DOI: 10.13140/RG.2.2.18645.83687

A Survey for Maximizing the Steganalysis Embedding efficiency using Various Steganography Schemes.

Palak Sindhi[1], Er.Deepinder Kaur [2]

Student(m.tech),[1], Assistant Professor[2]

Shaheed Udham Singh College of Engineering & Technology Tangori (Mohali)

Abstract— The art of sending and displaying the hidden information particularly in public places has conventional more attention and confronted many challenges. Therefore, different methods have been suggested so far for hiding information in different cover media. In this paper a technique for hiding of information on the commercial display is presented. For good security and large payload in steganography, it is preferred to embed as many messages as possible per change of the cover object, i.e., to have high embedding efficiency. Many methods are used to hide data in numerous formats in steganography. The most generally used mechanism on account of its ease is the use of the Least Significant Bit. Least Significant Bit or its alternatives are normally used to hide data in a digital image. The other bits may be used but it is extremely likely that image would be distorted. This paper converses the art and science of Steganography in general and suggests a novel technique to hide data in a colourful image using least significant bit.

Keywords—*Steganography; Discrete Wavelet Transforation(DWT); Back Propagation Neural Network(BPNN); Artificial Bee Colony Optimization(ABC).*

I. INTRODUCTION

Steganography is a talent of hiding statement by embedding message into an innocuous observing cover media. Using steganography, an underground message is embedded inside apiece of unsuspicious information. Image steganography is a technique of conceal information into a cover image to hide it.

In this research work the first approach we have implemented is DWT based approach and is the most accepted steganography methods in frequency domain due to its simplicity and hiding ability. This wavelet provides adequate security to the load because with no significant the transformation rules no one can extract the secret data. Second Approach, we can implement the Artificial Bee Colony Optimization Technique for extracting the message from the cover image or original image. After that we can classify the design system using Back Propagation Neural Network which has been creating in two modules like Training Module and other one Testing Module.

Many information security algorithms have been developed steganography algorithms to enhance information security. One of the most recent algorithms is Neural Network. In this paper it encrypts the secret message to protect it from being accessed by unauthorized users before being hidden. The PSNR of the stego image was estimated to measure the stego images quality. The obtained results demonstrated that using secret key provides good security and PSNR value higher than previous image steganography methods. The other parameters we have used are for embedding, extractions as well as security purpose are MSE, RMSE and Time.

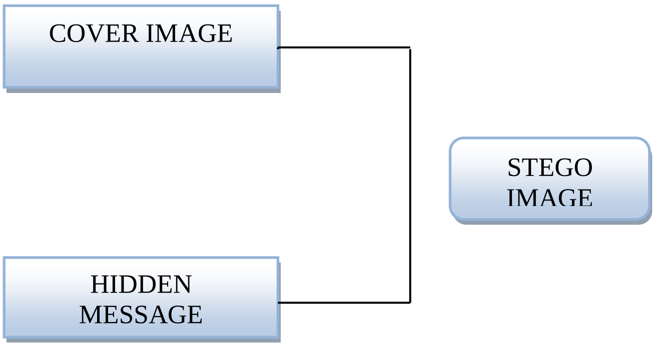

Fig1: Steganography

Cover medium + embedded message + stego-key = stego-medium

Fig 2: Mechanism of Steganography

II. RELATED WORK

Bingwen Feng et.al, described as, a binary image steganography scheme that aims to minimalize the embedding distortion on the texture is presented. They extracted the complement, rotation, and mirroring-invariant local texture patterns from the binary image first. The weighted sum of crimp changes when flipping one pixel is then employed to measure the spinning alteration corresponding to that pixel.

VojtˇechHolub et.al, 2014 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 breakdown 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.

III. PROPOSED WORK

The proposed work uses algorithms like Artificial Bee Colony algorithm of Swarm Intelligence, Back Propagation Neural Network algorithm of Artificial Intelligence and spatial domain technique called as Discrete Wavelet Transformation.

A. Artificial Bee Colony Algorithm

Kind of social insect, honey bees live in colony and exhibit many features. These features comprise bee foraging, bee party, queen bee, task selection, shared decision making, nest site assortment, mating, pheromone laying and direction-finding systems, which can be used as models for intelligent submissions. Actually, a lot of investigators have been inspired to develop algorithms by the behaviors of bees. A review of the algorithms based on the intelligence in bee swarm and their applications has been accessible in. As mentioned, the ABC algorithm proposed is one of the most accepted algorithms.

The main steps of the algorithm are given below:

- Initial food sources are produced for all employed bees.
- REPEAT
  - Each employed bee goes to a food source in her memory and determines a neighbour source, then evaluates its nectar amount and dances in the hive
  - Each onlooker watches the dance of employed bees and chooses one of their sources depending on the dances, and then goes to that source. After choosing a neighbour around that, she evaluates its nectar amount.
  - Abandoned food sources are determined and are replaced with the new food sources discovered by scouts.
  - The best food source found so far is registered.
- UNTIL (requirements are met).
- STOP.

B. Back Propagation Neural Network

The Back Propagation neural network is artificial neural network based on error back propagation algorithm. The Back Propagation (BP) neural network model consists of an input layer, some hidden layers and an output layer. Each 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 by to hidden layer which is an interior information processing layer and is answerable 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 wanted output. Each weight is reviewed and back propagated layer by layer from output layer to hidden layer and input layer. This process will be sustained until the output error of network is reduced to an acceptable level or the predetermined time of learning is achieved. The processing results of information are exported by output layers to the outside.

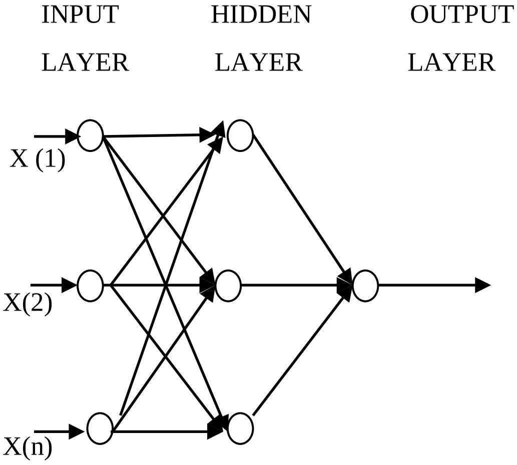

Fig 3: Back Propagation Neural Network

BP neural network consists of many neurons that are arranged in a form of three layers: input, hidden and output. The neurons are linked by weights W y In training the network with a given architecture, the back propagation approach, finds a single best set weight values by minimization of suitable error function. In a multi-layer feed forward neural network, the processing elements are arranged in layers and only the rudiments in adjacent layers are connected. It has a minimum of three layers of elements (i.e., input layer, the central or hidden layer, and the output layer). The name “back propagation” (BP) derives from the fact that computations are passed feed forward from the input layer to the output layer, following which calculated errors are propagated back in other direction to change the weights to obtain a better performance. BP algorithm is an extension of the smallest mean square algorithm that can be used to train multi-layer networks. The three-layered free forward neural network is displayed in Figure no 3 which is comprised by input layer, hidden layer and output layer.

C. Methodology

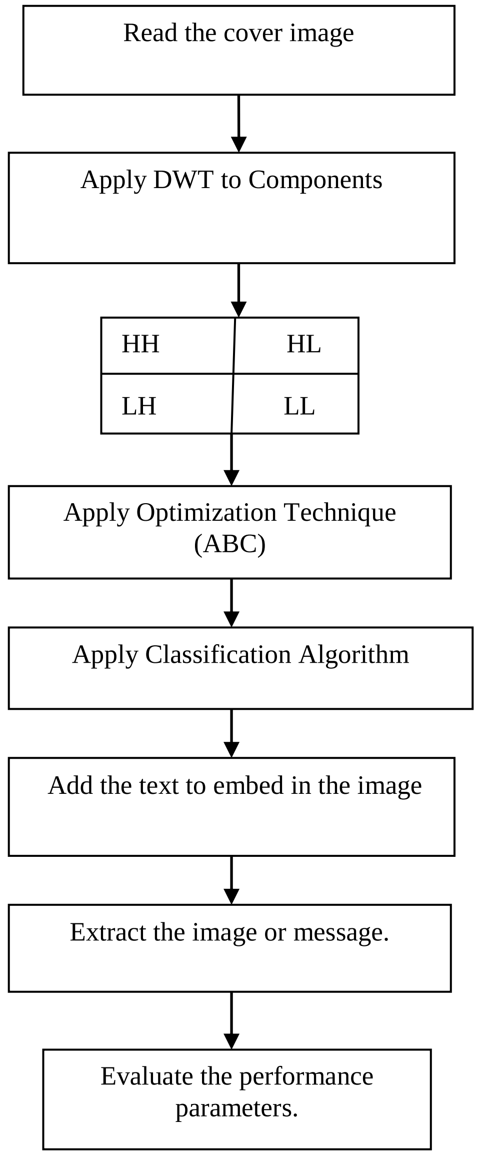
Read the cover image
Apply DWT to Components
HH
HL
LH
LL
Apply Optimization Technique (ABC)
Apply Classification Algorithm
Add the text to embed in the image
Extract the image or message.
Evaluate the performance parameters.

Fig 4: Flow Chart

D.Performance Analysis

The proposed work is compared with the existed one using various performance parameters like PSNR, MSE, RMSE & time.The research work has been implemented to enhance the image steganographic technique so that the quality of image remains same. 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, MSE, RMSE and Time consumption values.

Image no.	MSE	RMSE	PSNR	Time Consumed
1	0.15406	0.3925	56.288	0.04842
2	0.19865	0.4457	55.184	0.0021732
3	0.10447	0.32322	57.9749	0.0021516

Table No. 1 Performance Parameters

Image No.	**Mean Square Error(BP)**	**Mean Square Error(PP)**	**Peak Signal To Noise Ratio(BP)**	**Peak Signal To Noise Ratio(PP)**
1	0.13174	0.15406	50.9881	56.288
2	0.34574	0.19865	39.6562	55.184
3	0.049877	0.10447	42.1034	57.9749

Table No. 2 Comparisons Between the previous & proposed work

DOI: 10.13140/RG.2.2.18645.83687

IV. PERFORMANCE PARAMETERS

PSNR: Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the determined possible power of a signal and the power of corrupting noise that affects the reliability of its representation.

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

MSE: In measurements, the mean squared error of an estimator is one of many ways to quantify the variance between values implied by an estimator and the true values of the quantity being estimated.

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)|$$

Root Mean Square Error: RMSE of the image which methods the average sum of glossary in each pixel of the stego image or translated image and maximum pixel is the maximum value of the pixel.

$$RMSE = \sqrt{MSE}$$

Time Consumption: This parameter is used to check efficiency of the algorithm based on detection time of any information form a stego image. Because of the main part of process to find the content from the stego image so that the extraction time consumption parameter considered. Time consumption is in milli seconds for reconstruct the data bits and generate the original embedded message.

V. CONCLUSION & FUTURE SCOPE

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 optimized using seed values algorithm.

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.

VI. REFERENCES

[1] G Adel Almohammad and 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,2011.

[2] Attalla M. Al-Shatnawi, “A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, no. 79, 3907 – 3915, 2012.

[3] Deeply "Steganography with Data Integrity”, International Journal Of Computational Engineering Research (ijceronline.com), Vol.2, Issue 7, nov 2012.

[4] Diwedi samidha, and Agrawal Deepak. "Random image steganography in spatial domain." Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013 International Conference on. IEEE, 2013.

[5] 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.

[6] Gabriel Hospodar, “Algorithms for Digital Image Steganography via Statistical Restoration"_ ESAT/SCD-COSIC and IBBT, Katholieke Universities Leuven Kasteelpark Ehrenberg 10, bus 2446, 3001 Heerlen, Belgium.

[7] Gupta Rajesh, and Singh TanuPreet "New proposed practice for secure image combing cryptography,steganography and watermarking based on various parameters." Contemporary Computing and Informatics (IC3I), 2014 International Conference on.IEEE, 2014.

[8] 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.

[9] Huayong, Ge and Wang Qian. "Steganography and Steganalysis based on digital image." Image and Signal Processing (CISP), 2011 4th International Congress on.Vol. 1.IEEE, 2011.

[10] Islam, Saiful, Mangat R. Modi, and Gupta Phalguni "Edge-based image steganography." EURASIP Journal on Information Security 2014.1 (2014): 1-14.

Palak Sindhi, Student(M.tech in CSE). My wide area is DIP and I have completed my work in its sub area Steganography under the Supervision of Assistant Professor , Er. Deepinder Kaur at SUSCET, tangori mohali on “Maximizing The Steganographic Embeding Efficiency Using Wavelet Transformation.”