# Increase of Capacity and Quality of Frequency Based Image Steganography Using Particle Swarm Optimization

Samadrita Guha
Symbiosis Institute of Technology
Symbiosis Knowledge Village,
Gram:Lavale,Tal:Mulshi,Pune412115
(91)9830916912
samadrita.guha@sitpune.edu.in

Dipti Kapoor Sarmah
Symbiosis Institute of Technology
Symbiosis Knowledge Village,
Gram:Lavale,Tal:Mulshi,Pune412115
(91)9552527637
dipti.sarmah@sitpune.edu.in

## ABSTRACT

This paper proposes a steganography technique to enhance the capacity and quality of the stego object. The method is proposed for frequency domain grayscale images. It is assumed that hiding varied number of secret bits in the original image blocks depending upon the DCT coefficients remaining after quantizing the blocks might increase the capacity of the stego image. To enhance the quality PSO can be used to find the appropriate DCT coefficients to conceal the secret data. The secret message is to be encrypted using AES before embedding in the original image blocks to ensure security.

## Specifications of the Proposed System

The proposed method works on frequency domain based image steganography. DCT is used to transform the cover image from spatial domain to frequency domain. Grayscale image is used as the cover file and the secret message to be hidden is a text file. The system will be implemented using MATLAB. Peak signal to noise ratio (PSNR) will be the measure to evaluate the system.

## Keywords

AES, DCT, frequency domain, PSNR, PSO, stego object

## 1. INTRODUCTION

The extreme usage of digital technology and ever increasing communication over internet has led to the increase of fraudulent activities in cyberspace. Under this scenario the invention of techniques to secure data transmission is demanded. The technique of transmitting a file over the internet by hiding it in another file so that the existence of the hidden file remains undetectable is the main idea of steganography [13] [15] [16]. During transmission a stego object is likely to undergo attacks or encounter compression techniques resulting in transformation of secret message or loss of information at receiver's side. To secure the system further cryptography [14] [15] [18] is combined with steganography. Steganography can be of different types depending upon the kind of cover file used. Image steganography is to two types viz. spatial domain image steganography and frequency domain image steganography [6] [17]. In spatial domain image steganography least significant bit of pixel values of the cover image is replaced by bits of secret data in order to conceal the secret message in the cover file. In frequency domain image steganography all the pixel values are first transformed into frequency coefficients using any of the transforms like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). The secret bits are concealed in LSBs of the frequency coefficients of the cover file. In this proposed method frequency domain image steganography will be used where DCT [5] is used for the transformation. The main priority in a steganography technique is that the deformity caused to the cover file due to addition of secret bits should be undetectable. The stego file should have enough potential to withstand attacks so that there is no loss of data during transmission and the intact message can be obtained at the receiver's side. Least Significant Bit (LSB) substitution [9] [12] [15] method is used to embed the secret message. In LSB substitution method the secret message bits are hidden in the least significant bits of the pixels. In this proposal the secret message bits will be hidden in the LSB positions of the optimal coefficients selected by PSO [4].

## 2. RELATED WORK

Many researchers have used PSO to encrypt the secret message but PSO has not yet been applied to find the optimal coefficients for embedding purpose in frequency domain. Jpeg Quantization Table Modification (JQTM) [1] has also been used previously to increase the hiding capacity of the cover file but this increases the stego file size which may attract the attention of the intruders. So the standard Joint Photographer's Expert Group (JPEG) quantization table is used for quantizing the cover image in the proposed method.

Xiaoxia Li et al. in 2007 [20] proposed the use of Particle Swarm Optimization algorithm to find an optimal substitution matrix which would encrypt the entire secret message. The method also used modified quantization table to increase the capacity of the stego object. Saeid Fazli et al. in 2008 [7] improved Li, Wang's method and used Particle Swarm Optimization to find unique optimal substitution matrices to encrypt each block of the cover image. Debnath Bhattacharyya et al. in 2009 [3] proposed a novel method DCTIASMTT for DCT based Image authentication and secret message transmission scheme. In 2011 Feno Heriniaina et al. [11] proposed three distinct schemes to improve DCTIASMTT using PSO. The three schemes had three distinct objective functions. First scheme used only one matrix to transform the entire block of secret data and measured the cost between transformation of cover image to frequency domain and cost to transform the secret data.

Second scheme used unique transformation matrices to transform each block and stored all tables. It measured the distortion between cover image and stego image produced. Third scheme measured

*ICTCS '16*, March 04-05, 2016, Udaipur, India
© 2016 ACM. ISBN 978-1-4503-3962-9/16/03…$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905059

distortion between original secret data and recovered secret data. In 2013 Punam Bedi et al. [2] used PSO to select the best pixel positions in a spatial domain cover image in order to obtain high quality stego object after embedding secret message bits in it. P.Aswini et al. in 2015 [10] introduced a technique where the cover image was preprocessed before hiding the secret message. The secret message was encrypted using PSO. After embedding, optimal pixel adjustment process (OPAP) is used to enhance the quality.

**Table 1. PSNR values obtained by different researchers using PSO in steganography techniques**

| Methods | Cover image | Secret Image | PSNR |
|---|---|---|---|
| Xiaoxia Li et al 2007 [20] | LENA | TEXT | 37.06 |
| Saeid Fazli et al. 2008 [7] | LENA | TEXT | 37.57(3. A.2 - 3LSBs) |
| Debnath Bhattacharyya et al. 2009 [3] | LENA | PLANE | 46.51 |
| Feno Heriniaina et al. 2011 [11] | LENA | PLANE | 46.54 (PSO1) |
| Punam Bedi et al. 2013[3] | LENA | BOAT | 47.13 (spatial domain-1LSB) |
| P.Aswini et al. 2015 [10] | LENA | KEY | 59.21 |

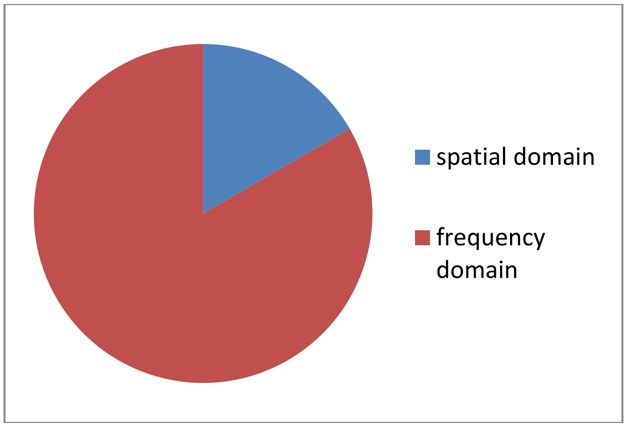


Fig.1 Pie chart showing the use of PSO in spatial and frequency domain **in image steganography** between 2007 and 2015

## 3. Particle Swarm Optimization

James Kennedy and Russel C. Eberhart in 1995 first explained PSO [4] technique inspired by two concepts. The concepts are flocking and schooling patterns of birds and fish and the concept of evolutionary computation. Each solution in the search space of a given problem is considered as a particle. The solutions or particles are evaluated based on local and global information. The local and global variables associated with the particles are adjusted based on the values of those members that are closest to the target solution at any given moment. The particles flow in the search space to satisfy the objective function and get the optimal solution.

The following equations are used to calculate and update the positions and velocities of the particles:

$$Vi=w * Vi + c_1 * rand_1 * (pbest_i - Xi) +c_2 * rand_2 * (gbest - Xi) \quad (1)$$

$$Xi = Xi + Vi \quad (2)$$

$$w = w_{max} - n. \frac{w_{max} - w_{min}}{\max\_iter} \quad (3)$$

Fig. 2 Particle Swarm Optimization (fish schooling) [21]

Where, Xi denotes the positions of the particles and is represented as Xi = ($x_{i1}$, $x_{i2...}$ $x_{iD-1}$). As the PSO algorithm works through the iterations, the position of the particles is updated using equation 2. Velocity Vi is represented as Vi = ($v_{i1}$, $v_{i2...}$ $v_{iD-1}$). $c_1$ , $c_2$ and $rand_1$ , $rand_2$ are acceleration constants and random real numbers in the range [0, 1] respectively. pbest is the personal best position reached by an individual particle. gbest is the global best position obtained by the particle that is closest to the target solution. w is the inertia weight. Its value decreases linearly from a large value denoted as $w_{max}$ to a small value denoted as $w_{min}$ until the PSO algorithm reaches max_iter. max_iter is the maximum number of iteration the algorithm will work. n specifies the current iteration.

## 4. Advanced Encryption Standard (AES)

Three block ciphers namely, AES-128 [8] [20], AES-192, AES-256 are combined to form AES. Encryption and decryption of data are done in blocks of 128 bits by each block cipher using keys of 128 bits, 192 bits and 256 bits respectively. Symmetric and secret-key ciphers share the same key for encryption and decryption. Each cipher consists of a specific number of rounds (10 for 128 bit cipher, 12 for 192 bit cipher and 14 for 256 bit cipher). These rounds transform the plaintext into ciphertext through a number of processing steps that include substitution, transposition and mixing the input of the plaintext.

## 5. Discrete Cosine Transformation (DCT)

Discrete Cosine transformation [5] [12] is used to convert an image from spatial domain to frequency domain.

Let I be an image with M columns and N rows represented by a 2D signal P(x,y) ,where, x=0,1,2, ... , M-1 and y=0,1,2, ... , N-1. The DCT of P(x,y) is given by the following equation,

$$F_{u,v=}\alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} P_{x,y} \cos\left(\frac{(2x+1)\pi u}{2M}\right) \cos\left(\frac{(2y+1)\pi v}{2N}\right) \text{....(4)}$$

where, $\alpha_u = \begin{cases} \sqrt{\frac{1}{M}}\ for\ u = 0 \\ \sqrt{\frac{2}{M}}\ for\ \neq 0 \end{cases}$ and $\alpha_v = \begin{cases} \sqrt{\frac{1}{N}}\ for\ v = 0 \\ \sqrt{\frac{2}{N}} for\ \ v \neq 0 \end{cases}$

u=0,1,2,.., M-1 and v=0,1,2,...,N-1. $P_{x,y}$ is the (x,y)th position in the original spatial domain image. $F_{u,v}$ is the (u,v)th frequency component.

The first frequency domain component is found to be the average of al the image pixels and is called the DC Coefficient. All the other coefficients of the image are called the AC coefficients.

The inverse DCT converts the frequency domain signal $F_{u,v}$ back into the spatial domain form f(x,y) and the equation is given as,

$$P_{x,y} = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} \alpha_u\, \alpha_v F_{u,v} \cos\left(\frac{(2x+1)\pi u}{2M}\right) \cos\left(\frac{(2y+1)\pi v}{2N}\right) \quad (5)$$

Where, $\alpha_u = \begin{cases} \sqrt{\frac{1}{M}}\ for\ u = 0 \\ \sqrt{\frac{2}{M}}\ for\ u \neq 0 \end{cases}$ and $\alpha_v = \begin{cases} \sqrt{\frac{1}{N}}\ for\ v = 0 \\ \sqrt{\frac{2}{N}}\ for\ v \neq 0 \end{cases}$

# 6. PROPOSED METHOD

## 6.1 Description of Proposed Method

The number of bits in the secret message is calculated. Let the number be **m.** The grayscale cover image is decomposed into blocks each having 8X8 dimension. Let the number of blocks obtained be **n**. Minimum number of secret bits that can be embedded in each block is calculated as **m/n**. DCT is applied on each block. The transformed blocks with DCT coefficients are quantized. Zig-zag scanning is done on each block to convert 2D matrices to 1D vector. Let the coefficients remaining after discarding the higher frequency values in the quantization step be **r**. This value of **r** varies from block to block. If **r is** zero in a block then no secret bits will be embedded in that block. If **r** is found to be less than **m/n** then **r/2** number of positions will hide **r** number of secret data in that block. If **r** is equal to **m/n** then **r** number of positions will hide **r** number of secret data. If**s** is greater than m/n then is found to be more than half of min value of r then number of bits to be hidden is increased by 2 with every increase of r by 2. PSO is used to find the [(m/n)/2] coefficients in the vectors. As variable number of bits are embedded in each vector there will coefficients left that can hide more secret bits after the secret message we started with is entirely embedded. Let this number be p. Thus another secret message with bit size p can be embedded in the stego image.

## 6.2 Finding the optimal coefficients

PSO is to be applied to find all min, a, b, max number of coefficients. For each (min, a, b, max) a huge number of particles are to be created by selecting DCT coefficients randomly. PSNR values for each of such particles will be calculated using the following equations

$$\text{PSNR}=10\text{x}\log_{10} (255^2/\text{MSE}) \quad (6)$$

$$\text{MSE}=\frac{1}{MN}\sum_{I=1}^{M}\sum_{J=1}^{N}\big(S(i,j) - C(i,j)\big)^2 \quad (7)$$

Where M, N represents the columns and rows of pixels in the cover image and S(i, j) and C(i, j) represent the pixel values of stego image and cover image. The best PSNR value will give the gBest. Based on the obtained gBest the velocity and position of each particle will be updated up to a certain maximum time mentioned. In each iteration pBest of each particle will be adjusted based on how close the particles fitness value has moved closer to the target. The final gBest obtained at the end of the maximum iteration gives the final optimal solution. The proposed method can be further enhanced by considering the hiding capacity of white and black pixels. Based on the consideration 3 or 4 LSB substitution method can be used. This will increase the capacity of the stego image to hide more information without hampering the quality. Again to reduce the computation time the cover image can be decomposed into 16X16 blocks and experimented with the same method.

## 6.3 Block Diagram

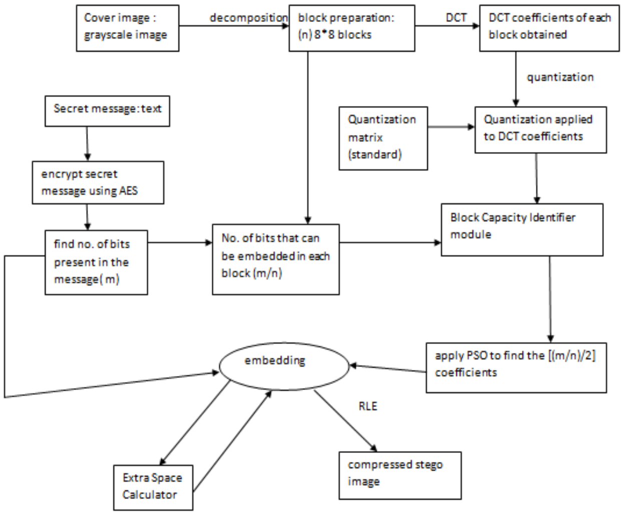


Fig. 3 Block diagram of the proposed method

### 6.3.1 Steps in Block Diagram

The block diagram in fig. 2 depicts the method proposed in this paper.

**Cover image:** A grayscale image is chosen as the cover image. **Decomposition:** The grayscale cover image is first divided into blocks of size 8X8. Each block therefore consists of 64 pixel values.

**DCT:** Discrete cosine transformation is applied on each block to transform the cover image from spatial domain to frequency domain.

**Quantization:** Standard JPEG quantization table is used to apply quantization technique on the DCT coefficients to determine the high frequency coefficients that are imperceptible to the human eye. These high frequency coefficients are dropped.

**Optimization:** Particle Swarm Optimization technique is applied on the quantized cover image to select Frequency coefficients that will be best suited for concealing the secret message.

**Secret message:** Plain text is chosen as the secret message.

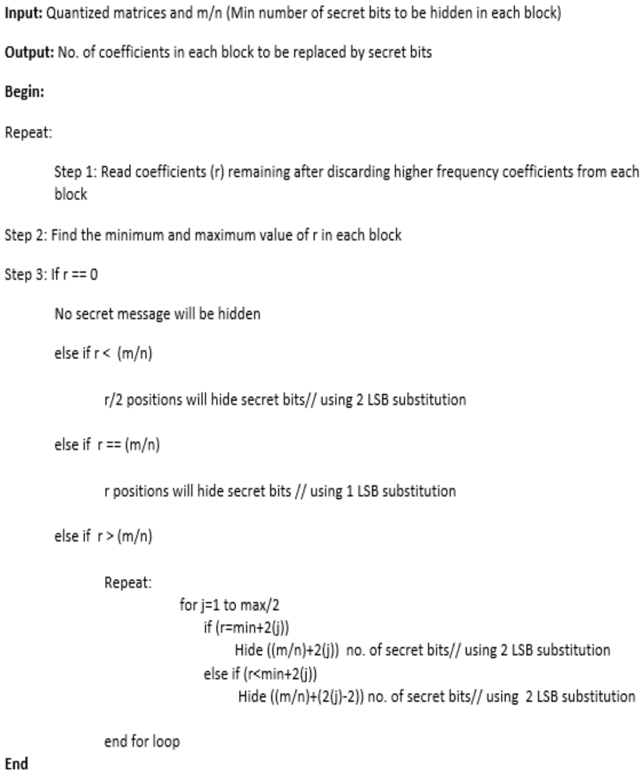
**Encrypted message:** The plaintext will be encrypted to cipher text using AES.

**Embedding:** Least significant bit substitution method is used to hide the transformed secret message into the optimal frequency coefficients of the cover image.

**RLE:** The stego image obtained is further compressed using run length encoding and the final compressed stego image is obtained.

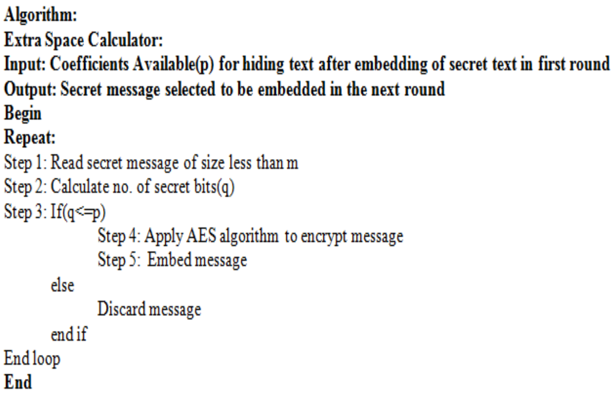
**Block Capacity Identifier** module and the **Extra Space Calculator** are explained in the following pseudo codes given in sections 3.3.2 and 3.3.3 respectively.

### 6.3.2 Block Capacity Identifier



```
Input: Quantized matrices and m/n (Min number of secret bits to be hidden in each block)

Output: No. of coefficients in each block to be replaced by secret bits

Begin:

Repeat:

        Step 1: Read coefficients (r) remaining after discarding higher frequency coefficients from each
        block

Step 2: Find the minimum and maximum value of r in each block

Step 3: If r == 0

        No secret message will be hidden

        else if r <  (m/n)

                r/2 positions will hide secret bits// using 2 LSB substitution

        else if  r == (m/n)

                r positions will hide secret bits // using 1 LSB substitution

        else if  r > (m/n)

                Repeat:
                            for j=1 to max/2
                                if (r=min+2(j))
                                     Hide ((m/n)+2(j))  no. of secret bits// using 2 LSB substitution
                                else if (r<min+2(j))
                                     Hide ((m/n)+(2(j)-2)) no. of secret bits// using  2 LSB substitution

                end for loop
End
```

### 6.3.3 Extra Space Calculator



```
Algorithm:
Extra Space Calculator:
Input: Coefficients Available(p) for hiding text after embedding of secret text in first round
Output: Secret message selected to be embedded in the next round
Begin
Repeat:
Step 1: Read secret message of size less than m
Step 2: Calculate no. of secret bits(q)
Step 3: If(q<=p)
                Step 4: Apply AES algorithm  to encrypt message
                Step 5:  Embed message
        else
                Discard message
        end if
End loop
End
```

## 7. LIMITATION

It is estimated from the Extra Space Calculator module that it is not always possible to find secret messages of the same size as p. In such a case some of the coefficients with data hiding potential may be wasted. Also the constant check for a secret message of size less than m and less than or equal to p will increase time complexity.

## 8. CONCLUSION

An efficient technique of frequency domain image steganography with application of particle swarm optimization is presented in this paper. The technique proposed in this paper encrypts a plaintext using AES and hides it in a gray scale cover image. The grayscale cover image is converted from spatial domain to frequency domain using DCT. PSO selects the frequency coefficients that are to be replaced by the secret bits. This proposed technique will result in better quality stego image with greater capability to noise tolerance. Depending on the hiding capacity of each block varied number of secret bits is embedded in each block therefore enhancing the capacity of the stego image. The performance measure to evaluate the entire proposed technique is MSE and PSNR. It is expected that the PSNR values obtained from the proposed method will be better than other methods as optimization technique is used to select the best positions in the cover image to hide the secret message.

## 9. ACKNOWLEDGEMENT

We thank our Director and HOD to allow us to work in this field.

## 10. REFERENCES

[1] Almohamad, A., Ghinea, G. and Hierons, R. M. 2009. JPEG steganography: a performance evaluation of quantization tables. IEEE. 1550-445X/09. DOI=10.1109/AINA.2009.67

[2] Bedi, P., Bansal, R. and Sehgal, P. 2013. Using PSO in a spatial domain based image hiding scheme with distortion tolerance. Elsevier Ltd. 24 Jan. 2013. DOI= http://dx.doi.org/10.1016/j.compeleceng.2012.12.021

[3] Bhattacharya, D., Dutta, J., Das, P., Bandyopadhyay, S. K. and Kim, Tai-hoon. 2009. Discrete Cosine Transformation based Image Authentication and Secret Message Transmission scheme. IEEE. 978-0-7695-3743-6/09. DOI= 10.1109/CICSYN.2009.11

[4] Blondin, J. 2009. Particle Swarm Optimization: A Tutorial. www.dmi.unict.it/mpavone/nc-cs/materiale/**pso_tutorial**.pdf

[5] Cabeen, K. and Gent, P. Image Compression and the Discrete Cosine Transform. Math 45, College of the Redwoods

[6] Chanu, Y.J., Tuithung, T. and Singh, K. M. 2012. A Short Survey on Image Steganography and Steganalysis Techniques. IEEE. 978-1-4577-0748-3/12

[7] Fazli, S. and Kiamini, M. 2008. A High_Performance Steganographic Method using JPEG and PSO Algorithm. IEEE. 978-1-4244-2824-3/08

[8] Kadam, P., Nawale, M., Kandhare, A. and Patil, M. 2013. Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique. IEEE. 978-1-467-5848-3/13

[9] Kaur, N. 2013. Steganography Using Particle Swarm Optimization- A Review. IJESRT. ISSN: 2277-9655. 3345-3347.

[10] Prabhu, S. M., P. A., B. B., P. V. and P. S. 2015. Highly Secured Image Steganography Using Particle Swarm Optimization. IJETS. ISSN (P): 2349-3968, ISSN (O): 2349-3976, Vol. 2, Issue 3.

[11] Rabevohitra, F.H. and Sang, J. 2011. Using PSO Algorithm for Simple LSB Substitution Based Steganography Scheme in DCT Transformation Domain. Springer. ICSI 2011, Part I, LNCS 6728, pp. 212-220.

[12] Raja, K.B., Chowdary, C.R., Venugopal, K.R. and Patnaik, L.M. 2005. A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images. IEEE. 0-7803-9588-3/05.

[13] Saha, B. and Sharma, S. 2012. Steganographic Techniques of Data Hiding using Digital Images. DEF. SCI. J. Vol. 62, No. 1, pp. 11-18, DOI=10.14429/dsj.62.1436

[14] Song, S., Zhang, J., Liao, X., Du, J. and Wen, Q. 2011. A Novel Secure Communication protocol Combining Steganography and Cryptography. Elsevier. pp. 2767-2772. DOI=10.1016/j.proeng.2011.08.521.

[15] Thangadurai, K. and Sudha, G. 2014. An analysis of LSB Based Image Steganography Techniques. IEEE. 978-1-4799-2352-6/14.

[16] Vanmathi, C., and Prabu, S. 2013. A Survey of State of the Art technique of Steganography. IJET. ISSN: 0975-4024. Vol 5, No 1.

[17] Parekh, R. 2013. Principles of Multimedia, 2e. McGraw-Hill. ISBN (13): 978-1-25-900650-0.

[18] Forouzan, B. A. 2013. Data Communications and Networking, Fourth Edition. McGraw-Hill. ISBN-13: 978-0-07-063414-5

[19] Kachitvichyanukul, V. 2012. Comparison of Three Evolutionary Algorithms: GA, PSO and DE. KIIE. Vol II, No 3, September 2012, pp. 215-223. ISSN 1598-7248, EISSN 2234-6473. DOI= http://dx.doi.org/10.7232/iems.2012.11.3.215.

[20] Li, X. and Wang, J. 2007. A steganographic method based upon JPEG and particle swarm optimization algorithm. Elsevier. pp. 3099-3109, DOI=10.1016/j.ins.2007.02.008

[21] Varadi, D. 2013. Social Learning Algorithm: Particle Swarm Optimization (PSO). CSSA. https://cssanalytics.wordpress.com/2013/09/06/social-learning-algorithms-particle-swarm-optimization-pso/