

# Enhanced Secure Data Hiding Technique In Digital Image Steganography Using Hybrid Optimized Algorithms

Deepika Sharma<sup>1</sup>, Jaskiran Kaur<sup>2</sup>

*M.Tech(Scholar), Assistant Professor*

*Department of Computer Science Engineering , CEC Landran, Punjab*

**Abstract**-Steganography differs from cryptography in their traits. Cryptography has the power of retaining a message secret, whereas steganography has the power of retaining the existence of a message secret. Steganography and cryptography are conjunctively used for guarding information from third parties, but neither technology alone is substantial and can be compromised. Once the revelation of hidden information is made or even doubtful, the purpose of steganography is partly subjugated. The strength of steganography can thus be boosted by uniting it with cryptography. In this approach steganography and cryptography is aggregated together. During the communication process typical LSB steganography is not a secure way for message transmission. So a first level secure DWT based steganography technique is proposed in integration with back propagation neural network, which is further optimized with ant colony optimization algorithm using a fitness function. In this research paper is to provide more security and better image quality. The effectiveness of the proposed method can be estimated by calculating the peak signal to noise ratio, mean square error and time consumption. The proposed work has been implemented using MATLAB and a Back Propagation Neural Network training function has been incorporated with it. The number of iterations of the Ant Colony algorithm evaluates fitness function. This will constitute to the enhancement of stego image quality.

**Keywords:** Steganography, methods of Steganography, Back Propagation Neural Network, ACO approach.

## I. INTRODUCTION

Steganography, the talent of transmission information just between you and me, is appreciated by embedding secret messages into innocent cover-objects such as digital images [1], audios and videos. The very presence of the communication itself is hidden since the stego-object looks the same as the cover. However, as the cover object is inescapably changed, the covert communication can still be perceived by some numerical resources.

Most steganography values hides information inside images, as it is comparatively easy to implement. People refer image steganography as the art and knowledge of invisible message, which is to secrete the very presence of hidden message in digital images. Some evidences have interested active investigators and plentiful journals in the field of image steganography. For instance, images can convey a large of

information, especially on the internet. Moreover, the non-stationary of images makes image steganography hard to break. Nowadays, ordinal image has become a significant channel to bear stego information [2].

Categories of Steganography:

- **Text Steganography:** In this approach the cover text is produced by generating random character sequences, changing words within a text, using context-free grammars or by changing the formatting of an existing text to conceal the communication [3]. The cover text produced by this approach can qualify for linguistic steganography if text is linguistically driven. Although this text-based methods has its own unique characteristics for cover text but suffers from various complications from both a linguistic and security stand point[4].
- **Image Steganography:** This Steganography method is additional general in recent year than other steganography possibly because of the flood of electronic image information available with the arrival of digital cameras and high-speed internet delivery[5]. It can involve hiding information in the obviously occurred noise within the image. Most kinds of information contain some kind of noise. Noise refers to the limitations inherent in the process of rendering an analogue picture as a digital image. In Image steganography we can hide message in pixels of an image. An image stenographic scheme is one caring of stenographic systems, where the underground message is hidden in a digital image with some hiding method. Someone can then use a proper decrypting technique to recover the concealed message from the image. The unique image is called a cover image in steganography, and the message inserted image is called a stego image [6,7].

Table 1. Methods of Image Seteganography

Methods Name	Advantages	Disadvantages
Data Hiding	Secure Info.	Connected with this type of coding [8].
Embedding	Recover info.	Solid regions and regions without projecting edges will not be marked
Extracting	Recover the original image [9]	-

## II. RELATED WORK

Bingwen Feng et.al,2014 [10] described as, a binary image steganography scheme that aims to minimize the embedding distortion in the texture is presented. They extracted the complement, rotation, and mirroring-invariant local texture patterns from the binary image first. The weighted sum of crmiLTP changes when flipping one pixel is then employed to measure the spinning alteration corresponding to that pixel. Vojtěch Holub et.al,2014 [11] proposed a worldwide distortion design called worldwide wavelet qualified distortion that can be applied for entrenching in an arbitrary domain. The embedding distortion was computed as a sum of comparative changes of coefficients in a directional filter bank decomposition of the cover image. The directionality forces the embedding changes to such parts of the cover object that are problematic to model in multiple directions, such as traces or noisy regions, while avoiding smooth districts or clean edges. Saiful Islam et.al,2014 [12] proposed a novel steganography method, where edges in the cover image have been used to surround messages. Amount of data to be embedded plays a significant role in the selection of edges, i.e., the more the quantity of data to be embedded, larger the use of weedier edges for embedding. Dr. Diwedi Samidha et.al,2013[13] in this purposed many steganography methods can be used like Least Significant Bit, layout,organization schemes, substituting only 1's or only zero's from lower nibble from the byte are measured for hiding a secret message in an image. Along with these systems, some more methods were proposed, grounded on the selection of random pixels from an image and again secret data is hidden in accidental bits of these randomly designated pixels. Ge Huayong et.al,2011[14] reviewed steganography and steg-analysis based on the digital image. Perception and principle of steganography and steganalysis were demonstrated. Spatial domain and transform domain inserting methods are generalized.

## III. RESEARCH TECHNIQUE USED

In this section, we discussed proposed techniques i.e, Discrete Wavelete Transformation, ACO and Neural Network.

- **Discrete Wavelet Transform:** It gives the best consequence of image transformation. It separations the signal into a set of basic functions. There are two types of wavelet transformation one is continuous and other is discrete. This is the new idea in the application of wavelets; in this the information is stored in the wavelet constants of an image [8,10] instead of changing bits of the actual pixels. It also performs local analysis and multi-resolution analysis. DWT transform the object in the wavelet domain and then processes the coefficients and performs inverse wavelet transform to show the innovative format of the stego object. It is very helpful for designing the way to manage the exploration of signal as well as picture, primarily helpful in the exploration of multi-resolution description. The signals are disintegrating into different way components in the frequency area. One-dimensional discrete wavelet transforms decays the input into two different averages and detailed components. The 2-D DWT distributes an input picture information into four

frequency sub-bands, one lower frequency (LL) and three higher frequency bands and components (LH, HL, HH) are shown in Figure below 1 (a) .

LL	HL
LH	HH

Fig. 1: (a) DWT components

Formula of Discrete Wavelet Transform:

$$y[n] = (x * g)[n] = \sum x[k]g[n - k]$$

- **Ant Colony Optimization:** Ant Colony Optimization (ACO) has a recently proposed met heuristic approach for solving hard combinatorial optimization problems. The inspiring source of ACO is the pheromone trail laying & following behavior of real ants, which use pheromones as a communiqué medium. In analogy to the biological sample, ACO is based on the indirect communication of a colony of simple agents, called (artificial) ants, mediated through (artificial) pheromone trails. The pheromone trails in ACO serve as distributed, numerical info which the ants use to probabilistically construct solutions to the problem being solved and which the ants adapt during the set of rules execution to reflect their search experience. (i) Swarm intelligence studies the co-operative performance of unsophisticated agents that interrelates locally through their situation [15]. (ii) It is motivated through social insects, such as ants and termites, or other animal societies, like as fish schools and bird flocks. (iii) Although each separate has only limited capabilities, the complete swarm exhibitions complex overall behavior. Therefore, the intelligent behavior can be seen as an emergent distinguishing of the swarm.

- **Back Propagation Neural Network :** This Back Propagation neural network is an artificial neural network based on the error back propagation set of rules. The Back Propagation Neural Network model consists of an input layer, some hidden layers and an output layer. Every connection, connecting neurons has a distinctive weighting value. In training the network, the nodes in the BP neural network obtain input information from exterior sources, and then go with two hidden layers which is an interior information processing layer and is answerable [16] for the information conversion, and then the nodes in the output layer supply the required output material. After that, the anti-propagation of error is transported by distinct the actual output with wanting output. Each weight is reviewed and back propagated layer through layer from the output layer to hidden layer and input layer. This process will be sustained until the output error of the net is reduced to an acceptable level or the predetermined time of learning is realized. The processing consequences of information are exported by output layers to the outside [17].

## IV. PROPOSED WORK

The proposed method embeds the message in Discrete Wavelet Transform coefficients based on back propagation neural network and then optimizing it with Ant colony

algorithm. This section describes this method, and embedding and extracting algorithms in detail.

**A. Cover image:**

It is the carrier image which is to be transmitted to the receiver side. It will carry the concealed data.

**B. Transformed image:**

It will denote the probable composition of the frequencies for the cover image. Thus the image will be composed of DWT coefficients.

**C. Optimized bound:**

The approach of neural network training plus ant colony algorithm will find the optimized empty bit coefficients from the actual part of DWT, which are responsible for concealing the data.

**D. Embedding process:**

It will embed the stego key, password, cipher text inside the trained bits unit using sum rule. Thus, our carrier image will be embedded with an encrypted secret message which is concealed within the image carrier.

**E. Stego image:**

The final processed image concealing secret data inside the cover image will be called as the stego image.

**Explanation of Methodology :**

The following steps present the different stages that need to be accomplished:

- Upload the cover image (original Image).
- Apply the Frequency domain technique to divide the image in Lower bound and upper bound.
- To add the text in image for hiding (Security), after hiding, we use the ant colony algorithm for reduction.
- Last one to classify the data into two sets like Training and Testing set.
- To evaluate the performance parameters like Peak signal to noise ratio and Mean square error.

## V. RESULT EXPLANATION

In this section, we implement the result and explanation of the Image Steganography. We design the Code using MATLAB 2013a language and tool used Graphical User Interface.

We described that the Proposed performance parameters and comparison defined with existing algorithm and performance parameters.

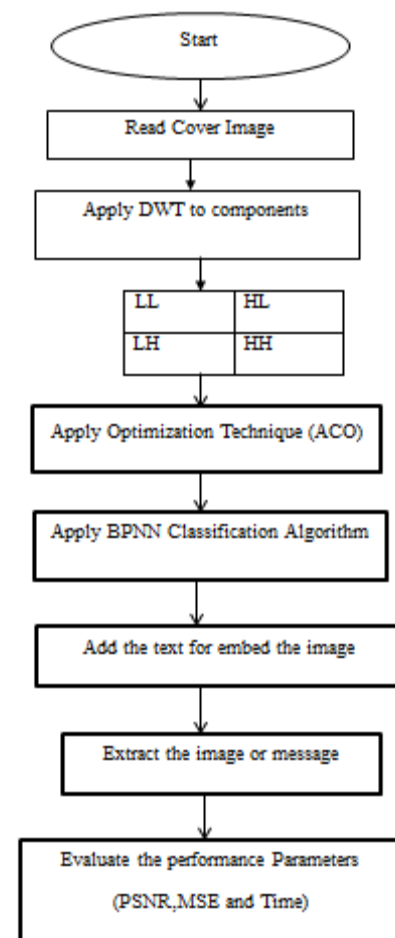







Fig. 2: Proposed Flow Chart

Table 2. Proposed Work

The Below table 2 described the Proposed Values.

Image s					
PSNR	56.28	56.89	57	57.8	60
MSE	0.15	0.12	0.1	0.013	0.01
TIME	0.4	0.3	0.2	0.1	0.06

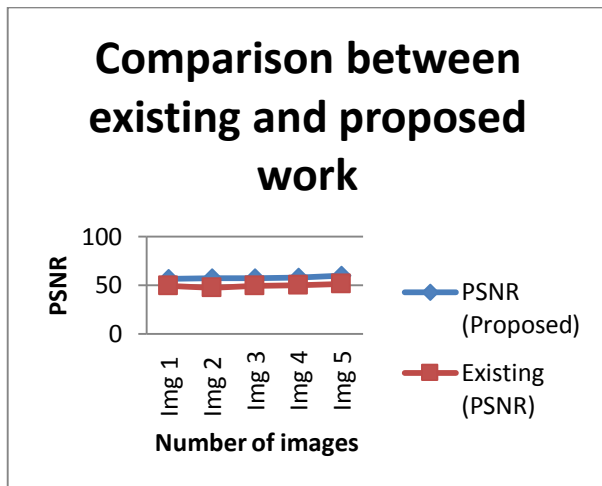


Fig. 3: Comparison between Existing and Proposed Work

Peak signal-to-noise ratio in decibels, returned as a scalar of type double, except if A and ref are of class single, in which case peaksnr is of class single.

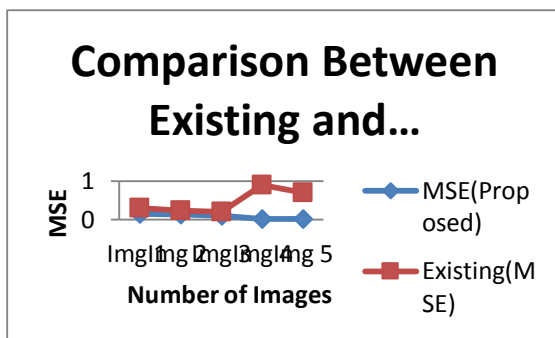


Fig. 4: Comparison between Existing and Proposed Work

The above figure shows that the mean square root increases in base paper. MSE is the computed average of percentage errors by which forecasts of a model differ from actual values of the quantity being forecast.

Table 3. Comparison Between Existing and Proposed Work








Img no.	PSNR	MSE	Existing (PSNR)	Existing(MSE)
	56.28	0.15	48.9	0.29
	56.87	0.12	47.5	0.23
	57	0.1	49	0.2
	57.8	0.013	50	0.9
	60	0.01	51	0.7

Table 4. Compariosn with previous and proposed parameters

Img no.	Techniques Defined (Existing)	PSNR (Existing)	Techniques Defined (Proposed)	Proposed (PSNR)
	dwt Split +	25.1	DWT +ACO	57.8
	dwt Split +	25.6	DWT+ACO	60
	DWT+Split	27	DWT+ACO	59

In table 3 define the previous and proposed performance parameters improve the image quality of the performance (PSNR).

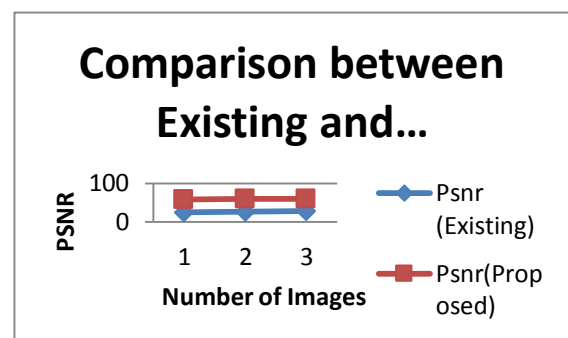


Fig. 5: Compariosn Existing and Proposed(Psnr) (DWT and Split, DWT and ACO approach)

In previous approach used DWT and Split Compression results value is 25.1,25.6 and DWT+ACO proposed approach value is 57.8 and 60.

## VI. CONCLUSION AND FUTURE SCOPE

The proposed system has discussed implementation of securely using steganography technique based on BPNN , ACO and DWT algorithm. It can be concluded that when normal image security using steganography technique is applied, it makes the task of the investigators unfeasible to decrypt the encoded secret message. The security features of the steganography are highly encrypted data using secret key . This research work has been implemented to enhance the image steganography technique so that the quality of the image remains the same. To implement our objective, we have used Back Propagation Neural Network, artificial bee colony and DWT. We overall concluded that managing the pixels to a deeper level increases the capacity of the image to hide certain messages. Back Propagation Neural Network has been found effective enough to find pixels to merge the data bits without much affecting the original pattern of the image. The whole

implementation is being taken place in MATLAB environment. From the results it has been concluded seed values algorithm achieves good results in data hiding in terms of PSNR, and Mean Square Error Rate values.

In future, this technique is applied to computer forensic images. So that the system can generate highly undetectable secret shares using encryption techniques certain set of training data which might be automatically generated and is disposed after the task has been performed.

## VII. REFERENCES

- [1]. Deeply(Nov 2012) "Steganography With Data Integrity", International Journal Of Computational Engineering Research (ijceronline.com), Vol.2, Issue 7.
- [2]. Attalla M. Al-Shatnawi(2012), "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, no. 79, 3907 – 3915.
- [3]. T. Morel, J.H.P. Elf, M.S. Olivier, "An Overview Of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science ,University of Pretoria, 0002, Pretoria, South Africa.
- [4]. Prof. Akhil Khare, Meenu Kumar, J Palla Vi Khare(Oct 2010), "Efficient Algorithm For Digital Image Steganography", Journal Of Information, Knowledge And Research In Computer Science and Applications, ISSN: 0975 – 67281, Nov 09 to Oct 10, vol.1, Issue 1.
- [5]. Sneak Aurora et al, Sanlam(Feb 2013), "A Proposed Method for Image Steganography Using Edge Detection", International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 2).
- [6]. Gabriel Hospodar, "Algorithms for Digital Image Steganography via Statistical Restoration"\_ ESAT/SCD-COSIC and IBBT, Katholieke Universiteit Leuven Kasteelpark Ehrenberg 10, bus 2446, 3001 Heerlen, Belgium.
- [7]. Shamim Ahmed Laskar and Kattamanchi Hemachandran(Dec 2012), "High Capacity Data Hiding using LSB Steganography and Encryption", International Journal of Database Management Systems ( IJDMS ) Vol.4, No.6.
- [8]. Adel Almohammad, Robert M. Hierons "High Capacity Steganography Method Based Upon JPEG", The Third International Conference on Availability, Reliability and Security The JPEG standard uses 8x8 quantization tables.
- [9]. Ross J. Anderson, Fabien A.P. Petitcolas(May 1998), "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481.
- [10].Feng, Bingwen, Wei Lu, and Wei Sun. "Secure binary image steganography based on minimizing the distortion on the texture." Information Forensics and Security, IEEE Transactions on 10.2 (2015): 243-255.
- [11].Holub, Vojtěch, Jessica Fridrich, and Tomáš Denemark. "Universal distortion function for steganography in an arbitrary domain." EURASIP Journal on Information Security 2014.1 (2014): 1-13.
- [12].Islam, Saiful, Mangat R. Modi, and Phalguni Gupta. "Edge-based image steganography." EURASIP Journal on Information Security 2014.1 (2014): 1-14.
- [13].Samidha, Diwedi, and Deepak Agrawal. "Random image steganography in spatial domain." Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013 International Conference on. IEEE, 2013.
- [14].Huayong, Ge, Huang Mingsheng, and Wang Qian. "Steganography and Steganalysis based on digital image." Image and Signal Processing (CISP), 2011 4th International Congress on. Vol. 1. IEEE, 2011.
- [15].M. Dorigo and G. Di Caro. The Ant Colony Optimization meta-heuristic. In D. Corne, M. Dorigo, and F. Glover, editors, New Ideas in Optimization, pages 11–32. McGraw Hill, London, UK, 1999.
- [16].M. Dorigo, G. Di Caro, and L. M. Gambardella. Ant algorithms for discrete optimization. Artificial Life, 5(2):137–172, 1999.
- [17].Channalli, Shashikala, and Ajay Jadhav. "Steganography an art of hiding data." arXiv preprint arXiv:0912.2319 (2009).