Steganography using Social Impact Theory based Optimization (SITO)

Amanjot Kaur
M.E - CSE
CU, Gharuan
Mohali, Punjab, India

Shruti Mittal
Assistant Professor - CSE
CU, Gharuan
Mohali, Punjab, India

ABSTRACT
With a great advancement in science and technology, efficient techniques are needed for the purpose of security and copyright protection of the digital information being transmitted over the internet and for secret data communication. Thus, Steganography solves this purpose which has been used widely. Even though, a Stego-object may be exposed to noise or compression due to which the secret data cannot be extracted correctly at the receiver's end, when the transmission occours.

This paper presents an efficient image hiding scheme, Social Impact theory based Optimization (SITO). Here, a fitness function is computed based on certain texture properties and entropy of a host image. According to this, the block holding the most relevant fitness value is the place where embedding of the secret data (secret image) is done. Thus, a stego-image is retrieved at the other end, which is not only good in quality but is also able to sustain certain noise and compression attacks during the transmission. The objective function is defined in such a manner that both quality and robustness of the stego image are acceptable, for which the performance analysis parameter values of the stego-image are also determined.

The results, when compared with some other data hiding technique show better stego image quality along with distortion tolerance.

Keywords
SITO, Image Steganography, MSE, PSNR

1. INTRODUCTION
Steganography [10] is generally termed as the procedure that exhibits hiding the private information from the third person, in a manner that it cannot be known to anyone other than the sender and the recipient [14]. Thus, doing so, it cannot be revealed. This name has been derived from Greek word, meaning "covered-writing". Steganography and Cryptography are considered as the cousins in the spy craft family. In Cryptography, the message is usually scrambled in a manner that it becomes difficult to get the information. Steganography hides the existence of a message so that it cannot be recognized other than the intended recipient. The process that is incorporated in order to reveal the real message content is known as the Steganalysis. This process is opposite to Steganography. Moreover, the use of keys is usually done so as to provide authentication. If the sender has used any key, then if it is known by the recipient, then he would be able to find the information as exactly it was sent by the sender.

Various other techniques are applied for getting the work done related to the concept. These can be seen as:

1. LSB

Least Significant technique is one of the most common technique [4], in which a colored image is converted into the gray image and text image is converted into binary format.

2. PVD

In this scheme of Pixel Value Differencing [19] [20], a difference value is principally derived for two consecutive pixels, which is fundamentally relevent on the difference values.

3. Soft Computing (GA and PSO)

Soft Computing technique refers to the technique that has been widely used in the image processing. Various different methodologies have been used keeping in consideration about the quality of the images. Particle Swarm Optimization [1], Genetic Algorithm [17], Fuzzy Logic, Neural Networks, and Ant Colony Optimization, etc have been implemented for the processing.

2. PROPOSED METHODOLOGY

2.1 Social Impact Theory Based Optimization (SITO)
The Social Impact Theory Based Optimization Technique (SITO) is basically referred to as the soft computing technique which exhibits natural based phenomenon. It is laid on the basis of Psychology that exhibits social behavior [24]. This is concerned with the effect of surroundings on individuals that are taken as particles. Just like human beings are considered best in comparison with other individuals of the society i.e. animals. It has an impact related to the feelings of the living beings. It deals with the psychology related to the social behavior. It deals with the population where an output is foreseen, based on the attitude of the population. The Fitness function is introduced by which the strength of each individual is computed. It has been stated as a better soft computing technique because of the fact that the population gets distributed in a spatial manner. This incorporates main functions as one max, osito, gsito, etc.

2.2. Extraction of Secret Code
$$\text{SecretCode} = (\text{Stego Image} - (\beta * \text{Host Image})/\alpha$$
The proposed algorithm has been implemented on different host images and secret images.

2.3. Formation of the Stego-image
1) Conversion of RGB to Gray Image of Host Image and the Secret Image- The host and secret image have been converted into gray image which is an 8-bit image.
2) Sub plotting- The subplots has been made so that the host and secret images can be seen at individual levels of implementation.
3) Retrieval of the Stego-Image- Stego image is obtained in which the secret message has been embedded.

2.4. Fitness Function

In the applied technique, a Fitness Function is computed that basically means that the block is selected in a host image which seems to be the most relevant for embedding the secret data in it. This means it would be more secure area that is least prone to the attacks. Therefore, it provides better output for the stego-images.

Thus, a Fitness Function has been made by considering the values such as Entropy, and three texture properties i.e. Contrast, Energy, and Homogeneity. As seen by the execution, the Contrast and Entropy has been found to be the maximum whereas the Energy and Homogeneity possess the minimum value.

Thus based on these four values, a Fitness Function has been made which is taken as follows:

Ratio = Max (Entropy + Contrast / Energy + Homogeneity)

The Maximum Ratio is basically the Fitness Function. The block where the ratio is found maximum that is considered as the fitness function in which embedding is done.

2.5. Proposed Algorithm

Step-i: Read the Host and Secret Image

Step-ii: Convert both images into Gray Images using rgb2gray function

Step-iii: Scan the host image for minimum entropy block as that of the secret image.

Step-iv: Get the row and column of the identified block for secret image embedding

Step-v: Initialize α=0, and β=1- α as host and secret code insertion level.

Step-vi: Embed the secret image using the following formula:

Stego Image WMI = (α * Host Image + β * Secret Image)

Step-vii: Reconstruct the stego image from step-5.

Step-viii: Compute the entropy of Stego Image.

Step-ix: If entropy of Stego Image is less than the predefined entropy limit, increment the 'α' by a small fraction and go to step-6. Otherwise go to next step.

Step-x: Compute the MSE and PSNR value.

3. RESULTS

The performance of the proposed technique has been evaluated and compared with other data hiding techniques like the simple DWT technique, Particle Swarm Optimization (PSO) technique, and Matlab 2012 has been used for the implementation of the proposed technique. In the implementation, the host images have been used which are further converted as gray scale images to hide smaller standard secret images using the proposed and the above mentioned methods. The secret images have also been converted into gray scale images. The results have been tabulated for three standard images used as covers and the three standard images used as secret images as shown below as Figure1, Figure 2, and Figure 3. Figure 4 shows the flow chart of the proposed technique. The objective quantitative measures used for comparison between the original and the secret images of dimension m* n are as follows:

Peak Signal to Noise Ratio (PSNR): This is generally referred to as the measurement of the quality that exists between the cover image and final stego-image [1].

$$PSNR=10\log10^{*}(255^{*}255)/MSE$$

Mean Square Error (MSE): The term may be defined as the square of error that occurs between the original image (cover or host image) and the finally obtained steno image [19].

$$MSE = \frac{1}{(\text{row x col})}\sum_{r=1}^{row}\sum_{c=1}^{col}(x^{1}_{(r,c)} - x^{2}_{(r,c)})^{2}$$

Following table shows the results obtained:

Host Image Secret Image Stego Image

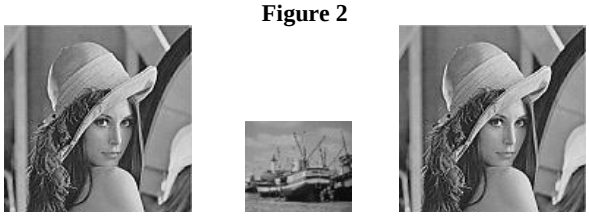
Figure 1

Table 1

S. No.	Host Image	Secret Image	DWT	PSO	Proposed method SITO
1.	Lenna	Text	19.647	45.21	66.244
2.	Baboon	Lenna	25.767	44.31	66.243
3.	Lenna	Ship	25.102	45.39	66.246

Host Image Secret Image Stego Image

Figure 2



Host Image Secret Image Stego Image

Figure 3

4. CONCLUSION

The proposed algorithm is based on Image Steganography using Social Impact Theory based Optimization (SITO) algorithm that finds an optimum image block in the host or cover image that may be the best location for embedding the secret image code. The optimum block search is based on the optimization of the fitness function value. The fitness function taken here is the maxima of ratio of sum of contrast and energy and entropy and homogeneity. The results so obtained are measured based on Performance analysis parameter values. Hence, results are fair enough and show superiority above the existing algorithm as Particle Swarm Optimization (PSO) based Image Steganography. Further, the speed of operation is good enough in order to embed the given secret image.

5. FUTURE SCOPE

The presented work has been tested and validated on different host images with same secret image and vice versa. The

algorithm efficiency is evaluated based on parameter values. The results show a fair performance over the existing methods like PSO, LSB, and DWT. The presented algorithm finds limitations in terms of speed of operation. And as the size of host and/or secret images increases, the speed of operation suffers. The work in enhancing the speed of operation irrespective of size of host/secret image may be exercised.

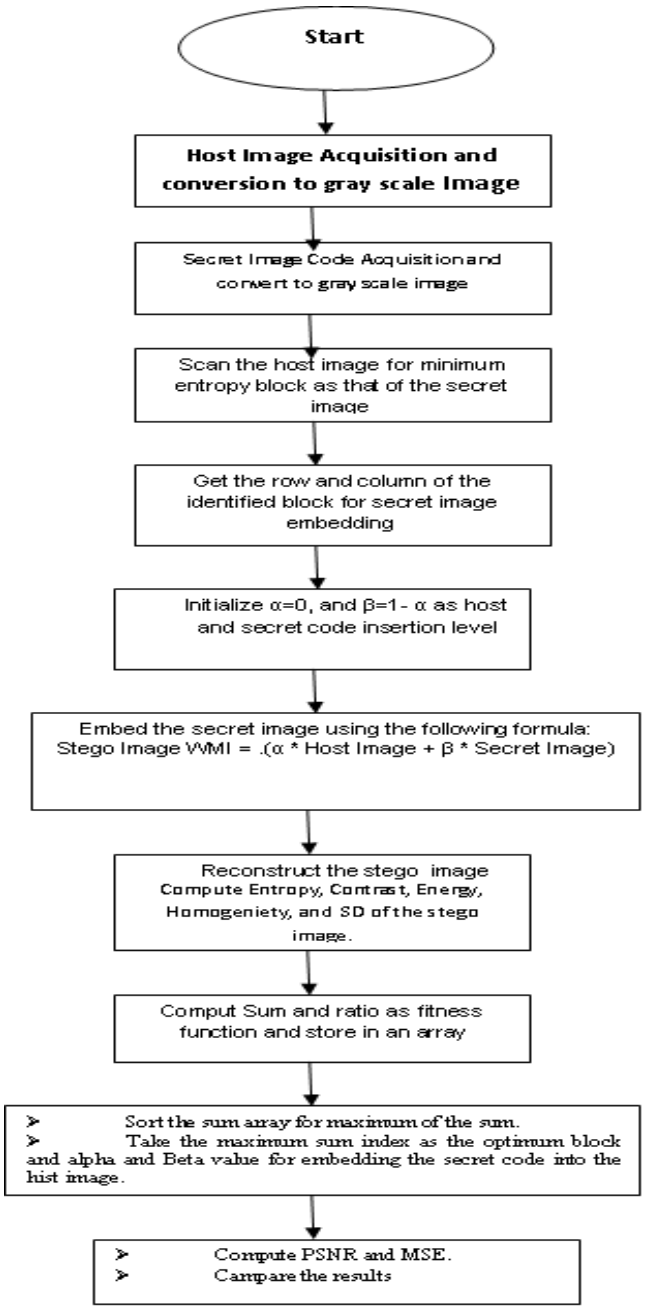


Figure 4

6. REFERENCES

[1] Punam Bedi, Roli Bansal, Priti Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance", Elsevier Springer, 2013

[2] Sunil. K. Moon 1, Rajeshree. D. Raut, "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security", IEEE, 2013.

[3] Ali K. Hmood1, Z. M. Kasirun1, Hamid A. Jalab1, Gazi Mahabubul Alam3, A. A. Zaidan2 and B. B. Zaidan2, "On the accuracy of hiding information metrics", International Journal of the Physical Sciences Vol. 5(7), pp. 1054-1062, August, 2010

[4] Cheng-Hsing Yang, Chi-Yao Weng,"Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems "IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, September 2008

[5] Neil Johnson, Eliminating Steganography in Internet Traffic with active wardens", Springer, 2003

[6] M.Al Htammami, "A proposed Modified Data Encryption Standard algorithm by using Fusing Data Technique", WCSIT, Vol.1.No. 3, 88-91-2011

[7] Adnan Abdul-Aziz Gutub, Wael Al-Alwani, and Abdulelah Bin Mahfoodh ,"Improved method of arabic text steganography using the extension "Kashida' character", BUJICT, vol3, Issue 1, Dec 2010

[8] Lei Zheng, Ingemar J Cox, "JPEG based conditional entropy coding for correlated steganography", IEEE, 2007

[9] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", International Arab Journal of Information Technology, Vol 7, No. 4, Oct 2010

[10] Rosziati Ibrahim, "Steganography Algorithm to hide Secret Message inside an image", Computer Technology and Application, Feb 2011

[11] Nelly Fazio, Antonio R. Nicolosi and Irippuge Milinda Perera "Broadcast Steganography", Springer, Vol 8366, 2014

[12] Biswapati Jana, Debasis Giri,Shymal Kumar Mondal, Pabitra Pal,"Image Steganography based on Cellular Automata", IJPAM, Vol 83, No.5, 2013

[13] Parisa Gerami, Subariah Ibrahim, Morteza Bashardoost, "Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment", IJCA, Volume 55– No.2, October 2012

[14] Xiaoxia Li, Jianjun Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm", Elsevier, Science Direct, Feb 2007

[15] Faramarz Sadeghi, Marjan Kuchaki Rafsanjani, Fatemeh Zarisfi Kermani, "Hiding Information in Image by Compound Meta-Heuristic Algorithm PSO-SA", IJCSAI, Vol. 3 Iss. 4 Dec. 2013

[16] Amrita Khamruia, J K Mandal, "A Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT)", Elsevier, ScienceDirect, 2013

[17] Parisa Gerami, Subariah Ibrahim, Morteza Bashardoost, "Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment, IJCA, Volume 55– No.2, October 2012

[18] Ko-Chin Changa, Chien-Ping Changa, Ping S. Huangb, and Te-Ming Tua "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia, Vol No.2, 2008

[19] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, " A high quality steganographic method with pixel-value differencing and modulus function", Elsevier, Science Direct, 2007

[20] V.Nagaraj, Dr. V. Vijayalakshmi and Dr. G. Zayaraz, "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function", Elsevier, Science Direct, 2013

[21] A OS.A.Z.Ansaef, "High Security Cover File of hidden data using statistical technique and AES encryption algorithm", Vol3, 2009

[22] Weiqi Luo and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE, Vol5, No. 2, June 2010

[23] Martin Maca's and Lenka Lhotsk'a, "Simplified Social Impact Theory Based Optimizer in Feature Subset Selection", Springer, 2011

[24] Macas, M., Lhotska, L. and Kremen, V, "Social Impact based Approach to Feature Subset Selection", International Workshop on Nature Inspired Cooperative Strategies for Optimization, Studies in Computational Intelligence, Springer, 2007

[25] Macas, M. and Lhotska, L., "Social Impact Theory based Optimizer", Advances in Artificial: 9th European Conference on Artificial Life, Heidelberg: Springer, pp. 635-644, 2007

[26] Macas, M. and Lhotska, L, "Social Impact and Optimization", 2nd European Symposium on Nature-inspired Smart Information Systems, 2006

7. AUTHOR'S PROFILE

The author1 is pursuing her M.E. (CSE) thesis work in Image Steganography from CU, Gharuan, and Mohali (Punjab) India. Her field of interest is in image processing based application development.