International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

PSO (Particle Swarm Optimization) Based Reversible Data Hiding

Kritika Jaidka[1], Amandeep Mavi[2]

[1, 2] Department of Computer Science and Engineering, Chandigarh Engineering Collage Landran, Mohali

Abstract: ***Text fusion in images is an important technology for image processing. We have bulks of important information related to the reports and need lots of space to store and the proper position and name which relates that image to that data. The principle of separable reversible data consists of three steps in a first step we encrypt the host image with the help of encryption key, then in a second step we hide a text in image with data hiding key and in the last step we extract the data and recover the original image. The proposed work is based on AOI (area of interest). AOI is calculated with the help of particle swarm optimization for the particular image and will fuse the related document in that position or area and in this we use a text as a hidden data.***

Keywords: Image encryption, Separable Reversible Data Hiding, Particle Swarm Optimization

1. Introduction

Data hiding [1] is defined as embedding a secret message into a media context. Data hiding can apply to images, text, software, audio/video, etc. But when we are hiding the covet information into an image, it destroys the host image after extracting the covert information. In various application area like military, medical, artwork preservation and law enforcement, etc. disfigurement of an image is unsuitable. For example, in case of Medical area, slight alterations in an image can origin the risk of physician mistake in the image so that RDH Technique is introduced to solve the difficulty of lossless embedding of message in digital images. Reversible Data hiding is defined as after the embedding covert information is extracted [2], the image can be restored completely as original one. Many reversible data hiding techniques are proposed recently [3] - [5]. Reference [3] proposed a Reversible data hiding based on Genetic algorithm. In this paper optimized region is selected with the help of Genetic algorithm and in that reserved regions data hider hide a data. Using genetic algorithm good image quality is achieved. Paper [4] proposed iterative strategy is present to compute the optimal value transfer. In this work host image is split into no. of subsets as well as secret data are also divided into subsets and subsets of auxiliary information is always embedded in the estimation error in the next subset. In this paper Secret and auxiliary information is used for image recovery, and transfer by the difference between original pixel value and corresponding values from a neighbor. With this method better performance is achieved. [5] Proposed a concept of separable reversible data hiding technique. First of all, in this paper use text as the data and large amount of data is to be hide into the image and at receiver side after extracting the data unite quality index and higher PSNR are observed.

This paper is organized as follows. Section II justifies the detail about Particle swarm optimization (PSO). Section III details the proposed work. Section IV experimentally compares the proposed Work with Existing Work. Section V concludes the Paper.

2. Particle Swarm Optimization

Particle swarm optimization is first introduced by Kennedy and Eberhert in 1995.PSO (Particle swarm optimization) is an evolutionary computation model and inspired by birds Action. In this optimization technique each and every particle of swarm proceeds repetitively to predict the best position. A particle of swarm finds the best position using its own experience and global best position is predicted by using the best experience of whole swarm. The best solution is given by the best experience of whole swarm. [6] .PSO has two major component techniques first one is artificial life and the second one is fish schooling, Bird flocking and swarming theory.

3. Proposed work

There are two types of techniques are used in reversible data hiding. First one is Non-Separable Reversible Data hiding and Separable Reversible data hiding. In proposed work Separable Reversible Data Hiding technique is used. It consists of three phase's image encryption, data embedding, data extraction /image recovery. At sender side, First of all image is encrypted with the help of encryption keys and then data hider hide a data into a particle position with the help of data hiding key as shown in Fig.1

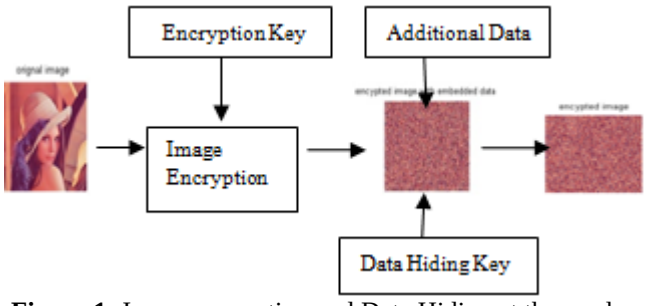

Figure 1: Image encryption and Data Hiding at the sender side

After hiding the data into an image, then encrypted image containing data is sent to the receiver. At the receiver side, there are three cases:

Case 1: If the receiver has data hiding key, then the receiver can extract data with the help of key but he does not know the image content. Fig 2 shows the case 1 on the receiver side

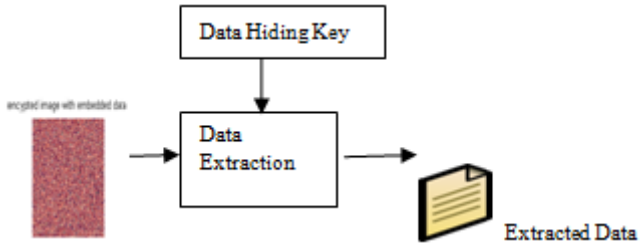

Figure 2: the receiver has Data hiding key

Case 2: If the receiver has decryption key, the receiver can extract decrypted version of image with the help of key but he does not know the data content. Fig 3 shows the case 2 on the receiver side

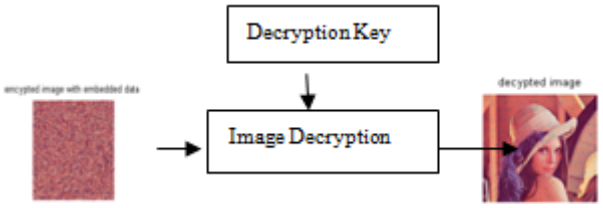

Figure 3: Receiver has decryption key

Case 3: If the receiver has both key (Data hiding Key and Encryption Key) then receiver extract data as well as image as per term as shown in Fig. 4.

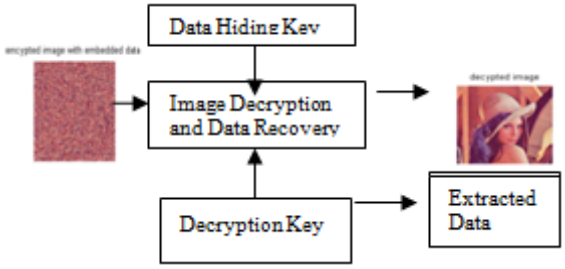

Figure 4: Receiver has both keys

There are three phase done in, separable reversible data hiding. First one is image encryption, Data embedding and image recovery and data extraction as same as original one

3.1 Image Encryption

In this phase, Import RGB image and also import data into the MatLab environment. Sender Pick a RGB host image and implement an encryption algorithm to an image. Algorithm used for image encryption is Random-Hash-generation. In this Row and column are shuffle random and generate a private key. Same key was used for image decryption at the time of image extraction. Image encryption is done for security. Encrypted image is sent to data hider but Data hider does not know the original content of the image. Fig.5. Show the flow chart of proposed work.

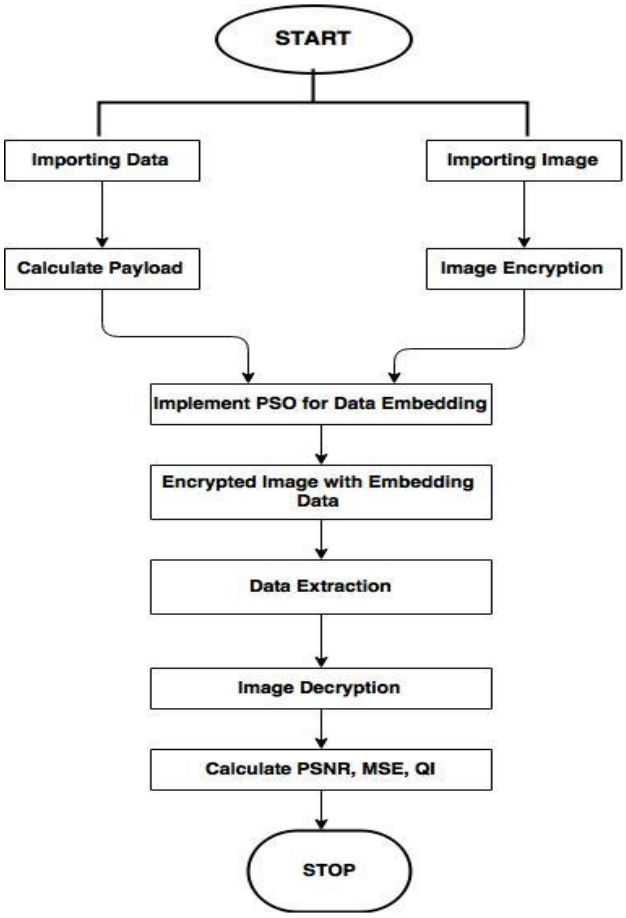

Figure 5: Flow chart of proposed work

3.2 Data Hiding

In this phase data hider hide secret information into it. In our work large amount of payload is hiding into image. In this we apply a PSO (Particle swarm optimization) for finding out the best positions in an image for hiding information. For finding the global best position following algorithms are considered:

ALGORITHM
Input: In this we consider Encrypted Image as an Input
Output: Give a global best position
Procedure
01. For P= 1 to P
02. P P_p = Rand [SS_s]
03. End For
04. For P= 1 to P
05. P F_p = FF [PP_P]
06. End For
07. $pbest$ = [PF_P]Max
08. For j=1 to j
09. For P=1 TO P
10. C P_p = (Rand [SS])v+ PP_P
11. End For
12. For P =1 TO P
13. CF_P = FF[CP_P]
14. End For
15. For p=1 to P
16. If C F_p>[PF_P]
17. PP_P = C P_p
18. End If

19. End For
20. $pbest > [PP_P]max$
21. If $pbest > gbest$
22. $gbest = pbest$
23. End If
24. End For

Whereas: P= Particle
PP_P = pth Particle
Rand [SS_s] = Random Function with search limit SS
J= iteration
FF= fitness function for pth Particle
C P_p = Shifted pth Particle
C F_p & PF_P = Fitness value for pth Particle
$gbest$ = Global best for gth iteration
v= velocity
Fitness value is given by

$$E = \sum_{i=1}^{p} |I_i - D_i| \quad (1)$$

$$\text{Fitness value} = [1 - (E/255 \times L))] \quad (2)$$

Where E is the summarization error for hiding
D_ith data into host I_{ia} Pixel
L is the no. of byte to be hide

After finding the gbest position in encrypted image generate a data hiding key and then at that particular positions we hide a data. After hiding data into an encrypted image that encrypted image with embedded data is send to the receiver side.
Embedded rate can be calculated as*:*

$$Embedded\ Rate = {}^{Payload}/_{Total\ no.\ of\ Host\ image\ Pixal} \quad (3)$$

Embedded rate is defined as the ratio of payload and Total number of host image pixel.

3.3 Data and Image Recovery

In both above steps we generate a two keys first one is an encryption key and the second one is data hiding key. At receiver side there are three cases i.e. receiver has only data hiding key, only decryption key and receiver have both keys (data hiding key and decryption key)
Case1: Receiver has the only data hiding key. Then the receiver extracts data from LSB of encrypted image. Extract two groups of LSB each having four bits to make a one byte and then convert it into ASCII value after that convert a value into a text. We can extract a data as same as original one.
Case2: Receiver has the only decryption key. With the help of a decryption key receiver get an image as same as the original one, but does not extract the secret data. As we know the data embedding method does not change the most significant bits. So decrypted most significant bits are same as original one.

The mean square error can be calculated as

$$MSE = \frac{1}{m*n} \sum_{i=1}^{n} \left((I_i - K_i)\right)^2 \quad (4)$$

Where I is a original cover image and K is the Decrypted image. PSNR is calculated after computing a MSE.

PSNR is computed by given formula

$$PSNR = 10 \cdot \log_{10}(MAX_1^2/MSE) \quad (5)$$

Case 3: if the receiver has both key, i.e. data hiding key and decryption key, then receiver get both secret data as well as image same as original one.

4. Result and Discussion

Evaluation parameters: Performance of Particle swarm optimization in Reversible data hiding is evaluated. By following method

1) Decrypted image Quality: - It describes the image quality.
2) Payload or data capacity limit: - it describes the how much data are implanted. [7]

So those above terms are calculated by peak-to-signal noise, quality index and large amount of data is implanted in the image

In this work, we are embedding a large amount of data into an encrypted image and Extract data and check the PSNR of decrypted image. Table 1 shows that the value of PSNR for huge data. The main interest of this work is that PSNR of encrypted image is high, so that very negligible change in decrypted image. In Fig. 6 we see that value of PSNR according to embedded rate is high. In Fig 7 we see that range of quality index is in between 0.99 and 1. The experimental result is compared with [5]. Fig.6. shows embedded rate Versus PSNR of the proposed method and [5] Fig. 6 reveals that the proposed method offers Higher PSNR than that of [5].

Table 1: Payload capacity in cover image and related PSNR

Sr. No	Payload (In Number of words)	Approximate Text size (In KB)	PSNR of image recovered after Decryption (Agham et. al. Method) (in dB)	PSNR of image recovered after Decryption (Proposed Method) (in dB)
1	500	3.20	45.8573	65.3313
2	1000	6.41	42.9012	58.2412
3	1500	9.61	41.1306	54.0031
4	2000	13.3	39.946	51.2237

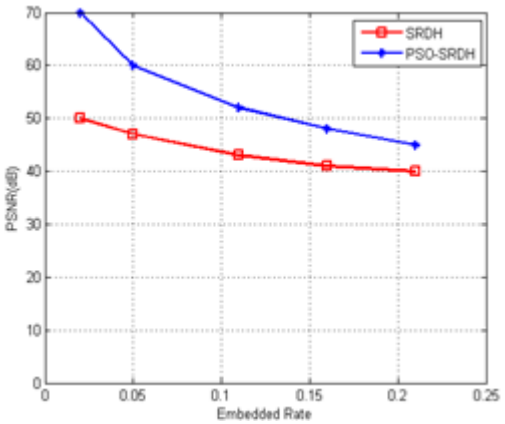

Figure 6: Value of PSNR according to embedded rate

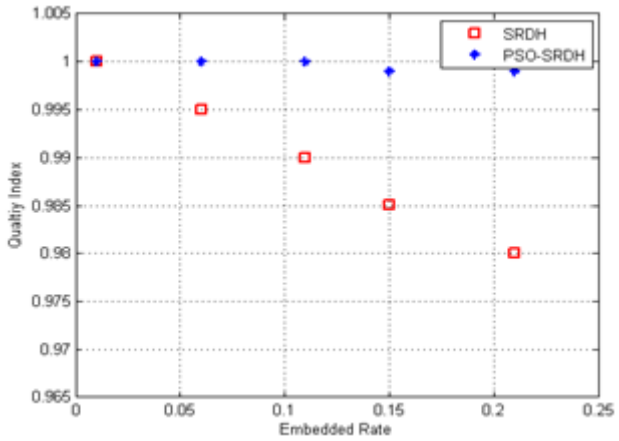

Figure 7: Value of Quality index according to embedded rate

5. Conclusion

In Proposed scheme we have used the particle swarm optimization which is a very successful approach to increasing the hiding capacity. The goal of proposed work is to increase the embedding rate and related PSNR value and improve the quality index. In order to achieve good payload distortion performance of RDH, in this work firstly encrypt the image with the help of encryption key and the encrypted image is send to data hider to hide a secret data in to the encrypted image with the help of data hiding key and at receiving end get a data as well as cover image as per terms. The experimental result present that our proposed work significantly improves the PSNR and quality index over [5]. The implemented RDH method can be enhanced in the future by using an image as a secret data in place of text data. In that case we are hiding image in to the cover image.

References

[1] Z Ni, Y. -Q Shi, N. Ansari and W. Sue "Reversible data hiding," IEEE Trans. Circits Syst. Video Technol, vol. 13, no. 3, pp. 354-362, Mar. 2006)
[2] Xiaolong Li, Weiming Zhang , Bo Ou and Bin Yang" A brief review on reversible data hiding-current technique and future prospect," IEEE, pp. 426-430, July 2014.
[3] Patil K.U.&Nandwalkar B.R., "GA Based Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption, " IOSR Journal of Electronics and Communication Engineering (IOSR-JECE.), p-ISSN: 2278-8735, pp.37-44.
[4] X. zhang, "Reversible data hiding With Optimal Value Transfer," IEEE Trans. On Multimedia, vol. 15, no. 2, pp. 316-325, Feb. 2013.
[5] Vinit Agham and Tareek Pattewar, "A Novel Approach Towards Separable Reversible Data Hiding Technique," IEEE International Conference on Issues and Challenges in Intelligent Computing Technique (ICICT), pp. 771-775, 2014
[6] J. Kennedy, and R. Eberhart, "Particle swarm optimization," in Proc. IEEE Int. Conf. Neural Networks,Perth, WA, pp. 1942-1948, 1995.
[7] Cheeny Bansal and Preeti Gupta "A survey on Histogram Shifting techniques in Reversible data hiding ," IEEE International Advance computing conference(IACC), pp. 1008-1012,Feb. 2014
[8] USC SIPI ---- The USC-SIPI Image Database.[online], http://sipi.usc.edu/database/Database.html