Proficient Encryption and Secured Password BPNN Approach for Data Hiding in Image Steganography

Vishal Garg[1], Vanita Rani[2]
[1]M.Tech Scholar, [2]Assistant Professor
CSE department, Indo Global College of Engineering

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 boasted by uniting it with cryptography. In this approach steganography and cryptography are aggregated together. During 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 neural network which is further optimized with genetic algorithm using a fitness function. The second level encryption is provided to the text which uses encryption algorithm for stego generating key and AES for encrypting text using key generated by encryption technique. So the main aim of the research work 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 and mean square error. 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, Cryptography, Least significant Bit, Discrete Wavelet Transformation, Advance Encryption Standard and Classification.

I. INTRODUCTION

Steganography is a talent of hiding statement by embedding message into an innocuous observing cover media [1]. Using steganography, an underground message is embedded inside a piece of unsuspicious information and sent without anyone knowing the survival of the secret message. Assurances can be hidden exclusive all sorts of cover information:

- Text,
- Image,
- Audio,
- Video and so on.

Most steganography values hide information inside images, as it is comparatively easy to implement. People refer image steganography as the art and information of imperceptible message, which is to secrete the very presence of hidden message in digital images. Some evidences have interested active investigates and plentiful journals in the field of image steganography [2].

.

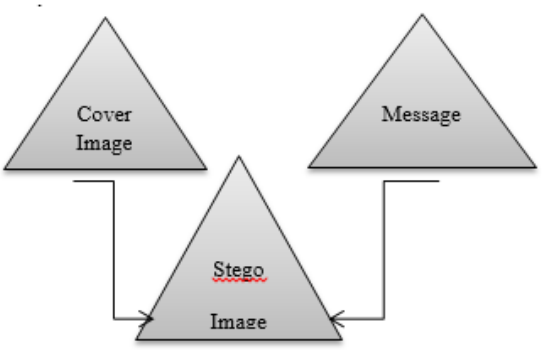


Fig.1: Scenario of Steganography

For instance, images can convey a large of information particularly on the internet. Furthermore, the non-stationary of images makes image steganography hard to break[3]. Nowadays, ordinal image has become a significant channel to bear stego information. The steganography can be categorized according to its significance and aims. So; several types of steganography are:

A. Language Steganography: Linguistic procedure [4] is used to hide the message within the cover text in non-obvious way such that the existence of message is invisible to an outsider. It is divided into two types:

a) Seagram's: It uses only signs and marks to hide the information. It is further categorized into two ways:

i) Visual Seagram's: A visual Seagram's uses corporeal objects used every day to convey a communication. For instance: the placing of items on a certain website.

ii) Text Seagram's*:* This type is used to hides a message by adjust the entrance of the carrier text, or by varying font size and type, or by addition extra space between words and by using dissimilar succeeded in letters or handwritten text.

iii) Open Code: In this method the message is entrenched in legitimate translations of cover text in the way such that it looks not obvious to an unsuspecting observer [5].

B. Technical Steganography: Technical steganography uses singular tools, devices or methodical methods to hide a message. In this type one can use

indistinguishable ink, microdots, computer based methods or various beating places to keep message secret.

(i) Cover*:* The cover communication is the carrier of the message such as image, video, audio, text, or some other digital media. The cover is separated into blocks and message bits which are hidden in each block. The material is encoded by changing various belongings of cover image. The cover masses remain untouched if message block is zero.

a) 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. The cover text produced by this approach can qualify for linguistic steganography if text is linguistically driven [6].

b) 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. 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.

II. TRANSFORMATION TECHNIQUES

Steganography has two types: a) spatial domain and b) Frequency Domain

In spatial domain, images are considered by pixels. Simple emblems could be embedded by adjusting the pixel values or the least significant bit values. It straight loads the raw data into the picture pixels. Some of its algorithms are LSB[7].

a) Spatial Domain: In this technique only the least significant bits of the cover object is swapped without modifying the comprehensive cover object. It is a simplest technique for data hiding but it is very weak in resisting even simple attacks such as compression, transforms.

i) Least Significant Bit: This is the most joint, simple method for embedding data in a cover image. The least significant bit (8th bit) of one or all of the bytes inside an image is changed to a bit of the secret message [8]. When we use 24-bit image, three colour bits apparatuses are used which are red, green, blue, each byte store 3 bits in every pixel. An 800 × 600 pixel picture, can thus store a total amount of 1,440,000 bits or 180,000 bytes of entrenched data. For sample a grid for 3 pixels of a 24-bit image can be as follows:

(00101111 00011100 11010100) (10100110 11010100 00001100) (11010010 10101101 01100011)

When the amount 200, which binary symbol is 11001000, is embedded into the least significant bits of this part of the image, the subsequent grid is as follows:

(00101101 00011101 01011100) (10000110 11000101 00001100) (11010010 10101100 01100011)

b) Frequency Domain

i) Discrete Wavelet Transformation

It gives the best consequence of image transformation, it separations the signal into 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 [9,10] instead of changing bits of the actual pixels. It also performs local analysis and multi-resolution analysis. DWT transforms the object in wavelet domain and then processes the coefficients and performs inverse wavelet transform to show the innovative format of the stego object.

III. RELATED WORK

Carlos Munuera et.al, 2014,[11] In this paper describes as knowledge the application of Show codes to wet paper steganography. To that end, they propose the use of decoding algorithms that do not verify the smallest distance property and current one of these algorithms. They review its properties and show consequences of some numerical experimentations. **V. Saravanan et.al ,2013 [12]** This paper decreases the obvious distortion in a joint photographic experts group file during data hiding process, by presenting new region selection rule. The new region selection rule reflects three factors, i.e., the horizontal difference, vertical difference and region size. The JPEG image will be split into quantity of blocks and each pixel in it will be inspected to calculate the differences. Depends upon the difference, the amount of secret material will be hide in an image. **Gandharba Swain et.al,2012 [13]** In this paper a new smallest significant bit array based image stenographic procedure using encryption by RSA algorithm is suggested. In the copy each pixel is 8 bits. The four arrays, namely the LSB, LSB1, LSB2 and LSB3 are framed unconnectedly by assembling the bits from the 8th (LSB), 7th, 6th and 5th bit locations of the pixels respectively. The cipher text is separated into four blocks. The first block is mapped and sided over the LSB array and embedded at maximum similar serving of LSB array. Correspondingly the second, third and fourth blocks are embedded at maximum matching portion of LSB1, LSB2 and LSB3 arrays individually. Where the blocks are embedded, the start indices are apprehended and embedded at a separate place in the image. The recovering process at the receiver is the reverse of the sender. The presentation of this technique is compared with other techniques.

Shashikala Channalli et.al; 2009 [14] in this paper propose a new form of steganography, on-line hiding of info on the

output screens of the instrument. This method can be used for broadcasting a secret memorandum in public place. It can be extended to other means such as electronic advertising board about sports stadium, railway station or airport. This method of steganography was very similar to image steganography and video steganography. Private marking system using symmetric key steganography technique and LSB technique was used here for hiding the secret information. **Weiming Zhang et.al [15]** In this paper propose a new method to construct stego-codes, display that not just one but a family of stego-codes can be produced from one covering code by combining Show codes and wet paper codes. This method can enormously expand the set of embedding schemes as applied in steganography.

IV. ISSUES IN STEGANOGRAPHY

The various studies revealed from the literature survey cannot fill the gaps that occurred in information security system. More research in terms of security is needed for optimization of previous techniques in terms of security point of view. Some of the demerits can be noted which existed in the previous approaches studied so far [16]**;**

Problem with the already existing scheme is that the quality of image degrades after merging any text content. This is because of the bit distortion during embedding extra data inside it[17]. MSE and PSNR need to be optimized which define the quality of image. Data embedding and extraction scheme should also be optimized. An approach is needed to be proposed for data embedding and extraction scheme which gives a better security and accuracy[18]. Existing system does not perform any check point on extraction so an approach has to be proposed by using a password protected mode. Hybridization of algorithms is needed for enhancement of the security [19,20].

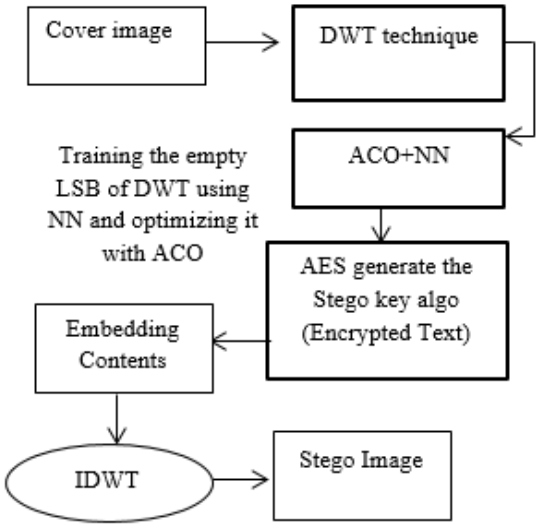
V. METHODOLOGY

In this section, we explained the proposed work with flow chart:

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

-Transformed image: It will denote the probabilistic composition of the frequencies for the cover image. Thus the image will be composed of DWT coefficients.

-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.

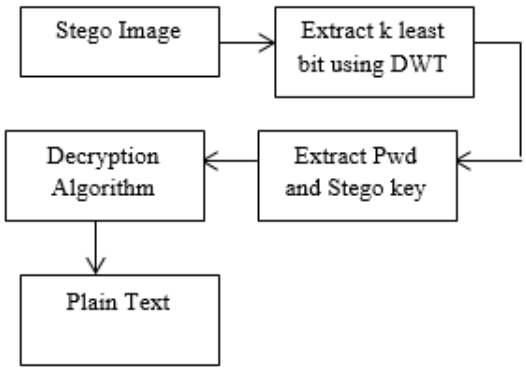


(i) Sender Side Process

-Encrypted text: It will denote the encrypted form of data that is the important message to be concealed inside least bit data.

-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 translated secret message which is covered within the carrier image.

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



(ii) Receiver Side Process

Fig.2. Sender and Receiver

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.

IV. RESULT AND DISCUSSION

It defined that the main screen source and destination side interface is given .First the input image which is either in jpg or png form is taken. The wavelet decomposition of input image is taken which is done using DWT transformation. It will compress image using 1D DWT function.

The above figure shows that the decryption time. Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

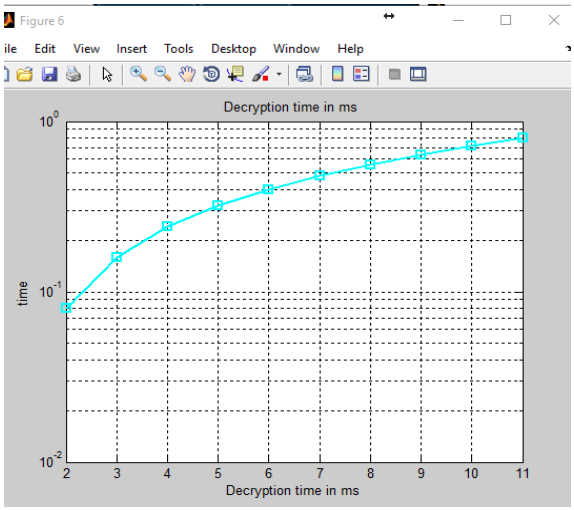


Fig.3. Decryption Time

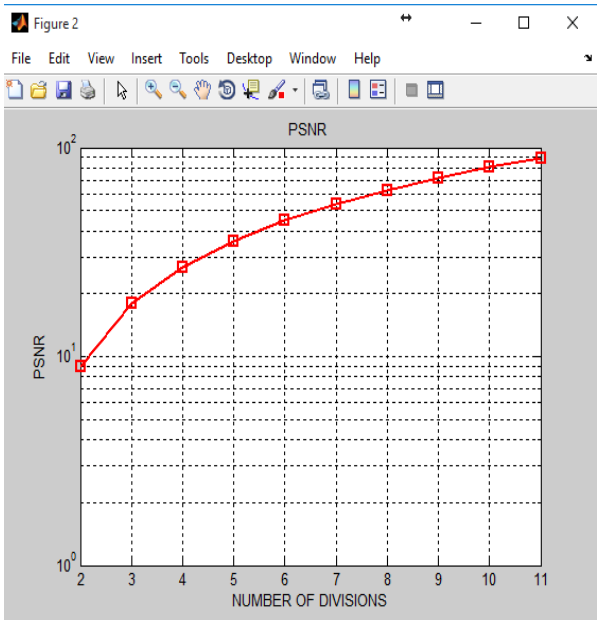


Fig.4 Psnr (Proposed Work)

The above figure shows that the Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of unbecoming noise that affects the fidelity of its symbol. ... PSNR is most easily defined via the mean squared error (MSE).Bit error rate means the rate at which errors occur in the transmission of digital data.

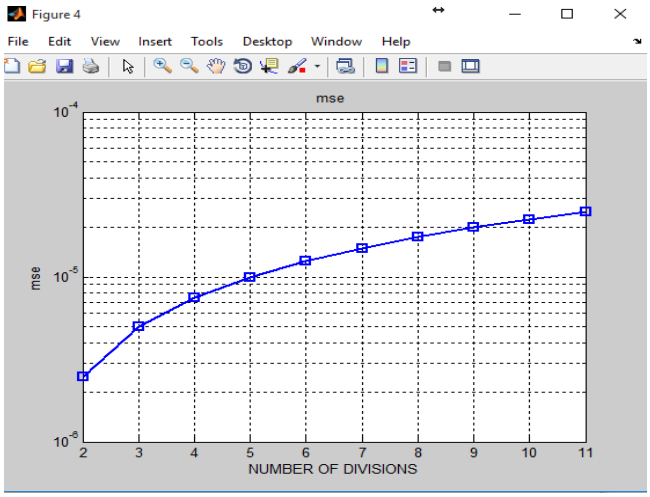


Fig.5. MSE (Proposed Work)

The Mean Squared Error (MSE) is a measure of how close a fitted line is to data points. For every data point, you take the distance vertically from the point to the conforming y value on the curve fit (the error), and square the value.

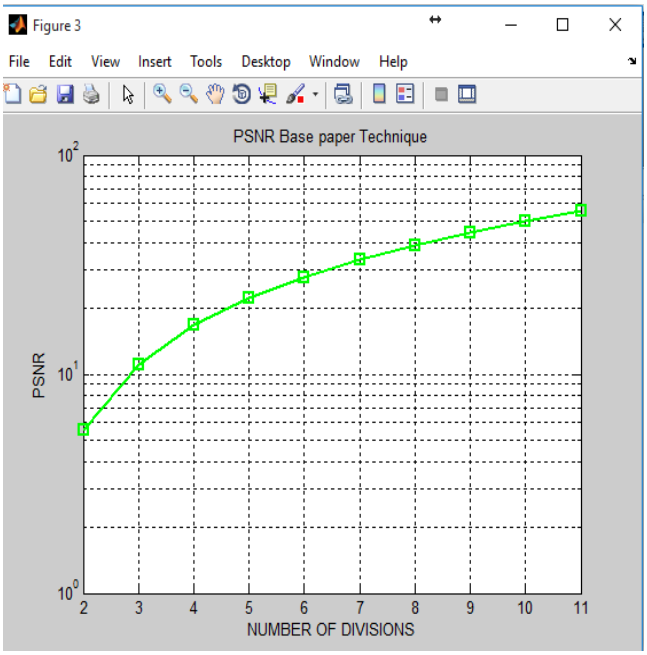


Fig.6. PSNR (base paper)

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

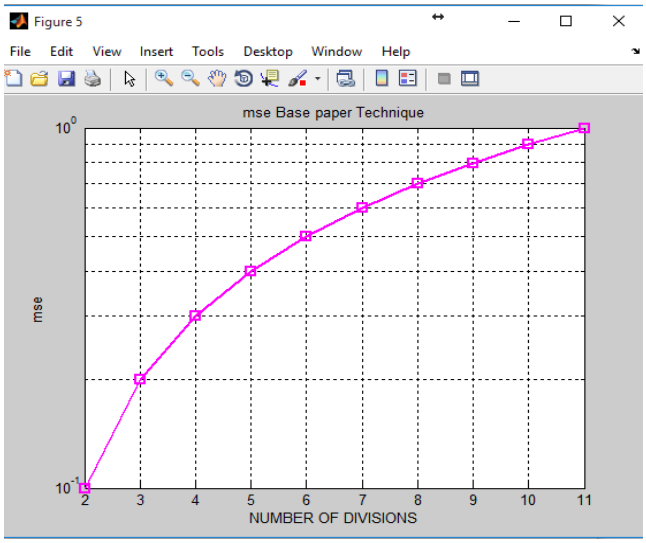


Fig.7. MSE (base Paper)

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.

V.CONCLUSION AND FUTURE SCOPE

The proposed system has discussed implementation of securely using steganography method based on BPNN, AES 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 application is being taken place in MATLAB atmosphere. 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 convinced set of training data which might be automatically produced and is disposed after the task has been performed.

VI. REFERENCES

[1]. Attalla M. Al-Shatnawi(2012), "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, no. 79, 3907 – 3915.
[2]. 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.
[3]. 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.
[4]. 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).
[5]. 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.
[6]. 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.
[7]. 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.
[8]. 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.
[9]. 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.
[10]. Prashanti, G., and K. Sandhyarani. "A New Approach for Data Hiding with LSB Steganography." Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Springer International Publishing, 2015.
[11]. Munuera, Carlos. "Hamming codes for wet paper steganography." Designs, Codes and Cryptography 76.1 (2015): 101-111.
[12]. Saravanan, V., and A. Neeraja. "Security issues in computer networks and stegnography." Intelligent Systems and Control (ISCO), 2013 7th International Conference on. IEEE, 2013.
[13]. Swain, Gandharba, and Saroj Kumar Lenka. "LSB array based image steganography technique by exploring the four least significant bits." Global Trends in Information Systems and Software Applications. Springer Berlin Heidelberg, 2012. 479-488.
[14]. Channalli, Shashikala, and Ajay Jadhav. "Steganography an art of hiding data." arXiv preprint arXiv:0912.2319 (2009).
[15]. Zhang, Weiming, Xinpeng Zhang, and Shuozhong Wang. "Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes." In International Workshop on Information Hiding, pp. 60-71. Springer Berlin Heidelberg, 2008.

[16]. EL-Emam, Nameer N. "Hiding a large amount of data with high security using steganography algorithm." Journal of Computer Science 3.4 (2007): 223-232.
[17]. 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.
[18]. M. Dorigo, G. Di Caro, and L. M. Gambardella. Ant algorithms for discrete optimization. Artificial Life, 5(2):137–172, 1999.
[19]. Sirisha, B. Lakshmi, S. Srinivas Kumar, and B. Chandra Mohan. "Steganography based information security with high embedding capacity." In Recent Advances in Electronics & Computer Engineering (RAECE), 2015 National Conference on, pp. 17-21. IEEE, 2015.
[20]. Koptyra, Katarzyna, and Marek R. Ogiela. "Key Generation for Multi-Secret Steganography." In Information Science and Security (ICISS), 2015 2nd International Conference on, pp. 1-4. IEEE, 2015.