JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Image Steganography Using Edge Detection Technique

[1*]Kirti Chopra, [2]Er. Ishpreet Singh Virk

Department of CSE Baba Banda Singh Bahadur Engineering College

Available online at: www.ijcseonline.org

Accepted: 12/Dec/2018, Published: 31/Dec/2018

***Abstract*—** Nowadays, the mechanisms are growing among the high speed and novel developments are accomplished day by day. Every day as a huge amount of data shared within the diverse users on the internet so the sharing of data is enhanced. In order to hide the occurrence of the communication, the steganography is utilized. In a suitable carrier such as image, video or audio this mechanism deals among the insertion of the secret message. Due to its broad utilization on the internet, the digital images are majorly preferred over the other carriers. For the implementation, the MATLAB software is utilized. In this paper, a couple of methods are utilized to embed the secret message. Those methods are original binary form and complemented form of a binary converted message, to advance security. For the embedding purpose, fuzzy edge detection technique is utilized and in order to hide the information into an image, the LSB mechanism is proposed. In the proposed work fuzzy technique will be utilized to offer more sharp edges having more data and to acquire the continuity. Huffman coding compression technique is utilized to compress the data and also to send more data on less space. The MSE, BER, and PSNR are utilized as a calculation of performance analysis.

***Keywords*—** PSNR, Bit Error Rate, MSE, Stegnography, Huffman Coding.

I. INTRODUCTION

Steganography is word taken from the two Greek words as "steganos" and "graphie" which imply "disguised" and "expressing" independently. Mutually it alluded as hid (covered up or secured) the message. In 1499 first term was used by the Johannes Trithemius in his Stegno-graphia. He has made a hypothesis on the cryptography and Steganography conceal as a book on enchantment. In this way message which is concealed under the dissent is considered as cover which can be of anything i.e. pictures, articles, shopping records or other cover content. Thus, it is a high security strategy considered for long data transmission.

Accordingly, Steganography is the route toward disguising the message before transmit it to the collector. Data can be covered up inside another electronic medium, for instance, content, picture, sound or video. With the use of this system interloper won't have the ability to the occurrence with the message. Steganography can be associated with cryptography. Following exhibits the model of Steganographic process with cryptography:

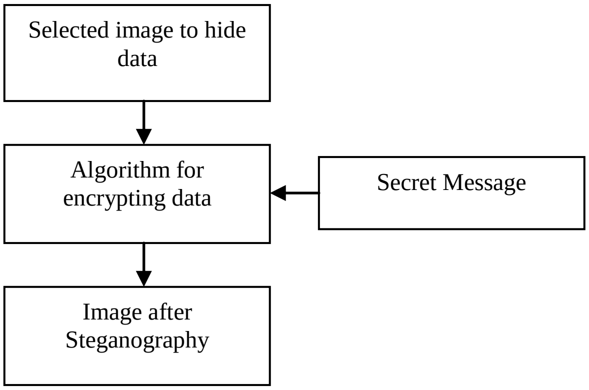
Selected image to hide data
Algorithm for encrypting data
Secret Message
Image after Steganography

Figure 1 building block of Steganography

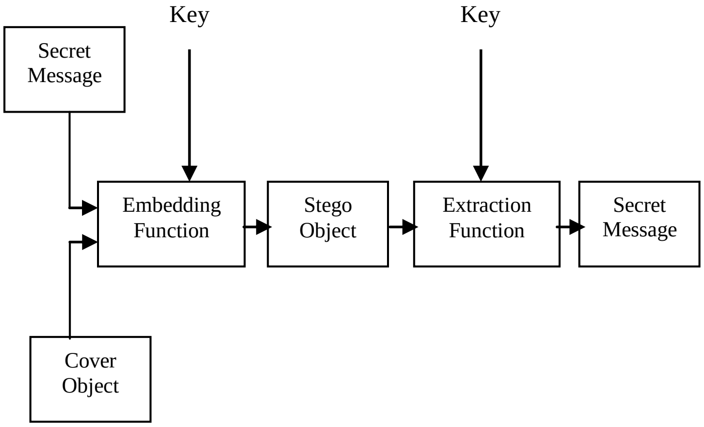

Figure 2 A model of the Steganographic process with cryptography

General Concept or motivation driving execution of picture Steganography is to impart between the people without having anxiety of being struck of messages. On account of its purposes of intrigue, it has been used in a couple of locales including military, learning operators or offices. These fields of covert work required a system which can hide their essential data and no direct individual can survey the significance of the data. The rule target of using Steganography is to keep up a key separation from the thought of the attacker from the covered information in the transmitted just as aggressor would come to understand that there is a covered data into the sent message then onlooker will endeavor each possible idea with the objective that he can read the covered message. Steganography joined with the frameworks known as Steganography frameworks utilizing wordings seem to be:

1. Cover Message
2. Secret Message
3. Secret Key
4. Embedding Algorithm
5. Extracting Algorithm

1. Cover Message is the carrier of the message which can be in any format such as an image, audio, video, text or any digital media.

2. Secret Message is the message that needs to be hidden which will be hidden using cover message discussed above.

3. Secret Key this key is use to embed the message with the help of different hiding algorithms.

4. Embedding Algorithms these algorithms are used to embed the message into the cover message.

5. Extracting Algorithm these algorithms are used at the receiving side where receiver extracts the hidden message from the stegno file using secret key.

II. PROBLEM FORMULATION

Steganography is a method utilized to transfer a secret message from a sender to a collector in a way with the end goal that a potential interloper does not expect the presence of the message. Generally this can be done by embedding the secret message within another digital medium such as text, image, audio or video. Different Steganography procedures have been proposed before but still the required outcomes were not accomplished. Based on writing survey it is established that the strategy that was generally utilized with the end goal of image Steganography was LSB (Least Significant Bit). The main problem in traditional method is that canny edge detection approach provides less no. of sharp edges due to which we can send less data. So there is a need to replace the old technique with the new one. So that new technique provides more sharp edges and continuity. More data will be transmitted on more number of sharp edges. Another problem is the size and the security of the data. In traditional methods less data covers large space so data compression technique is needed to compress the data so that more data will be transmitted on low space and security is also increased by one level with the use of compression technique.

III. PROPOSED WORK

In order to resolve the issues of the existing technique, a new method is combined with the LSB technique fuzzy edge detection technique. The image stegnographic algorithms are presented for embedding secret messages in images. In the proposed technique, initially the image is extracted from the database and then embedding and data hiding is performed. For the embedding purpose, fuzzy edge detection technique is used and to hide the data into an image LSB technique is proposed. In the proposed work fuzzy technique will be used which provides more sharp edges having more data and continuity will be achieved. In traditional methods firstly data is converted into ASCII code and then to binary code which covers a lot of space and security is also an issue here. So we need to compress the data by a compression technique. Hence there is a requirement to develop such a technique that can be able to secure the data as well as to send more data on less space by using compression technique that is Huffman Coding.

IV. METHODOLOGY

Image Embedding:

1. First step is to select the cover image for the purpose of image steganography.
2. Next step is to design fuzzy system.
3. Perform edge detection by using FIS.
4. The image with detected edges is obtained.
5. While selecting the image for steganography, simultaneously, the text for hiding is entered by the user.
6. After entering the text, next step is to convert the text to its ASCII code.
7. The ASCII code is then converted to the Binary code.
8. The compression is applied to the binary code.
9. Then the data hiding is done by using the edge detected image and compressed data.
10. Finally, the stego image is obtained.

Data Extraction

1. First step in this process is to select the stego image.
2. After selecting the stego image the edge extraction is performed.
3. The data from the detected edges is extracted in this step.
4. Perform the decompression of extracted data.
5. Convert the Binary data to the ASCII code.
6. In last the ASCII code is converted to the Characters for readability purpose.

4.3 Block Diagram of proposed work

1. Image Embedding Process

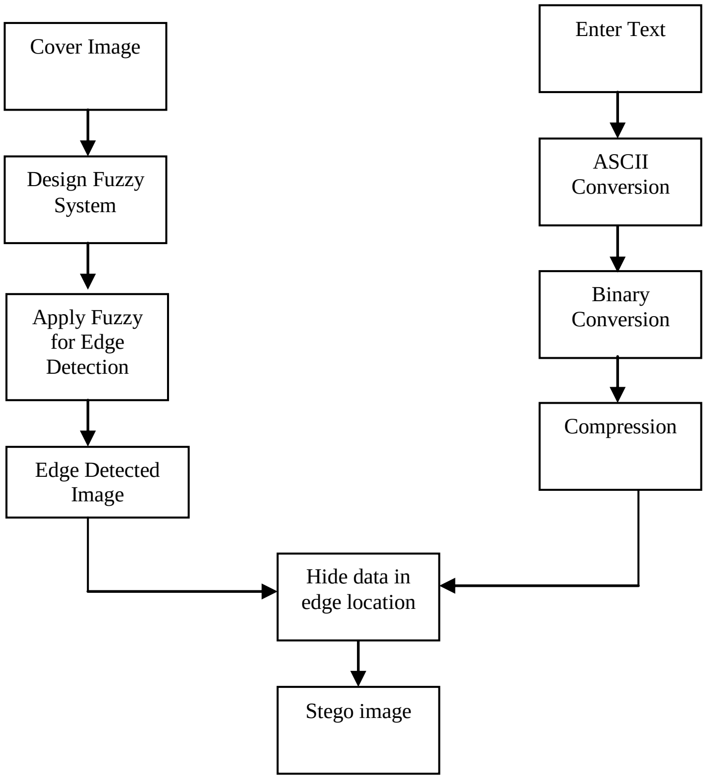

Figure 3 Proposed Data Embedding Process

2. Data Extraction

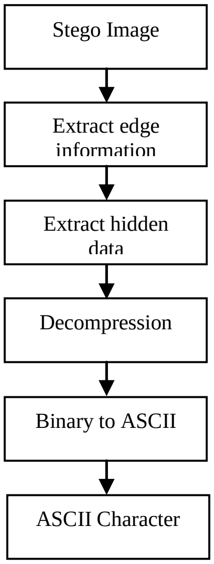

Figure 4 Proposed Data Extraction Process

V. SIMULATION MODELS

1. Result of the proposed work among original Binary stream of the secret message:

The graph of Figure 5 shows the Comparative Analysis of PSNR of Fabric of the proposed and the traditional method. The PSNR of the Fabric is shown on the y axis of the graph whereas the traditional and proposed mechanism is shown on the x axis. The value of the PSNR of Fabric ranges from 0 to 80. The PSNR of the proposed work is much higher than the traditional work.

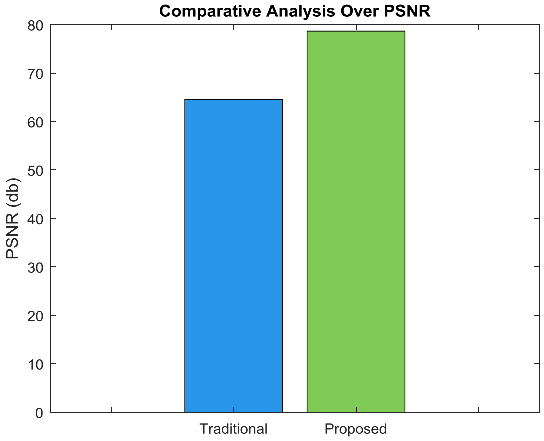

Figure 5 Comparative Analysis of PSNR of Fabric

The graph of Figure 6 shows the Comparative Analysis of PSNR of Onion of the proposed and the traditional method. The PSNR is shown on the y axis of the graph whereas the traditional and proposed mechanism is shown on the x axis. The PSNR of the proposed work is high comparative to the traditional work.

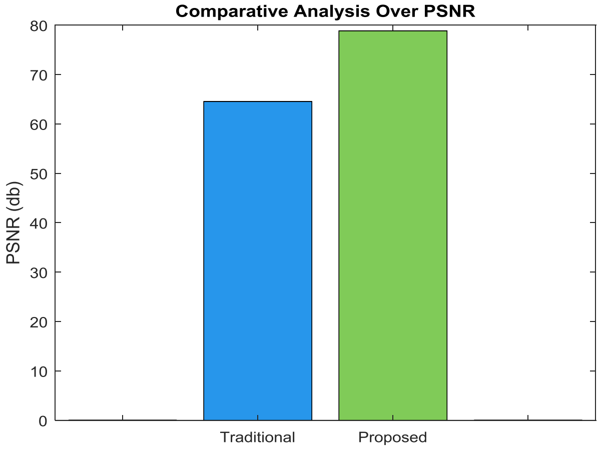

Figure 6 Comparative Analysis of PSNR of Onion

The graph of Figure 7 shows the Comparative Analysis of PSNR of Pears of the proposed and the traditional method. In the signal the proportion of the information and the noise is referred to the PSNR which supposed to be high. In this graph the PSNR of the Fabric increases gradually for different Q-Factors.

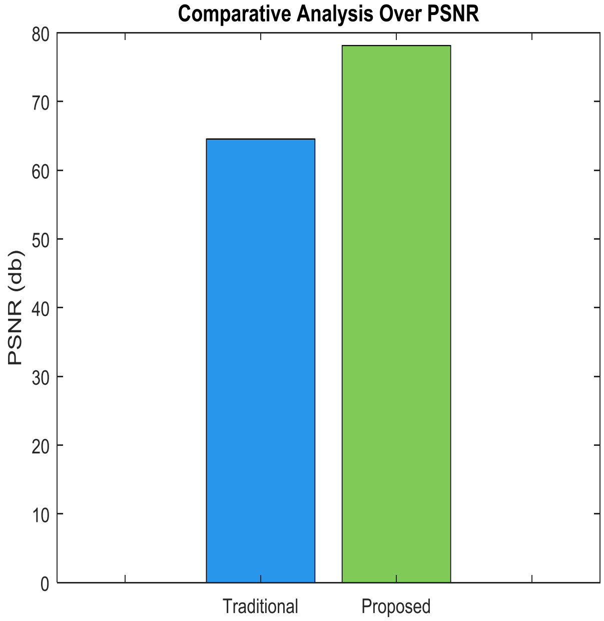

Figure 7 Comparative Analysis of PSNR of Pears

The graph of Figure 8 shows the Comparative Analysis of PSNR of Pears of the proposed and the traditional method. The value of PSNR ranges from 0 to 80. The PSNR should be high.

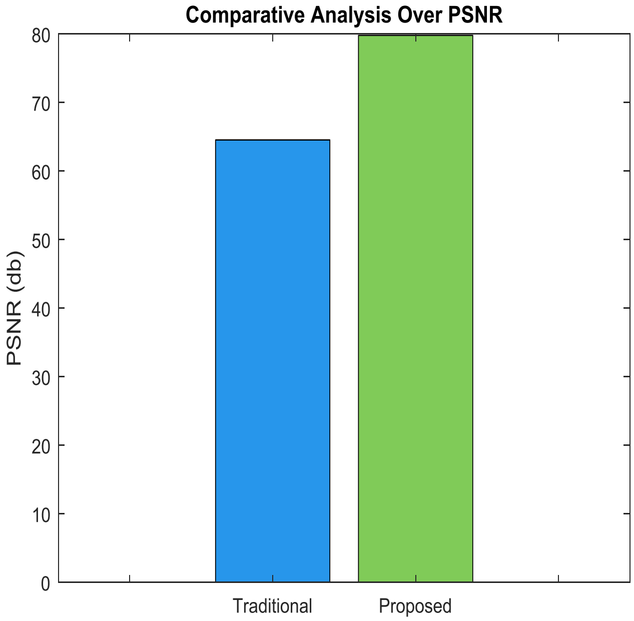

Figure 8 Comparative Analysis of PSNR of Pepper

2. Result of the proposed work among Complimented Binary stream of the secret message:

The comparison of PSNR of Fabric of the proposed and traditional work by using complimented binary stream of the message is shown in the Figure 9. In this graph it is shown that the PSNR of the proposed method is high by either using original binary stream or using complimented binary stream.

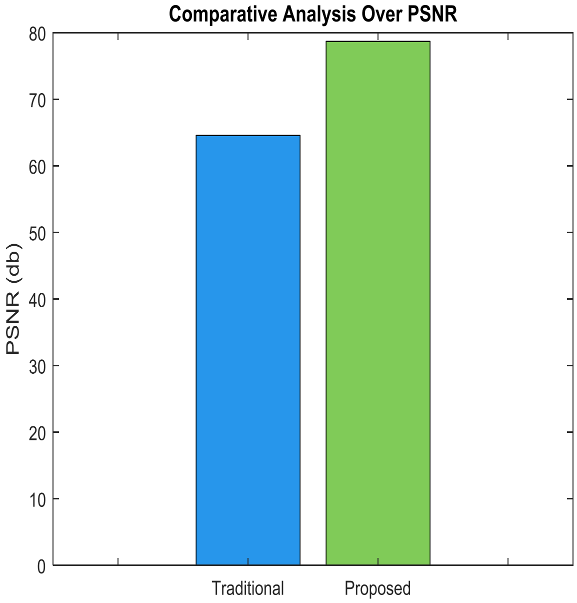

Figure 9 Comparative Analysis of PSNR of Fabric with Complimentary values

The graph of Figure 10 depicts the Comparative Analysis of PSNR of Onion with Complimentary values. The PSNR of the proposed work is high that is 79 whereas the PSNR of the conventional mechanism is 65.

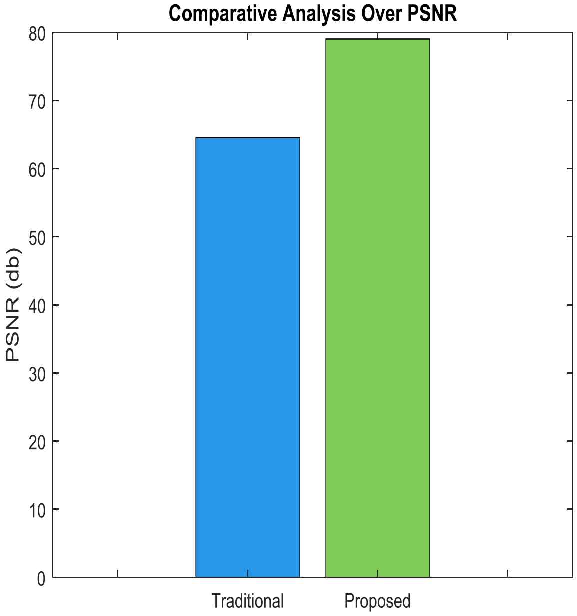

Figure 10 Comparative Analysis of PSNR of Onion with Complimentary values

The PSNR of Pears with Complimentary values is shown in the Figure 11 which represents the comparison of the existing method and the proposed work. The PSNR of the proposed work is high comparative to the existing method.

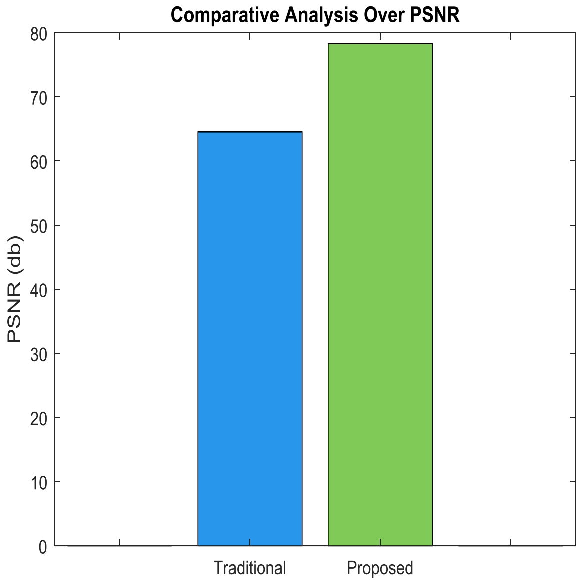

Figure 11 Comparative Analysis of PSNR of Pears with Complimentary values

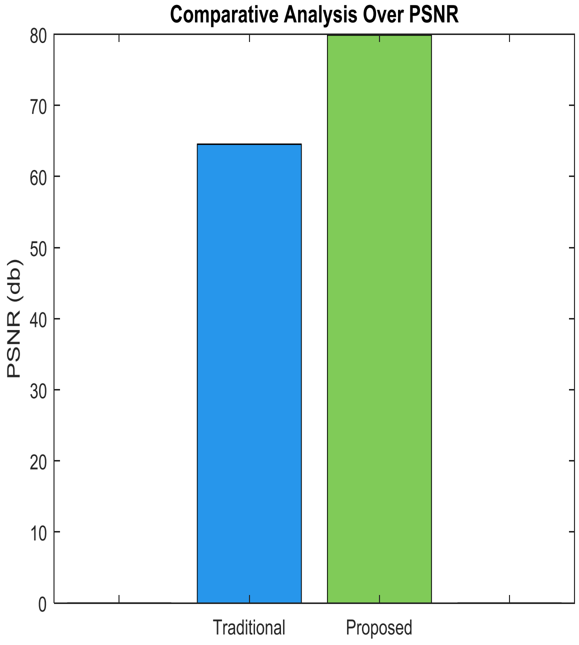

Figure 12 Comparative Analysis of PSNR of Pepper with Complimentary values

The graph of Figure 12 shows the Comparative Analysis of PSNR of Pepper of the proposed work with the conventional mechanism. In this graph it is shown that the PSNR of the proposed work is high.

The Table 1shows the PSNR values by using original binary stream and also by using complimentary values of binary stream of the secret message of the Proposed Work.

Table 1 PSNR of the Proposed Work

Image Name	Image size	PSNR (dB) by using Binary stream	PSNR (dB) by using Complimentary stream
Fabric	512*512	78.4305	78.6697
Onion	512*512	78.8418	79.0166
Pear	512*512	78.1406	78.3022
Pepper	512*512	79.7904	79.8803

VI. CONCLUSION

The steganography uses a cover image to hide the message, such that no intruder can ever detect any message being hidden in communicated image. The receiver extracts the message using a secret key provided by the sender to the particular and legal receptor of the message. Hence, the communication is established between the transmitter and the receiver secured of all possible threats from intrusion. In this paper the original binary converted data stream of secret message and the complemented version of the binary message have been embedded. The PSNR value is evaluated for these two mechanisms. A high PSNR is possessed by the acquired Stego image. Hence it is proved from the results that the PSNR of the proposed method in both the cases whether using original binary stream or using complimentary values is always high and better than the traditional method.

As the proposed work offers the better results but more amendments can be done by finding the optimum locations in the image to hide the data on those optimum locations in order that the quality will not be degraded.

REFERENCES

[1] Soni, A.; Jain, J.; Roshan, R., "Image Steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on , vol., no., pp.97,100, 1-2 March 2013.

[2] Masud Karim, S.M.; Rahman, M.S.; Hossain, M.I., "A new approach for LSB based image Steganography using secret key," Computer and Information Technology (ICCIT), 2011 14th International Conference on , vol., no., pp.286,291, 22-24 Dec. 2011.

[3] Shrutika Suri," Comparative Analysis of Steganography for Coloured Images", JCSE, vol 2(4), Pp 180-184, 2014

[4] Sabyasachi Pramanik," Image Steganography Using Wavelet Transform And Genetic Algorithm", IJIRAE, vol 1(1), Pp 17-20,2014

[5] Chin-Chen Chang," Meaningful Shadows for Image Secret Sharing with Steganography and Authentication Techniques", journal of information hiding and data processing, vol 5(3), Pp 342-352, 2014

[6] Komal Hirachandani, "New Approach of Information Security through Steganography by using Wavelet Transformation and Symmetric Encryption", IJCSIT, vol 5(5), Pp 6253-6260,

[7] Shemi P B," An Enhanced Image Steganography Technique in Art Images", IJCSMC, Vol.3 Issue.8, August- 2014, pg. 613-621

[8] Mohammad Sajid Khan, "Encryption Based Steganography-Modern Approach for Information Security", IJCSIT, Vol. 5 (3) , Pp 2914-2917, 2014

[9] Takashi Mihara," A New Framework of Steganography Using the Content of Cover Data", Journal of information hiding and multimedia signal processing, Vol 5(2), Pp 117-123, 2014

[10] Prof.Pramod Khandare," Data Hiding Technique Using Steganography", IJCSIT, Vol. 5 (2) , Pp 1785-1787, 2014

[11] Shikha Mohan," Image Steganography: Classification, Application and Algorithms", IJCEM, Vol 1(10), Pp 93-97, 2015

[12] M. Kameswara Rao, " Security Enhancement in Image Steganography a MATLAB Approach", Journal of scientific research, Vol 23(2), Pp 357-361, 2015

[13] Chaitali R. Gaidhani, " Image Steganography for Message Hiding Using Genetic", IJCSE, vol 2(3), Pp 67-70, 2014

[14] Mamta Juneja, "Improved LSB based Steganography Techniques for Color Images in Spatial Domain", IJNS, vol 16(6), Pp 452-462, 2014

[15] Bhattacharjee, T., Nov. 2014 "Progressive quality access through secret sharing and data hiding scheme"Pp 5-7,2014

[16] Preeti Parashar ,2014"A Survey: Digital Image Watermarking Techniques", ijsp, Vol. 7(6), pp. 111-124, 2014

[17] Monika Patel,Priti Srinivas Sajja," Analysis and Survey of Digital Watermarking Techniques", ijarcsse, Vol 3, Pp 203-210, 2013

[18] Sahar A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information", ELSEVIER, Pp 1-20, 2016

[19] Abhinav Shrivastav,"Survey report on Different Techniques of Image Encrption", IJETAE, vol 2, Issue 6, Pp 163-167, 2012

[20] Lauren Dubreuil,"Spread Spectrum, Cryptography and information Hiding",

[21] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography",IJARCSSE Volume 3, Issue 5, May 2013

[22] Anil Kumar (2013), "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, Pp 363-372

[23] Mehdi Hussain , A "Survey of Image Steganography Techniques", IJAST Vol. 54,Pp 113-124, 2013

[24] Dr. Mahesh Kumar,"Image Steganography using Frequency domain", IJST, vol 3, Issue 9, Pp 226-230, 2014

[25] Akanksha Kaushal,"Secured Image steganography using Different Transform Domain", IJCA, vol 77, Issue 2, Pp 24-38, 2013

[26] C.P.Sumathi, "A Study of Various Steganography Techniques Used for Information Hiding ",IJCSES) Vol.4, No.6, Issue 9,Pp 9-25, 2013

[27] Amritpal Singh,"An overview of Image Steganography Techniques", IJECS, vol 3, Issue 7, Pp 7341-7345, 2014

[28] Parmar Ajit Kumar Maganbha," A Study and literature Review on Image Steganography", IJCSIT, vol 6, Issue 1, Pp 686-688, 2015

Authors Profile

Ms. Kirti Chopra obtained her B.Tech. (Computer Engg.) Degree from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India in 2016. She is currently pursuing Master of Technology in Cyber Security at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India. Her current research interests include Image Steganography.

Mr. Ishpreet Singh Virk obtained his B.Tech (Computer Engg.) degree from Punjabi University, Patiala in 2009, M.Tech (CSE) from Punjabi University, Patiala in 2012 and pursuing Ph.D. degree from Punjabi University, Patiala in 2015. He is working as Assistant Professor in the Department of Computer Science and Engineering in Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab. He is the Lifetime Member of the International society for research and development and Member of ISCA. His research interests include Soft Computing and Digital Image Processing.