatial domain technique. The improved algorithm called the accelerated particle swarm optimisation converges faster than the usual particle swarm optimisation and improves the performance. This paper also analyses the modified particle swarm optimisation on the spatial domain technique which improved the PSNR and also reduced the computation time.

Index Terms—Chi-Square Test, Histogram error, LSB, PSO, APSO, PSNR., MSE, SSIM.

I. INTRODUCTION

In recent times it has been noted that the Internet, an easy medium of information interchange is very much prone to hacking. Information hiding, notably within images and videos has been the subtle mechanism of conveying critical evidence. Steganography is the much applied and tested application of information hiding for the purpose of secret communications. Steganography and Watermarking are both used to ensure data confidentiality. The main difference between them is that Watermarking preserves the cover by using the constant hidden text for authentication, while Steganography uses the cover as an innocuous means of conveying variable hidden messages. In Steganography, a covert message can be hidden in various cover media such as digital images, audio, video, TCP/IP packet headers and very recently GPRS packet headers. The digital image is currently one of the most popular media on the Internet for carrying stealth messages. The cover-image with some hidden data is referred to as stego-image and the marvel of the stealth communication lies in the over-all resemblance of the cover and the stego as identified by the human eye. There are a number of steganographic methods in practice and they are classified into substitution methods and transform techniques. All these techniques aim for good security as well as capacity of data hiding. These mechanisms use an innocuous image

referred to as cover image onto which the secret message is impregnated to generate a stego image. Recent research has focused a lot on the Least Significant Bit (LSB) substitution approach that could be applied to the spatial pixel domain directly with a number of variants. This is the most popular and simplest way of embedding textual messages. The basic idea here is to embed the secret message in the least significant bits of the image. The information stored in the least significant bit positions of the pixels could be considered as random noise. So altering them does not significantly affect the quality of the cover and so it can easily pass the HVS test. The popular procedure for such technique is to convert the desired hidden message into binary form and then embed each bit into a LSB bit of the cover image. Different variants to the basic LSB technique include LSB matching, Pixel Value Differencing (PVD) and Optimal Pixel Adjustment Process (OPAP). In LSB matching, if one secret bit does not match the LSB of the cover image, then another one will be randomly added or subtracted from the cover pixel value. PVD methods calculate the difference between two consecutive pixels to determine the depth of embedded bits. OPAP can improve efficiency and enhance visual quality of the stego image.

Transform domain techniques apply the Discrete Cosine transform (DCT) or the Discrete Wavelet Transform (DWT) or the Discrete Fourier Transform (DFT) to the cover image and embed the message by modulating coefficients in the frequency domain. These techniques are more robust towards frequency based attacks but are more prone to geometric attacks as the distortions introduced by the embedded data into the transform coefficients will spread over all the pixels in the spatial domain. Although the changes introduced in these pixel values are visually negligible, yet the overall image quality is affected. Security of Steganographic communications is a very serious matter. Several researchers, noteworthy among them Cachin have formulated qualitative measures for security of transmission. Security can be broadly defined as the undetectability of whether a cover contains hidden messages or not and is the basis for any Steganographic scheme [1]. Cachin has formulated the ϵ -secure measurement, where ϵ is the Kullback-Leibler (KL)

divergence between the distribution of the cover image and that of the stego image. This KL divergence introduced by the Steganographic scheme must be as small as possible close to zero. This is the figure of merit used in most data hiding mechanisms. The Image Quality Metrics (IQMs) used are Peak signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Index (SSIM) and these help to practically compare the stego and the cover [3, 4]. The main aim of the research is to maintain imperceptibility and improve stego quality and also achieve high embedding capacity. Most commonly used Steganographic techniques target the degree of secure encoding as a measure of successful information hiding, due to the reason that steganalytic mechanisms try to break the data hiding by analyzing some statistical features of the stego that can expose the presence of hidden data. Typically steganalysis methods inspect the histograms of cover and stego for any changes that signal presence of hidden data. More powerful technique involves Chi-square analysis [4, 5].

Particle Swarm Optimization (PSO) is a powerful heuristic algorithm that can be applied for non-linear optimization problems. It is a population based stochastic optimization technique developed in 1995 by Dr. James Kennedy and Dr. Russell Eberhart [6]. PSO algorithm can be used to find optimal solution to numerical and qualitative problems. On the one hand, PSO has roots in bird flocking, fish schooling and swarming theory in particular, and on the other hand, it is closely related to evolutionary computation such as Genetic Algorithms (GA). Compared to GA, it is much simpler, implementation can be done in a few line of coding and has been found to be computationally inexpensive in terms of both memory requirements and speed. Although like most other stochastic optimization schemes, it consumes time, yet, convergence is found to be much easier. A detailed study by Elbeltagi et al has compared other evolutionary based algorithms such as GA, Ant Colony Optimization, and Shuffled Frog Leaping with PSO and concludes that PSO method outperforms the others in terms of success rate, solution quality and processing time [12].

Similar to Particle Swarm optimization the accelerated particle swarm optimization is also simple but it converges faster compared to this simple particle swarm optimization[7]. Since accelerated particle swarm optimization converges more faster, accelerated particle swarm optimization along with mutation operator improves the performance and decreases the computation time.

II. LEAST SIGNIFICANT BIT METHOD

Least significant Bit method (LSB) is one of the simplest and greatly used methods in steganography. Here the least bit is interchanged with a single bit of secret image. Here the message is stored in the LSB of each pixel value of cover image. When converting an analog image to digital format, we usually choose between three different ways of representing colours:

- 24-bit colour: every pixel can have one in 2^{24} colours, and these are represented as different quantities of three basic colours: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- 8-bit colour: every pixel can have one in 256 (2^8) colours, chosen from a palette, or a table of colours.
- 8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray

Let's see the pixels before the insertion for a 24 bit:

- **10000000,10100100,10110101,10110101,11110011,**
- **10110111,11100111,10110011,00110011**

We need to hide a value say 30 whose binary is 11110 which after embedding becomes

- **10000001,10100101,10110100,10110101,11110010,**
- **10110111,11100111,10110011,10011001**

Let's see the pixels before the insertion for a 8 bit:

- **10000000,10100100,10110101,10110101,**
- **11110011,10110111,11100111,10110011**

We need to hide same value say 30 which after embedding becomes

- **10000000,10100101,10110101,10110101,**
- **11110010,10110111,11100111,10110011**

In both cases only three bits changed according to the message data, this small change is not visible to the normal human eye. So this method is more easy to implement but it is more vulnerable to attack. LSB method has good payload capacity and takes less time. Here the message can be protected by using two way key. LSB generally uses BMP images.

Algorithm for LSB

- Step 1. Read the cover image and the secret message or image to hide
- Step 2. Convert the message into binary bit stream.
- Step 3. Embedding the secret data using LSB operation.
- Step 4. Get the inverse transform. Step5: Write the stego image.

III. PARTICLE SWARM OPTIMISATION

It is a optimisation technique proposed by Kennedy and Eberhart in the year 1995 .The algorithm simulates the behaviour of bird flock flying in multidimensional space(like they fly in the sky for better food) search of food or for optimum place by adjusting their movements for a better place. The computation is similar to Genetic algorithm. Each particle or individual in the population (swarm) represents a potential solution. These particles

are flying through a multidimensional search space, where the position of each particle is adjusted according to its own experience and that of its neighbours. The swarm or particles are initialised randomly and then search for optimal solution. All the particles have fitness values which are calculated by the objective function to be optimised and have velocities which direct the movement of the particles. Let X_i denote the position of the particle and this position is changed by adding a velocity component V_i to it.

$$V_i = w * V_i + c_1 * rand_1 * (pbest_i - X_i) + c_2 * rand_2 * (gbest_i - X_i) \quad (1)$$

$$V_i = X_i + V_i \quad (2)$$

The experiential knowledge of a particle is generally referred to as the cognitive component, which is proportional to the distance of the particle from its own best position found since the first time step. The socially exchanged information is referred to as the social component of the velocity equation. c_1 and c_2 are the cognitive and social components and c_1+c_2 can be maximum upto 4. The personal best position $pbest$ associated with particle i is the best position the particle has visited since the first time step. $gbest$ is the global best position for the PSO. r_1 and r_2 are the two random numbers in the range $[0,1]$. $C * W$ is the inertia weight introduced to control and balance the exploration and exploitation trade off. W changes according to the number of iteration and the maximum value of w achieved is 0.99. C is taken to be 1.

The following objective functions will be minimized by PSO. $Fitness(C, S) = PSNR(C, S)$ where, C and S are original and stego images respectively.

A cover image is loaded in which the secret message is to be embedded. To begin with, simple LSB substitution method is applied on the cover and the resulting stego image is obtained [8]. The difference between the cover image and the obtained stego image is calculated through the image quality measures such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Structural Similarity index (SSIM). These measures are computed using MATLAB which takes as input the original cover image and the stego image [8]. After that, in order to improve the image quality, PSO algorithm is run on the image in order to get the best optimized positions in the form of 2D coordinates of the image pixel values where hiding of message bits can be done. The objective function for the PSO is set keeping in mind that an ideal objective function should be able to correctly identify and minimize the three factors of the image quality: i) the amount of image distortion ii) the type of distortion, and iii) the distribution of error [22]. To apply the algorithm the following steps were utilized:

Algorithm For PSO

- Step 1. Start the iteration.
- Step 2. Generate the number of particles and velocities,

initialise the population.

- Step 3. For each iteration find the global best position and local best for each iteration.
- Step 4. Update the velocity and position using equation 1 and 2.
- Step 5. Stop the iterations.

IV. ACCELERATED PARTICLE SWARM OPTIMISATION

PSO is similar to genetic algorithm but is not complex like genetic algorithm. It has shown good performance improvement when applied to data hiding algorithms. There are many variants of PSO. Till now the variants in PSO has been studied. The accelerated particle swarm optimisation is a variant of PSO. But compared to PSO it has shown faster convergence. APSO was developed by Xin She Yang in 2010.

The movement of swarming particles has a global best position and local best position. The PSO uses both the global best and local best to update the particle velocity and position. The individual best is used to increase the diversity in the search space and there is no compulsion in using this so in APSO we are concentrating only on the global best position so that convergence will be fast.

In APSO we can update the position and velocity using the simpler equation given below

$$V_i = V_i + \alpha \varepsilon_n + \beta * (gbest_i - X_i) \quad (3)$$

ε_n is a random vector in the interval $(0,1)$.

$$V_i = X_i + V_i \quad (4)$$

The rate of convergence increases with the above equation but the rate of convergence can be further increased by the particle in single step

$$X_{i+1} = (1 - \beta)X_i + \alpha \varepsilon_n + \beta * (gbest_i - X_i) \quad (5)$$

Where the α ranges from 0.1 to 0.4 and β ranges from 0.1 to 0.7

In the above equation we are taking only the global best into consideration so to increase the performance we can apply the cauchy mutation which considers only the global best.

Cauchy Mutation

There are many variants of PSO cauchy mutation is one of these. But one of the problem found in the PSO is that it easily fall to local optima. Once it falls to the best optima it can converge faster. Since APSO uses only the global best the cauchy mutation when applied improves the performance.

$$f(x) = \frac{1}{\Gamma} * \frac{t}{(t^2 + x^2)} \quad (6)$$

and the cauchy distribution function

$$F(x) = \frac{1}{2} + \frac{1}{\pi} \arctan\left(\frac{x}{t}\right) \quad (7)$$

The mutation operator increases the probability from escaping to local optima. Through the Cauchy mutation the whole particle moves to the global best in every generation.

$$W_i = \sum V_{(i,j)} / (\text{popsize}) \quad (8)$$

Where $W(i)$ is a weight vector within the interval $[-W_{\max}, W_{\max}]$, $V(j)(i)$ is the velocity vector and popsize is the population size of the particle. The global best position is calculated as given below:

$$gbest_i = gbest_i + W_i * N(x_{\min}, x_{\max}) \quad (9)$$

Where N is a Cauchy distributed function with scale parameter $t=1$ and $N(x_{\min}, x_{\max})$ is a random number.

Here the aim is to decrease the computation time and improve the PSNR. So, the following steps are followed:

Algorithm For APSO

- Step 1. Start the iteration.
- Step 2. Generate the number of particles and velocities, initialise the population.
- Step 3. For each iteration find the global best position.
- Step 4. Update the velocity or position using equation 3 or 5.
- Step 5. Apply global the Cauchy mutation operator using equation 9.
- Step 6. Stop the iterations.

V. PERFORMANCE MATRICES

Performance of the above techniques are compared using the Mean square error, Peak signal to noise ratio and computation time.

(i). Mean Square Error

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image

$$MSE = \frac{1}{W * H} \sum_{i=1}^W \sum_{j=1}^H ([S(i,j) - C(i,j)])^2 \quad (10)$$

Where $S(i,j)$ and $C(i,j)$ represent the pixel gray values of the stego-image and the cover-image in the position (i, j) respectively, and W and H represent the pixel numbers of the width and the height of the cover-image respectively.

(ii). Peak Signal to Noise Ratio

To compute the peak signal to noise ratio (PSNR), the following equation holds:

$$PSNR = 10 * \log_{10} \left(\frac{255 * 255}{MSE} \right) \quad (11)$$

(iii). Structural Similarity Index

The main issue with PSNR is its inflexibility to image transformations [13] and so the Structural Similarity between the Cover and Stego is to be taken recourse to.

Structural Similarity Index (SSIM) measures [9, 13] the similarity between two images and is quantitatively stated as:

$$SSIM(x, y) = \frac{2(\hat{x}\hat{y} + c_1)(2\sigma_{xy} + c_2)}{(\hat{x}^2 + \hat{y}^2)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (12)$$

Where x and y are corresponding windows of the same size of the original and stego images and \hat{x} and \hat{y} are the corresponding averages of x and y respectively.

σ_x^2 and σ_y^2 are the corresponding variances of x and y and σ_{xy} is the covariance of x and y .

c_1 and c_2 are appropriate constants.

VI. SECURITY OF DATA HIDING-STEGANALYSIS

It is the method to detect presence of any embedded data. The purpose of steganalysis is to find any secret message in an image. Many researches are going on in this area. So it is said to be successful if an image contains message or not. It may also find information of the image, hidden message and type of embedding algorithm based on the type of method. There are many steganalysis methods available. But each is specific to a particular method. Here the two steganalysis techniques basically the histogram attack and chi-square attack are analysed.

A) Histogram Attack

Histogram analysis is done visually by plotting the histogram of both stego and cover and analysis is done using this histogram plots.

B) Chi-square Attack

It was suggested by Andreas Westfeld and Andreas Pfitzmann in the year of 1999. It compares the statistical properties of the stego image with that of expected statistical properties cover image.

The average number of each pair of values is given by

$$N_i = \frac{n_i + n_{i+1}}{2} \quad (13)$$

And the chi-square is calculated using the formula

$$\chi^2 = \frac{n_i + N_i}{n_i} \quad (14)$$

The chi-square result is based on the dissimilarity and is considered as an apt thing and provides a quantifiable result.

VII. RESULTS AND DISCUSSIONS

The experiments were conducted on MATLAB IDE using the standard 8-bit gray scale images and the payload [8] for the LSB embedding with and without PSO to test the efficacy of the optimization. Four grayscale images were used in the experiments. A message of length 72 characters was deployed. To begin with the simple LSB hiding technique [8] is applied and the values of the various image quality measures are calculated.

The image quality measures used to measure the image quality of the obtained stego image are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM). Then the PSO approach was applied after finalizing the objective function. The various parameters in the PSO function were set by using the approach advocated in [9,23] and PSO is run in order to minimize the objective function. The number of iterations was initially fixed for 1000 with number of particles as message size. Convergence was an issue and a lot of parameter tweaking was used to get worthwhile results. An array is created that stores the XY indexes corresponding to the global best value for every iteration. The resulting pixel coordinates are then used for hiding the message to get the stego image after embedding the message bits using the basic LSB algorithm. Then again the IQMs are estimated. Several trials were made with the four basic images and the results are tabulated below. The computing times were generally more with the optimization used. The results show that the optimization approach yields lesser Mean Square Error in each case of the image used for the given payload and there is appreciable improvement in the PSNR as well as the SSIM.

Table 1. Comparison of Performance Parameters

Image	Simple LSB Without PSO			LSB with PSO		
	MSE	PSNR	SSIM	MSE	PSNR	SSIM
Airplane	0.4236	51.8612	0.9972	0.3694	52.4558	0.9984
Lena	0.4168	51.9315	0.9987	0.3946	52.1692	0.9992
Baboon	0.5407	50.8012	0.9949	0.5123	51.0355	0.9964
Cat	0.4350	51.7459	0.9902	0.3874	52.2492	0.9907

The Chi square attack is very simple and has been advocated to prove the security of proposed method. The purpose of this attack is to show that the probability of distribution of zeros and ones in stego-image and find the statistical evidence that is left by the embedding process [5]. The result of probability will be 50% that means half

of the numbers of bits are zero or one when the bits generates randomly in secret message. Pair of value (POV) is one of the results of an embedding algorithm which means the values of the pixel were embedded into one another. POV is a detection algorithm which is designed to perform chi-square attack on image and the output is the probability of embedding [24]. The chi square algorithm is performed in MATLAB for the series of cover and stego images, considering both the conventional and PSO based results.

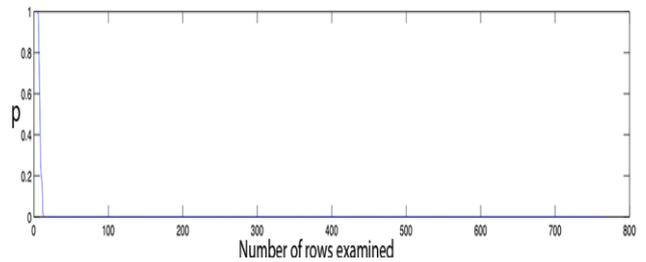


Fig.1. Unmodified Image

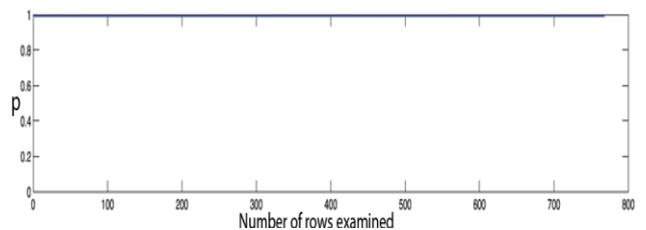


Fig.2. Image with Message Embedded

When the optimization scheme was used to hide the data results shows that the technique based on Particle Swarm Optimization achieves high data embedding capacity and minimizes distortion between cover image and the stego image and provide good security of data hiding

The results above compared the simple LSB and LSB with PSO. From the results it revealed that PSO gives higher PSNR rather than simple LSB. The results below compares the LSB with simple PSO and with modified PSO. The message length increased to a 565 character. The text message was embedded in cover using simple LSB, LSB with PSO and LSB with modified PSO. The results are compared and tabulated below. 100 of iterations was used both for PSO and APSO. The PSO gave better PSNR after 100 iterations.

But to converge faster we are going for accelerated PSO. To improve the performance further the Cauchy mutation operator is applied to it. Cauchy mutation also converges faster and speeds up the process.

The table below reveals the modified PSO algorithm gave the better PSNR than simple PSO. The computation time and mean square error also decreased showing the algorithm offers high payload size.

The simulation results of the images Babbon, lena and cameraman with their corresponding histogram plots of both stego and cover are shown below. Both cover and stego images doesn't show any difference visually even after embedding 565 character word.

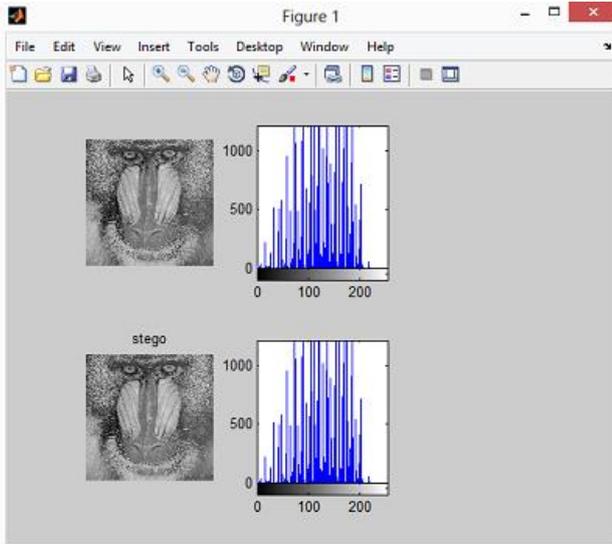


Fig.3. Simulation Result of Baboon using LSB PSO

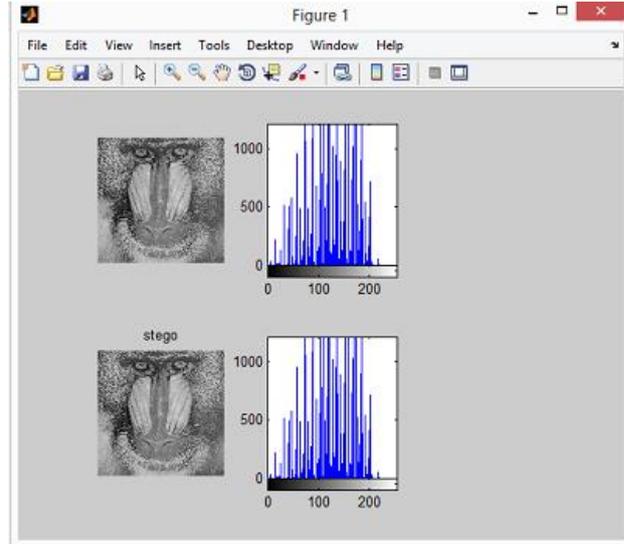


Fig.6. Simulation Result of Baboon using LSB Modified APSO

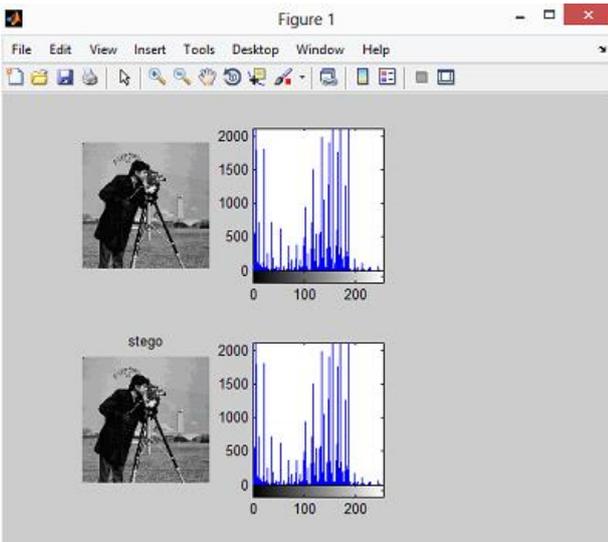


Fig.4. Simulation Result of Cameraman using LSB PSO

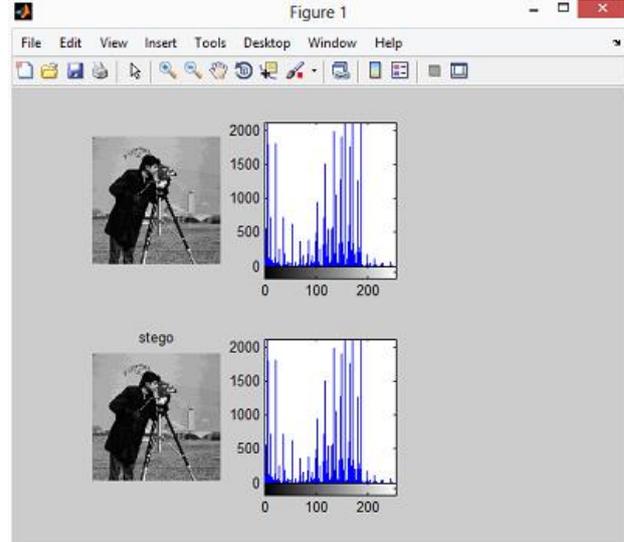


Fig.7. Simulation Result of Cameraman using LSB Modified APSO

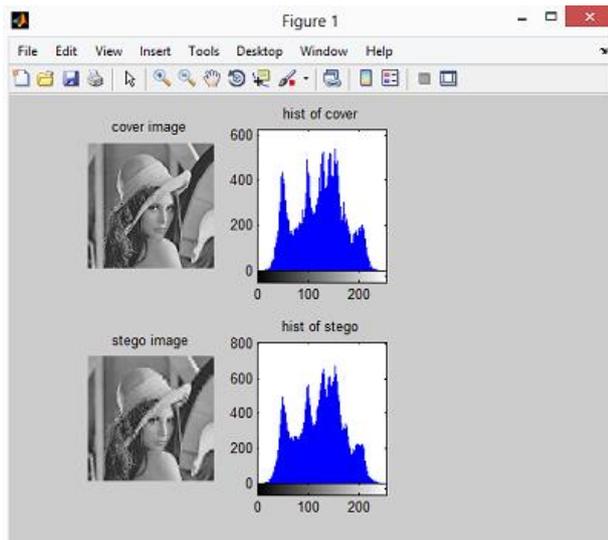


Fig.5. Simulation Result of Lena using LSB PSO

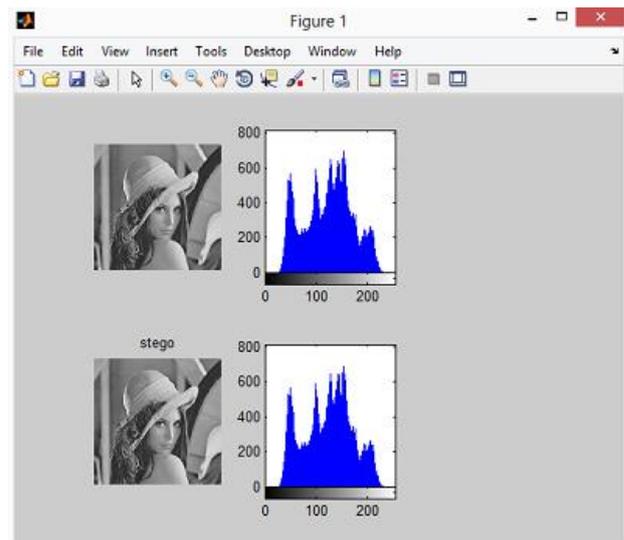


Fig.8. Simulation Result of Lena using LSB Modified APSO

Table 2. Comparison of PSNR

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	49.9304	69.611	73.05
Cameraman	49.9811	69.66	73.43
Lena	50.3016	69	73.14

Table 3. Comparison Of MSE

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	0.66	0.0052	0.0032
Lena	0.6582	0.0064	0.0030
Cameraman	0.6114	0.0055	0.0032

Table 4. Comparison of Computation Time (in seconds)

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	0.424	24.49	21.5
Lena	0.425	24.2	21.5
Cameraman	0.4250	25.019	22.5

In order to check the security of data hiding using the modified PSO, analysis of all the algorithm was carried out. The histogram analysis was done visually by plotting the histogram of the cover image and stego image. The histogram plots of all the results reveals the embedded message cannot be detected visually. Histogram test gave zero error for PSO and APSO. This is where the histogram analysis or the first order statistics fails so the second order statistics, i.e., the chi-square test is applied for checking the security.

The chi-square test reveals that the modified APSO is more secure compared to the simple LSB and LSB PSO

Table 5. Comparison of Histogram Test

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	63.9707	0	0
Lena	64	0	0
Cameraman	64	0	0

Table 6. Comparison of Chi-Square Test

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	246.7	16.62	13.7413
Lena	1221.36	82.2954	68.0169
Cameraman	1723.7	427.266	352.52

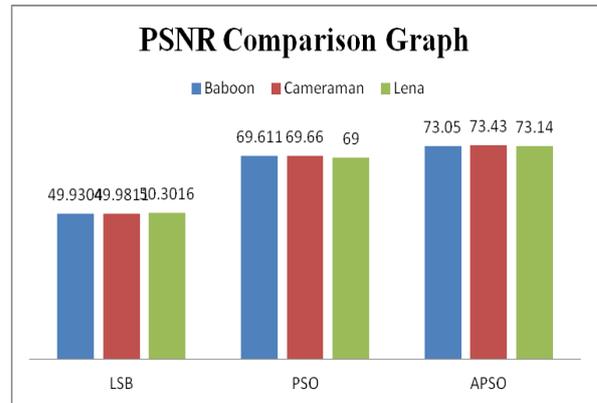


Fig.9. Comparison of PSNR Graph for LSB, PSO, APSO

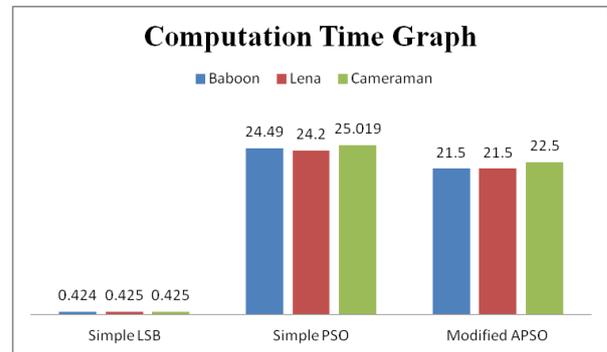


Fig.10. Comparison of Computation Time Graph for LSB, PSO, APSO

The text message was used to hide in the cover image. Instead of using a text message an image can also be hidden in an image. The zebra image was hidden in both Baboon and Cameraman test images. The simulation results of modified APSO are provided below. The performance of all the three, i.e., simple LSB, PSO and modified APSO of hiding an image is tabulated below. The security of data hiding was also analyzed for the above three.

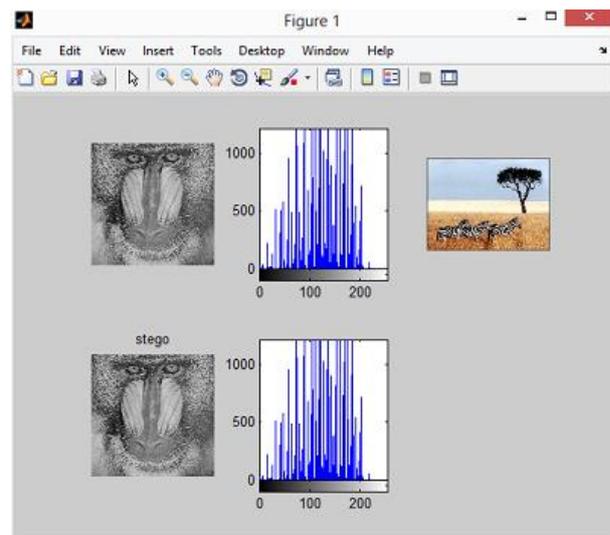


Fig.11. Simulation Result of Baboon Hiding Zebra using LSB Modified APSO

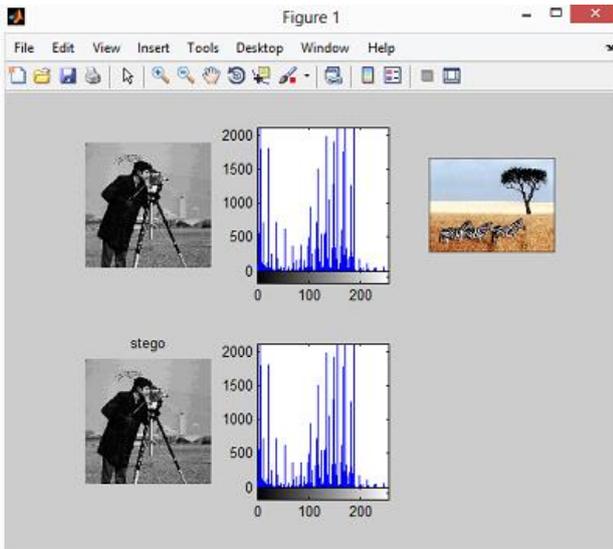


Fig.12. Simulation Result of Cameraman Hiding Zebra using LSB Modified APSO

Table 7. Comparison of PSNR

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	55.4992	75.9	78.89
Cameraman	56.1697	76.611	79.58

Table 8. Comparison of MSE

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	0.1847	0.0017	0.00154
Cameraman	0.1583	0.0014	0.00132

Table 9. Comparison of Computation Time

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	0.533	53.6	46.54
Cameraman	0.575	52.05	47.55

Table 10. Comparison of Histogram Test

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	63.97	0	0
Cameraman	64	0	0

Table 11. Comparison of Chi-Square Test

IMAGE	Simple LSB	Simple PSO	Modified APSO
Baboon	246.7	13.74	13.7413
Cameraman	1723.7	352.1	352.52

VIII. CONCLUSION

The main objective of this work was to apply optimization to hide the secret data messages effectively within innocuous cover images to ensure good hiding capacity, good security, distortion less transmission and effective recovery of the hidden messages without corruption. The optimization scheme used was Particle Swarm Optimization that provides the best pixel positions in the cover image that can be used to embed the secret message bits so that less image distortion occurs. The image quality measures were calculated to compare the results of simple LSB hiding in random pixels without using PSO algorithm and with the method based on PSO. Experimental results show that the technique based on Particle Swarm Optimization achieves high data embedding capacity and minimizes distortion between cover image and the stego image and provide good security of data hiding.

The modified APSO converges faster than the PSO and when applied to LSB improved the performance (PSNR) and also decreased the computation time. This modified APSO improves PSNR as well as decreases the computation time. This algorithm is also having high payload capacity and high security. This can further be applied to other techniques and also in audio, videos, artificial and neural network.

ACKNOWLEDGMENT

This work is a part of the first author’s master research work done under the auspices of nehru college of engineering and research centre. the first author expresses her gratitude to prof.p.rajku mar, for his much valued guidance.

REFERENCES

- [1] A. P. Fabien, R. J. Anderson, and M. G. Kuhn. Information hiding—a survey. *Proceedings of IEEE Special Issue on Protection of Multimedia Content*, 87 (1999)7, 1062–1078.
- [2] Ingemar J. Cox et al., *Digital Watermarking and Steganography*, Morgan Kaufmann, Burlington, USA, 2008.
- [3] C. Cachin, “An information-theoretic model for steganography,” *Proc.2nd International Workshop Information Hiding LNCS 1525*, pp. 306–318, 1998.
- [4] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, “Image Steganography: Concepts and Practice”, *WPSC/Lecture Note Series*, pp.3, April, 2004. Source: www2.ims.nus.edu.sg/preprints/ab2004-25.pdf.
- [5] Chandramouli, R., M. Kharrazi, and N. Memon, *Image Steganography and Steganalysis: Concepts and Practice*
- [6] J. Kennedy and R.C. Eberhart, *Particle Swarm Optimization*, *Proceedings of IEEE International Conference on Neural Networks*, IEEE Service Centre, Piscataway, nJ, vol. 5, no. 3. pp. 1942-1948, 1995.
- [7] X.Li, J.Wang, A Steganographic method based upon JPEG and Particle Swarm Optimization, *Information Sciences* 177 (2007) 3099-3109.

- [8] Rajkumar P, R.Kar, A.K.Bhattacharjee, Dharmasa, "A Comparative analysis of Steganographic Data Hiding within digital images", International Journal of Computer Applications, September 2012.
- [9] Bedi.P, et al., Using PSO in Image Hiding Scheme Based on LSB Substitution. Springer-Verlag Berlin Heidelberg A braham. A et al. (Eds.): ACC 2011, Part III, CCIS 192, pp 259-268, 2011.
- [10] Bajaj.R et al., Best Hiding Capacity Scheme for Variable Length Messages Using Particle Swarm Optimization. SEMCCO 2010, LNCS 6466, pp 230-237, Springer-Verlag Berlin Heidelberg 2010.
- [11] Braik. M et al., Image Enhancement Using Particle Swarm Optimization. Proceedings of the World congress on engineering 2007 Vol 1 WCE, 2007, July 2-4, 2007, London, U.K.
- [12] Fazli, S, Kiamini, M, A High Performance Steganographic Method using JPEG and PSO algorithm, In: IEEE International Multitopic December 24, 2008.
- [13] Zhou Wang, Alan C. Bovik, Hamid R. Sheikh, and Eero P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 4, APRIL 2004
- [14] Yanqing .G, Xiangwei.K, Xingang.Y., Secure Steganography based on Binary Particle Swarm Optimization, September 4, 2008 Journal of Electronics China
- [15] J. Zollner, H. Federrath, H. Klimant, A. Pitzman, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the security of steganographic systems." 2nd Information Hiding Workshop, pp. 345-355, April 1998.
- [16] Wu, M.-N., M.-H. Lin, and C.-C. Chang, A LSB Substitution Oriented Image Hiding Strategy Using Genetic Algorithms Content Computing, 2004, Springer Berlin / Heidelberg. p. 219-229.
- [17] Mathkour, H., B. Al-Sadoon, and A. Touir A New Image Steganography Technique, in IEEE. 2008. p. 1-4.
- [18] Digital Watermarking, T. Kalker, I. Cox, and Y. Ro, Editors. 2004, Springer Berlin / Heidelberg. p. 204-211.
- [19] Wang, R.-Z., C.-F. Lin, and J.-C. Lin, Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition, 2001: p. 671- 683.
- [20] Zanganeh, O. and S. Ibrahim, Adaptive Image Steganography Based on Optimal Embedding and Robust Against Chi-square Attack. Information Technology Journal, 2011. 10: p. 1285-1294.
- [21] Walia, E., P. Jain, and N. Navdeep, An Analysis of LSB & DCT based Steganography. Global Journal of Computer Science and Technology, 2010. 10: p. 4-8.
- [22] Chan, Y.-K., Y.-A. Ho, and Y.-P. Chu, Image Hiding with an Improved Genetic Algorithm and an Optimal Pixel Adjustment Process, in IEEE. 2008. p. 320-325.
- [23] Bajaj, R., P. Bedi, and S. Pal, Best Hiding Capacity Scheme for Variable Length Messages Using Particle Swarm Optimization Swarm, Evolutionary, and Memetic Computing, 2010, Springer Berlin / Heidelberg. p. 230-237.
- [24] Westfeld, A. and A. Pfitzmann, Attacks on Steganographic Systems - Breaking the Steganographic Utilities EzStego in Citeseer. 2000. p. 1-4.
- [25] H. Wang et al., "Opposition-based particle swarm algorithm with Cauchy mutation," in Proceedings of the IEEE Congress on Evolutionary Computation, 2007, pp. 4750-4756.
- [26] Ratnakirti Roy, Suvamoy Changder¹, Anirban Sarkar¹, NarayanC Debnath, "Evaluating Image Steganography Techniques: Future Research Challenges" IEEE transactions 2013
- [27] Emad Elbeltagi, Tarek Hegazy, Donald Grierson, "Comparison among five evolutionary-based optimization 43-53.
- [28] N. Lavanya, V.Manjula, N.V. Krishna Rao, Robust and Secure Data Hiding in Image Using Biometric Technique, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5133 – 51.
- [29] K.Prajna,et.al, "A New Dual Channel Speech Enhancement Approach Based on Accelerated Particle Swarm Optimization (APSO)" ,I.J. Intelligent Systems and Applications, 2014, 04, 1-10 Published Online March 2014 in MECS.
- [30] E Divya and P Rajkumar titled "Image to Image Hiding Using PSO" in IJRAE, Issue 2, vol 5, May 2015.
- [31] E Divya and P Rajkumar titled "Steganographic Data Hiding in DWT Using PSO" in IJCA, vol 117, number 14, pp 30-34, May 2015.

Authors' Profiles



E DIVYA received her B.Tech Degree in Electronics And Communication Engineering in the year 2010 from College Of Engineering Thalassery. She is currently pursuing her Master From Nehru College Of Engineering And Research Centre Pampady (2013-2015). Her research interest include Signal and Image Processing.



P.Raj Kumar is working as Sr. Assistant Professor in ECE with NGI. He completed Bachelor in Engineering in 1987 and Master in Engineering in 1990 from PSG College of Technology. He is currently pursuing doctoral research. Areas of research interest include Image Processing and VLSI design.

How to cite this paper: E Divya, P Raj Kumar, "Steganographic Data Hiding using Modified APSO", International Journal of Intelligent Systems and Applications (IJISA), Vol.8, No.7, pp.37-45, 2016. DOI: 10.5815/ijisa.2016.07.04