The Secure Data Hiding Framework Design in DWT and optimization approach in 3D images in Steganography

Deepika Sharma[1], Jaskiran Kaur[2]

[1]M.Tech(Scholar), [2]Assistant Professor

Department of Computer Science Engineering , CEC Landra, Punjab

Deepikasharma025@gmail.com[1],jaskiran.kaur15@gmail.com[2]

Abstract – Steganography is doing to define it significance due to the exponential development and secure information of computer consumers over the internet. It could be defined as the survey of hidden communication that normally describes with the path of abstracting the presence of communicated message. Normally, data embedding is realized in message, imagery, test, mutli-media and voice, military communication, authentication and various other resolutions. In Image Steganography, secure communication is realized to hide a message into original or cover image and calculate a stego-image. In this paper, we proposed Discrete Wavelet Transformation, Ant Colony Optimization Approach and classification (BPNN) algorithm. In proposed technique improve the image quality with PSNR parameter according defined and using MATLAB (GUI) 2013a simulation tool.

Keywords:- 3D-images, Data hiding, steganography, secure communication and Classification.

I. INTRODUCTION

With the growth of computer network, security of data has become a main concern and thus data hiding technique has concerned people around the world. Steganography techniques are used to deal with digital copyrights management, protect information, and conceal secrets. Data hiding techniques provide a motivating challenge for digital forensic investigators. Data is the backbone of today's communication [1]. To ensure that data is secured and does not go to unplanned destination, the concept of data hiding came up to protect a part of information. Digital data can be delivered over computer networks with little errors and often without interference. The Internet provides a communication method to distribute information to the masses. Therefore, the privacy and data reliability are required to protect against unauthorized access and use.

Sending of massages safely and securely has been top priority for any organization that deals with confidential data. Information hiding techniques are necessary for military, intelligence agencies, internet banking, privacy, etc. so it is on-going research area in present time [2]. Increased uses of internet, information become available on-internet, a person who possesses an internet can easily get data from internet for information that they want. As more and more techniques for hiding information are developed and improved, more and more different information detecting techniques are also developed. That has produced a strong need to create new techniques for protecting confidential information from hackers. There are numbers of data hiding techniques available for different purpose and applications like steganography, cryptography, and watermarking.

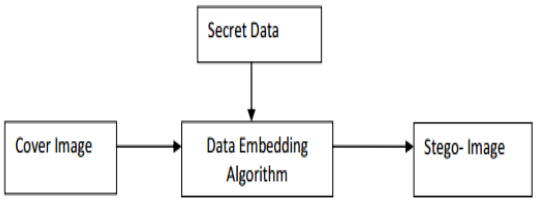


Fig. 1: Steganography Block Diagram

Application:

- Confidential Communication and Secret Data Storing
- Protection of Data Alteration
- Access Control System for Digital Content Distribution
- E-Commerce
- Media
- Database Systems.
- Digital watermarking.

In Section I , defined that the introduction defined steganography, secure communication and data hiding. Section II discuss the previous work in various paper survey and found the issues and benefits in Steganography. Section III described the problem on Image Steganography. Section IV. Defined that the techniques of the Steganography and transformation. Section V. discussed the result of the proposed

work. Section VI. Conclusion and future scope described that an image

II. RELATED WORK

Hilal Almara et al., 2016 [3] discussed with due to the evolution of computer technologies and the internet, the security of information considers as the most challenges in communication to protect information. A large variety of stenographic techniques exists for hiding information in an appropriate carrier such as text, image, audio, video, and protocol, and can be sent to a receiver secretly. The techniques of audio and video steganography can be used to hide secret information by using another mechanism such as audio and video files. This paper presents a general review of steganography and a critical study of research papers in various techniques used in audio and video steganography. Dr. Rajkumar et al.,2016 [4] data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. In image Steganography, secret communication is achieved to embed a message into cover image (used as the carrier to embed message into) and generate a stego-image (generated image which is carrying a hidden message). In this paper we have critically analysed various stenographic techniques and also have covered steganography overview its major types, classification, applications. Jigar Makwana et al., 2016 [5] provides several advantages like better quality, ease of editing, high fidelity, compression, etc. But with rapid growth of World Wide Web and advance computer network, there are some issues related to content security, privacy, and media authentication. In modern age in which data is conveyed through digital medium, the protection of data is top priority concern for any organization. Digital steganography is an advance technique in which secret data can't be detected easily. Steganography envelopes and information to such degree that it is invisible to a spectator. In this proposed paper the focus is on increasing data security using dual steganography. In dual steganography secret message is first embedded into cover medium and then resulted stego-object will be again embedded into other cover medium. Sumeet Kaur et al., 2014 [6] Information is wealth of any organization and in present era in which information transferred through digital media and internet, it became a top priority for any organizations to protect this wealth. Whatever technique we adopt for the security purpose, the degree and level of security always remains top concern. Steganography is one such technique in which presence of secret message cannot be detected and we can use it as a tool for security purpose to transmit the confidential information in a secure way. It is an on-going research area having vast number of applications in distinct fields such as defence and intelligence, medical, on-line banking, on-line transaction, to stop music piracy and other financial and commercial purposes. There are various steganography approaches exist and they differs depending upon message to be embedded, use of file type as carrier or compression method used etc. The focus of this paper is to classify distinct image steganography techniques besides giving overview, importance and challenges of steganography techniques.

III. TYPES OF STEGANOGRAPHY

A. Text steganography:

It consists of hiding the information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file [7]. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.

B. Image steganography:

Hiding the data by attractive the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are extensively used cover source because there are number of bits presents in digital representation of an image.

C. Audio steganography:

It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods [8] of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

D. Video Steganography:

It is the technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

E. Network or Protocol:

Steganography It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. In the OSI layer network model there exist secret channels where steganography can be used.

IV. PRIOR ALGORITHM

In this section, we discussed the previous algorithm using LSB, DWT and DCT Algorithm:

A. Least Significant Bit Algorithm:

LSB (Least Significant Bit) replacement is the process of adjusting the LSB pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is distorted to the bit of secret message. For JPEG, the direct substitution of stenographic techniques is not possible since it will use loss compression. So it uses LSB substitution for embedding the data into images [9].

B. SPIHT Algorithm:

The SPIHT algorithm is a more efficient implementation of EZW (Embedded Zero Wavelet) algorithm which was presented by Shapiro. After applying wavelet transform to an

image, the SPIHT algorithm partitions the decomposed wavelet into significant and insignificant partitions based on the following function [10].

V. PROBLEM FORMULATION

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 The difficult in the hiding info or Steganography is the size of data that user want to embed inside the multimedia file, image is one of the program file, the most commend method for hiding information in the image is LSB, LSB[11] is effectual instead of that it's not easy to analysis, however, it is not effective in term of the data hidden quantity, all investigators decided the fact that the size of data hidden is a problem in that particular area, the other difficult that challenged there, in fact if we try to increase the quantity of data in the image there will be a suspect deviations which become clear to human eyes, for instance, this research will face a challenge that high rate data hidden without disturbing the images quality, there are many trends that needs to be fallowed, initially; how can the new algorithm growth the amount of data, then what is the feature in the new image, how can the new algorithm deal with, all this objects will be converse in-depth in this research by suggest an enhancement to the work of hiding information in the image using the human vision system.

As a summery, the main problems in the Steganography fallow as [12]:

- The size of data hidden
- Quality of image
- Algorithms that apply should also cover the gray level image
- Level of data protecting
- The level of suspecting

The aim of the thesis is to hide the data i.e., hide the data over an image using dissimilar steganography algorithms and to associate those algorithms in the context of speed, quality of hiding and the use of marks and to describe their functionality in data security.

VI. RESULTS AND DISCUSSIONS

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.

A. Discrete Wavelet Transformation:

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 [13] 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 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 2 (a) [14,15] .

LL	HL
LH	HH

Fig. 2: (a) DWT components

Formula of Discrete Wavelet Transform:

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

In next paper we will described the implementation algorithm i.e Ant Colony Optimization and Classification Approach.

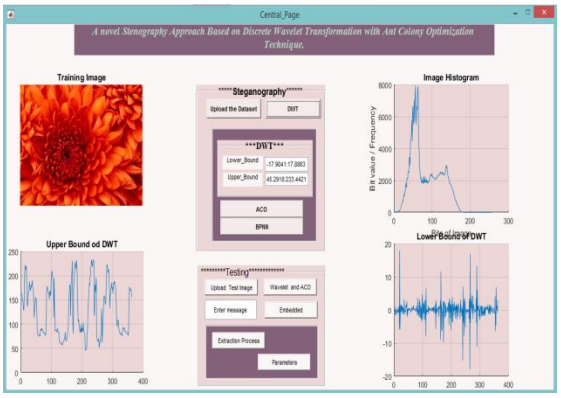


Fig. 3: Main Frame

Figure no. 3 the main screen source and destination side interface is given.The first input image which is either in jpg or png form is taken. The wavelet decomposition of the input image is taken which is done using DWT transformation. It will compress the image using 1D DWT functions. Plot the histogram means identifying the minimum and maximum frequency of the original image. The diagram consisting of rectangles whose area is proportional to the frequency of a variable and whose width is equal to the class interval. The lower bound with the help of Discrete Wavelet Transform. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information. The above figure shows that the higher values of the wavelet transformation.

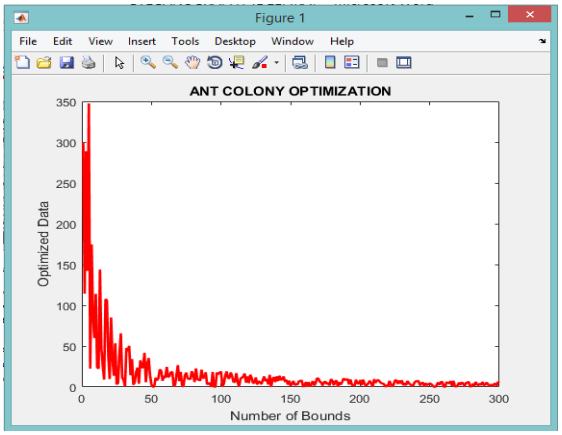
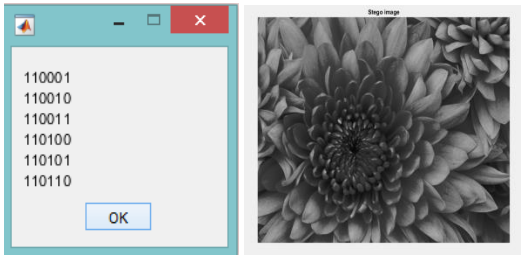
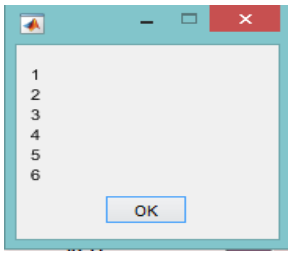


Fig. 4: Ant Colony Optimization

The above figure shows that the Ant colony optimization technique used for optimized the output data. We use the fitness function for calculate the fit value of the transform image. A classification technique to improve the server performance, according to the training module and testing module. Run time set the 1000 epochs work in real time only 4 epochs and time consumed 0.1 second, performance is 0.212 exp and used 3 validation checks. the best validation performance, according to the number of iterations corresponding to the mean square error rate.



(i) (ii)



(iii)

Fig. 5: (i) Stego image, (ii)Secret Data and (iii) extract message from the original image.

Figure 5. Destination Ask the Password to decryption and Generate the Stego image. The destination point ask the enter the encrypt password and the message is ready for the retrieval.

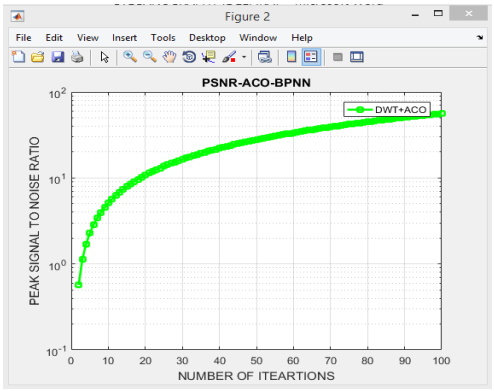


Fig. 6: Peak Signal to Noise In proposing Work

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 corrupting noise that affects the fidelity of its representation. ... 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.

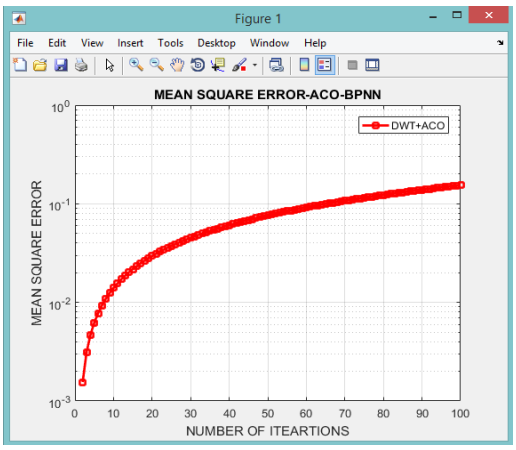


Fig. 7: Mean Square Error Rate

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 corresponding y value on the curve fit (the error), and square the value.

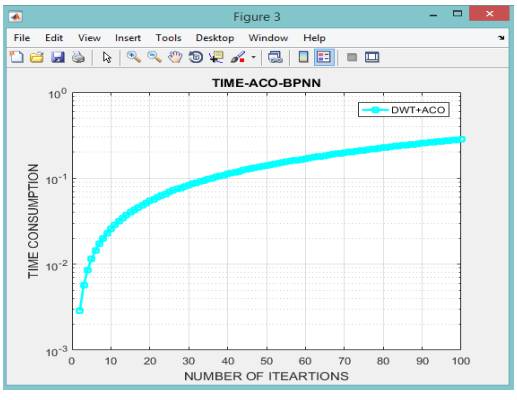


Fig. 8: Time Consumption

This parameter used to check the efficiency of the algorithm based on detection time of any information from 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 mili seconds for reconstructing the data bits and generate the original embedded message.

Table 1. Proposed Work

The Below table 1 described the Proposed Values.

Img no.	Img 1	Img 2	Img 3	Img 4	Img 5
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

VII. CONCLUSION AND FUTURE SCOPE

The proposed system has discussed implementation of securely using steganography technique based on BPNN , ACO and DWT algorithm. In these years, LSB is the most widely used technique for steganography. Some researchers have also used the techniques like water marking, distortion technique, spatial technique, ISB, MSB in their work and provided a strong means of secure information transmission.

In future scope, we can implement the High speed algorithm design to maintain the image quality and hide the information in Steganography.

VIII. REFERENCES

[1] Bawaneh, Mohammed J., and Atef A. Obeidat. "A Secure Robust Gray Scale Image Steganography Using Image Segmentation." *Journal of Information Security* 7, no. 03 (2016): 152.

[2] Mstafa, Ramadhan Jahfar, and Christian Bach. "Information Hiding in Images Using Steganography Techniques." In *American Society for Engineering Education (ASEE Zone 1), 2013 Zone 1 Conference*. 2013.

[3] Hilal Almara'beh," Steganography Techniques - Data Security Using Audio and Video", International Journal of Advanced Research in Computer Science and Software Engineeringm vol 2 Issue 3, feb 2016.

[4] Lakhani, Hardik, and Aspriha R. Das. "A Survey Paper on: Steganography Techniques." *Digital Image Processing* 7, no. 1 (2015): 23-25.

[5] Makwana, Jigar, and S. G. Chudasama. "Dual Steganography: A New Hiding Technique for Digital Communication." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , Vol. 5, Issue 4, April 2016.

[6] Kaur, Sumeet, Savina Bansal, and R. K. Bansal. "Steganography and classification of image steganography techniques." In *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*, pp. 870-875. IEEE, 2014.

[7] Thenmozhi, M. J., and T. Menakadevi. "A New Secure Image Steganography Using Lsb And Spiht Based Compression Method." *International Journal of Engineering* 16 (2016): 17.

[8] Kour, Jasleen, and Deepankar Verma. "Steganography Techniques–A Review Paper." *International Journal of Emerging Research in Management &Technology ISSN* (2014): 2278-9359.

[9] Verma, JasleenKourDeepankar, and Deepankar Verma. "Steganography Techniques-A Review Paper." *International Journal of Emerging Research in Management &Technology* 3, no. 5 (2014).

[10] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[11] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[12] Ishwarjot Singh ,J.P Raina," Advance Scheme for Secret Data Hiding System using Hop field & LSB" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[13] G. Manikandan, N. Sairam and M. Kamarasan "A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme ", Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012.

[14] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[15] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, "Extracting spread-spectrum hidden data from digital media ", IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.information forensics and security, vol. 8, no. 7, july 2013.