ISSN:2231-0711

Anju PS et al | IJCSET(www.ijcset.net) | January 2016 | Vol 6, Issue 1, 27-32

A Survey On Steganographic Methods Used in Information Hiding

Anju PS[#1], Bineeth Kuriakose[#2], Vince Paul[#3]

[#]*Student, Computer Science and Engineering, Calicut University,*
Sahrdaya College of Engineering and Technology
Kerala, India

[#] *Assistant Professor, Computer Science and Engineering,*
Calicut University, Sahrdaya College of Engineering and Technology
Kerala, India

Abstract— **Due to Exponential growth in the internet technology, there are large amounts of images are available on the internet. Nowadays transmission of data is a daily routine and protection of such transmitted data is a big problem. Protection can be done with encryption of data or by using data hiding algorithms. Hiding techniques can be used in the environment where steganographic techniques fail. There are many different protocols and embedding techniques allows us to hide data in a given image. In this paper we have analyzed various information hiding techniques.**

Keywords— **DCT, DWT, LSB, Information hiding.**

I. INTRODUCTION

With the rapid development of technology, securing transmission of data is challenging. Various methods are developed to protect data that are transmitted through the internet. Encryption is most probably used for data security, then comes the information hiding or steganography. Information hiding refers to communication of information by embedding it in and retrieving it from digital media. Depending on the application the embedding process need to be imperceptible, robust, secure etc. There are many different protocols and embedding techniques allows us to hide data in a given image. We can hide data in audio, video, still images, documents, software and even in the hardware designs. Mainly we use images but concepts and techniques can be generalized to other media. Steganography refers to hiding secret data into a cover object to protect it from unauthorized access, a technique of invisible communication which hides the existence of the message. If the cover object is used is an image, the steganography is known as image steganography. It has many applications like online transactions, military communication etc. Fig 1 shows basic steganography technique.

The word steganography in Greek means "Covered Writing". The information hiding process in a Steganography with different techniques includes identifying cover mediums redundant bits. The embedding process creates a stego medium by replacing the redundant bits with data from the hidden message. During the process of hiding the information three factors must be considered that are ***capacity*** it includes amount of information that can be hidden in the cover medium.

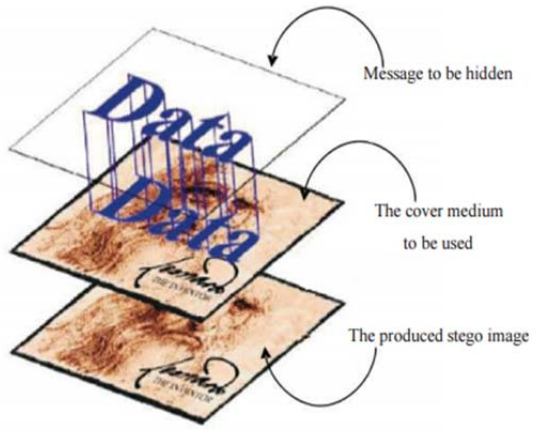

Figure 1. Basic Steganography

Security implies to detect hidden information and ***Robustness*** to the amount of modification the stego medium can withstand
before an adversary can destroy hidden information [1]. Main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer. Today steganography is mostly used on computer with digital data being the carriers and networks being the high speed delivery channel [2].

This paper is organized as follow. In section II, we describe survey of different Information hiding methods. In section III, we describe scope of research. In section IV, represents comparative analysis. In section V, represents conclusion and future work.

II. SURVEY OF DIFFERENT METHODS

There are several surveys that have already been done in this area of this knowledge. Some of the studies are discussed in this section.

In Mamta Juneja et. al's [3] research paper a secured robust approach of information security is proposed. It presents two component based LSB (Least Significant Bit)methods for embedding secret data in the LSB's of blue components and partial green components of random pixel locations in the edges of images. An adaptive LSB based steganography is proposed for embedding data based on data available in MSB's of red, green, and blue components of randomly

selected pixels across smooth areas. It is more robust as it is integrated with an Advanced Encryption Standard(AES).

In S.Shanmuga Priya et. al's [4] article the authors propose a novel method based on LSB. Data embedding is performed using a pair of pixels as a unit, where LSB of the first pixel carries one bit of information and a function to two pixel values carries another bit of information. The proposed method shows better performance in terms of distortion and resistance against existing steganalysis. Embedding is done in the sharper edge regions using a threshold. PSNR value is compared for adaptive and non-adaptive techniques of data hiding in gray scale & color images.

In Shweta Singhal et.al's [5] paper a new image steganography scheme is proposed in the spatial domain. In the technique, one byte of blue factor of pixels of an image have been replaced with secret bits of text data, which results in better image quality. A stego key is used for security purposes.

In M.B.Ould MEDENI et.al.'s article [6], the authors propose a novel method for hiding information within the spatial domain of the gray scale image. The Pixel Value Differencing (PVD) method segments the cover image into no overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. While embedding secret data, each pixel is split into two equal parts. The number of 1's in the most significant part is counted and the secret message is embedded in the least part according to the number of corresponding bits. The proposed method is based on four-pixel differencing and LSB substitution.

In Chin-Chen Chang et.al.'s paper [7] an adaptive method is proposed. Data is hidden based on codeword grouping. A set of code words generated using palette generation algorithm is employed in index-based images. A code word grouping based steganographic scheme for index encoding images is presented. The relationship of code words is explored to group different member sub-clusters. The size of the sub-cluster determines the hiding capacity. To enhance hiding capacity sub-clusters with larger members are grouped together & sub-clusters with smaller members are grouped together. In the embedding procedure the sub-cluster to which the closest searched codeword belongs is identified, and the original encoded codeword is modified to hide secret message. The number of sub-cluster members indicates how many bits of secret message can be embedded. A set of thresholds is used to determine members of sub-cluster. Therefore choosing an adequate threshold is important. To improve security the sequence of embedding pixels is reorganized using a pseudo random generator.

In Hemalatha.S et.al's [8] paper, the authors propose a method that uses two gray scale images of size 128 x 128 that are used as secret images and embedding is done in RGB and YCbCr domains. The quality of stego images are good in RGB domain by comparing the PSNR values. The authors have used Integer Wavelet Transform (IWT) to hide secret images in the color cover image. The authors have compared the PSNR values and image quality when embedding is done in the RGB and YCbCr domains.

In another article by Hemalatha .S et. al. [9] Integer Wavelet Transform (IWT) has been suggested to hide multiple secret images and keys in a color cover image which is more efficient. The cover image is represented in the YCbCr colour space. Two keys are obtained, encrypted and hidden in the cover image using IWT.

In Keith.L. Haynes's article [10] the author studies the use of image steganography to breach an organization's physical and cyber defences. The proposed method utilizes computer vision and machine learning techniques to produce messages that are undetectable and if intercepted cannot be decrypted without key compromise. To avoid detection DWT (Discrete Wavelet Transform) is used. The goal of a computer vision system is to allow machines to analyze an image and make a decision as to the content of that image. The computer vision can be categorized as Model-Based & Appearance Based which uses example images and machine learning techniques to identify significant areas or aspects of images that are important for discrimination of objects contained within the image. Machine learning is different from human knowledge / learning. A computer has to make decision of the presence of a face based on the numbers contained in a 2D matrix. The feature is identified by using Haar feature selection. The goal is to identify the set of features that best distinguishes between images in the different classes. In the proposed method the cover image does not contain a secret message, rather the classification of the image yields the hidden message. Since the proposed algorithm utilizes ordinary unmodified images, there are no inherent indicators of covert communication taking place.

In S.Arivazhagan et. al.'s work [11] the authors propose a method that works in the transform domain and attempts to extract the secret almost as same as the embedded one, maintaining minimal changes to cover image by using techniques like median maintenance, offset & quantization. A modified approach for embedding colour images within colour images is proposed and it overcomes the limitations in embedding. Arnold Transform is applied on the secret image to increase robustness. This transformed image is then split into the three colour planes R, G, B and are subjected to DWT individually, converted to bit stream and then concatenated to be embedded in the cover image which is also subjected to DWT.

In Anindya Sarkar et. al.'s paper [12] the authors propose a Matrix Embedding with Repeat Accumulate (ME-RA) based steganography in which the host coefficients are minimally perturbed such that the transmitted bits fall in a coset of a linear code, with the syndrome conveying the hidden bits. The hiding blocks are pseudo-randomly chosen. A powerful repeat accumulate code is used for error correction. The authors have compared QIM (Quantization Index Modulation) and ME-RA methods. The comparisons with a slight modification of the MERA (puncture and non-shrinkage) methods with different decoding methods are also tabulated. The authors highlight that the use of ME instead of QIM within the YASS (Yet another Steganographic Scheme) that provides improved steganalysis performance but software complexity is more.

In Prosanta Gope et. al.'s article [13], the authors introduce an enhanced JPEG steganography along with a suitable encryption methodology using a symmetric key cryptographic algorithm. The JPEG cover image is broken into 8 x 8 blocks of pixel. DCT is applied to each block and quantization is done and data is encrypted using a new encryption method which uses CRC checking.

In Po-Chyi et.al.'s article [14] the authors compare the advantage of embedding in JPEG 2000 images with the previous approach of embedding in JPEG images. Most of the steganographic methods are based on JPEG because as a block DCT codec JPEG lends itself a good candidate for information hiding due to its fixed block structure. JPEG 2000 which is an upcoming still image coding standard can be used to hide high volume data. If information is embedded in the output of tier-2 coding, i.e. the JPEG 200 packets, it can be guaranteed that all the embedded information will be received without error and in correct order. But, difficulty lies in the modification of packets for embedding, since the bit-streams are compactly compressed by the arithmetic coder. Careless modification would result in failure of expanding compressed image. In the embedding process the image is decomposed using wavelet transform. (Number of wavelet decomposing levels & image size should be related to the host image), Lazy Mode Coding (Magnitude Refinement pass is suitable for steganographic purposes) is used for embedding.

In Hideki Noda et.al.'s paper [15] the authors propose a method that is based on a seamless integration of JPEG2000 lossy compression scheme and bit-plane complexity segmentation (BPCS) steganography. In bit-plane decomposition an n bit image is decomposed into a set of n binary images by bit slicing operations, combined with replacing binary data in LSB bit planes with secret data. The BPCS steganography uses bit-plane decomposition and characteristics of human vision. In JPEG 2000, wavelet coefficients of an image are quantized into a bit-plane structure. Each bit plane of the cover image is segmented into small size 8x8 blocks and are classified into informative / noise like blocks, using a threshold of the complexity $\propto_0$ (e.g. value of $\propto_{0.03}$ $\propto_{max}$). $\propto_{max}$ is the possible complexity value. The secret file is segmented into a series of blocks containing 8 bytes of data that are regarded as 8x8 binary images. If secret block is less complex than the threshold $\propto_0$, conjugate (XOR) it to make more complex. ($\propto=\propto_{max}\propto$). The image will now be a conjugated image. Replace each noise like block in the bit planes with a block of secret data. If block is conjugated store it in the conjugation map. Blocks can be randomly selected by using a random-number generator. Also embed the conjugation map with secret data (usually the first noise like block). Secret data is embedded after tier-2 encoding.

Savita Goel et al. in [16] proposed a new method of embedding secret messages in cover image using LSB method using different progressions. Authors compare the quality of stego image with respect to cover image using number of image quality parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity (SSIM) index and Feature Similarity Index Measure (FSIM). Their study and experimental results shows that their proposed method is fast and highly efficient as compared to basic LSB methods.

Bingwen Feng, Wei Lu, and Wei Sun in their paper "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture" [17] purposed a state-of-the-art approach of binary image steganography. This technique is proposed to minimize the distortion on the texture. In this method of steganography firstly the rotation, complement and mirroring invariant texture patterns are extracted from the binary image. They also proposed a measurement and based on this proposed measurement this approach is practically implemented. Practical results show that proposed steganographic approach has high statistical security with high stego image quality and high embedding capacity.

Kazem Qazanfari and Reza Safabakhsh [18] proposed an improved version of LSB++ approach. In this improved LSB++ they make distinction between sensitive pixels and allow protecting them from embedding of extra bits, which results in lower distortion in the co occurrence matrices. They also extend this method to preserve DCT coefficients of JPEG format images. This improved method results in fewer traces in the co-occurrence matrices then old LSB++ technique. This method is also secure against histogram based attacks because this method does not make any changes in the histogram and hence histograms of both cover image as well as stego image will be same. The quality of stego images is also high because of elimination of extra bit embedding.

On the based on Huffman Coding, Amitava Nag et al. [19] present a novel steganographic technique of LSB substitution. Their technique basically focuses on high security, larger embedding capacity and acceptable level of stego image quality. Firstly Huffman tree is produced to encode every 8 bits of secret image. After encoding, they divide the encoded bits into four parts and have 0 to 3 decimal values. Location of embedding a message in cover image is determined by these decimal values. Experimental results show that it is very difficult for attacker to extract the secret information because Huffman table decrease the size of the cover image. Purposed techniques just have acceptable level of PSNR values and lie between 30 dB to 31 dB.

P. U. Deshmuk et al. [20] also present the edge adaptive steganography based on LSB substitution. They embed secret information in sharp (edges) regions of the carrier image using adaptive scheme and difference between two adjacent pixels of carrier image. Their technique performs well than other LSB and Pixel difference based techniques and maintains the quality of stego image.

E. Dagar and S. Dagar [21] present the steganography technique for color RGB images to improve the security level of data transfer through the internet. 24 bit RGB image is utilized as cover image to embed secret data in red, green and blue pixels. X-Box mapping is used and several boxes contain 16 different values. Here "X" represent any integer number from 0 to 9. After this values saved in X-Boxes are mapped with LSBs of carrier image. It is very difficult for the attacker to extract the secret information

because they make use of mapping. Thus this mapping provides high level of security to hidden information. PSNR value is also calculated and it has high PSNR value which leads to greater stego image quality.

M. R. Modi et al. [22] proposed a novel steganography technique to embed secret information of LSBs of cover image. In their method least two significant bits of edges are utilized to store secret message as edge regions are very good areas to embed the secret information than other smooth regions of cover image. In this method edge region are detected on basis of amount of secret information, which means it does adaptive edge detection. Experimental results analysis shows that their method performs better than traditional LSB image steganographic methods and has greater security against visual attacks.

Della Baby et al. [23] proposed a "Novel DWT based Image Securing method using Steganography". In their work new steganography technique is proposed in which multiple RGB images are embedded into single RGB image using DWT steganographic technique. The cover image is divided into 3 colors i.e. Red, Green and Blue color space. These three color spaces are utilized to hide secret information. Experimental results obtained using this system has good robustness. Value of PSNR and SSIM index have been used by authors to compare the quality of stego image and original cover image. Proposed method has good level of PSNR and SSIM index values. Authors have found that their experimental results are better than existing approaches and have increased embedding capacity because of data compression. So security is high with less perceptible changes in stego image.

M. Chaumont et al., in [24] have proposed a DCT based data hiding method. It hides the color information in a compress gray-level image. It follows the color quantization, color ordering and the data hiding steps to achieve image steganography. The purpose of method is to give free access to gray-level image to everyone but restricted access of same color images to those who have its stego-key. It has high PSNR plus with noticeable artifact of embedding data.

K. S. Babu et al., in [25] proposed hiding secret information in image steganography for authentication which is used to verify the integrity of the secret message from the stegoimage. The original hidden message is first transformed from spatial domain to discrete wavelet transform (DWT); the coefficients of DWT are then permuted with the verification code and then embedded in the special domain of the cover image. The verification code is also computed by special coefficient of the DWT. So this method can verify each row of the image of modified or tampered by any attacker.

In [26] proposed a reversible data hiding method on encrypted images by reserving room before encryption. Here the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. This method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

In [27] Xinpeng Zhang proposed a method for data hiding for encrypted images. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.

In [28] Xinpeng zhang also proposed another method for data hiding for encrypted images called "Separable Reversible Data Hiding in Encrypted Image". This work proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large.

Wavelet-based steganography [29], [30], [31], [32] and [33] is a new idea in the application of wavelets. However, the standard technique of storing in the least significant bits (LSB) of a pixel still applies. The only difference is that the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. The idea is that storing in the least important coefficients of each 4 x 4 Haar transformed block will not perceptually degrade the image. While this thought process is inherent in most steganographic techniques, the difference here is that by storing information in the wavelet coefficients, the change in the intensities in images will be imperceptible.

III. Comparative Study

Based on the way of embedding data into cover images, steganography can be divided into two types,

- Spatial domain
- Transform domain

Spatial domain technique embeds data directly into the intensity of pixels. Least significant bit replacement, difference expansion, histogram modification etc are some examples of this type. In the case of LSB method, secret data hides in the least significant bit of pixel. Based on the survey, we can observe that lsb based hiding gives high capacity and is simple to implement, but it has low robustness and pros to some attacks like low-pass filtering and compression.

In Transform domain, images are first transformed and then the message is embedded into it. These are robust methods for data hiding. It is more complex method to hide secret message into an image. Two-dimensional discrete cosine transformation (DCT) discrete Fourier transformation (DFT) and discrete wavelet transformation (DWT) that are commonly used transform domain methods in image steganography. DCT based method embeds data by changing the coefficient of transform of image. Studies show that it has high security and PSNR, but it has low embedding capacity. Discrete wavelet transforms (DWT), which transforms a discrete time signal to a discrete wavelet representation. It also has high capacity and high security, but the cost of computing dwt is higher.

IV. SUMMARY

In this paper, we have discussed various methods of steganography proposed by different researchers. And we have also discussed about major categories of steganography, and its pros and cons. Based on this survey we can conclude that all methods have advantages and drawbacks. Hiding methods can be chosen based on our requirements. Future work is to develop a steganography technique that has high capacity, highly robust to different steganographic attacks.

ACKNOWLEDGMENT

Thanking to Asst.Prof. Bineeth Kuriakose, Computer Science Department for his valuable knowledge and support and guiding me to the right path.

REFERENCES

[1] Hniels Provos & Peter Honeyman,"Hide & Seek : An Introduction to Steganography" IEEE Computer Society Pub-2003.

[2] Amitava Nag, Sushanta Biswas,"A Novel Techniques for image steganography based on DWT and Huffman Encoading", IJCSS, Vol(4):issue(6).

[3] Mamta Juneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol9, No:3, pp.405-424.

[4] S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain" , International Journal of Engineering Research and Applications Vol2, Issue 3, pp. 2632-2637.

[5] Shweta Singhal, Dr.Sachin Kumar and Manish Gupta, (2011) "A New Steganography Technique Based on Amendment in Blue Factor" , International Journal of Electronics Communication and Computer Engineering, Vol.2, Issue 1, pp.52-56.

[6] M.B.Ould MEDENI and El Mamoun SOUIDI, (2010) "A Generalization of the PVD Steganographic Method", International Journal of Computer Science and Information Security, Vol.8.No.8, pp156- 159

[7] Chin Chen Chang, Piyu Tsai & Min-Hui Lin (2004) "An Adaptive Steganography for Index-Based Images using Codeword Grouping", Springer-Verlag Berlin Heidelberg 2004, pp.731- 738.

[8] Hemalatha.S, U.Dinesh Acharya and Renuka.A, (2013) "Comparison of Secure and High CapacityColor Image Steganography Techniques in RGB and YCBCR domains" , International Journal of Advanced Information Technology, Vol.3, No.3, pp.1-9.

[9] Hemalatha.S, U.Dinesh Acharya and Renuka.A, Priya.R Kamnath, (2013) "A Secure and High Capacity Image Steganography Technique", Signal & Image Processing , An International Journal, Vol.4, No.1, pp.83-89.

[10] Keith L.Haynes, (2011) "Using Image Steganography to Establish Covert Communication Channels", International Journal of Computer Science and Information Security, Vol 9, No.9, pp. 1-7.

[11] S.Arivazhagan, W.Sylvia Lilly Jebarani, and S.Bagavath (2011) "Colour Image Steganography Using Median Maintenance" , ICTACT Journal on Image and Video Processing, Vol. 2, Iss:01, pp.246-253.

[12] Anindya Sarkar, Member, IEEE, Upamanyu Madhow, Fellow,IEEE, and B.S.Manjunath, Fellow, IEEE, (2010) "Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography" , IEEE Transactions on Information Forensics and Security, Vol.5.No.2, pp.225-239.

[13] Prosanta Gope, Anil Kumar and Gaurav Luthra , (2010) "An Enhanced JPEG Steganography Schemewith Encryption Technique" , International Journal of Computer and Electrical Engineering ,Vol.2.No.5, pp924-930.

[14] Po-Chyi & C.-C.Jay Kuo, Fellow, IEEE(2003) "Steganography in JPEG 2000 Compressed Images", IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp 824-832.

[15] Hideki Noda, Jeremiah Spaulding, Mahdad.NShirazi & Eiji Kawaguchi (2002) "Application of Bit-Plane Decomposition Steganography to JPEG 2000 Encoded Images" .

[16] S. Goel, S. Gupta, and N. Kaushik, "Image Steganography Least Significant Bit with Multiple Progressions" , Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), vol. 2, Springer (2014).

[17] B. Feng, W. Lu, and W. Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE transactions on Information Forensics and Security, vol. 10, no. 2, (2015).

[18] K. Qazanfari and R. Safabakhsh, "A new Steganography Method which Preserves Histogram: Generalization of LSB++", Elsevier International Journal of Information Sciences, vol. 277, (2014).

[19] A. Nag, J.P. Singh, S. Biswas, D. Sarkar, and P. P. Sarkar, "A Huffman Code Based Image Steganography Technique" , 1st International Conference on Applied Algorithm (ICAA), (2014) January 13-15, Kolkata, India.

[20] P. U. Deshmukh and T. M. Pattewar, "A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique", IEEE International Conference on Information Communication and Embedded Systems (ICICES), (2014) February 27-28, Chennai, India.

[21] E. Dagar and S. Dagar, "LSB based Image Steganography using X-Box Mapping" , IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), (2014), September 24-27, New Delhi, India.

[22] M. R. Modi, S. Islam and P. Gupta, "Edge Based Steganography on Colored Images" , 9th International Conference on Intelligent Computing (ICIC), (2013) July 28-31, Nanning, China

[23] . Baby, J. Thomas, G. Augustine, E. George, and N.R. Michael, "A Novel DWT based Image Securing method using Steganography" , International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science, vol. 46, (2015).

[24] M. Chaumont and W. Puech, "DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image" , 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, (2006) September 4-8.

[25] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L.M. Pataki, "Authentication of secret information in image steganography" , IEEE Region 10 Conference, TENCON-2008, (2008) November, pp. 1-6.

[26] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li," Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, MARCH 2013.

[27] Xinpeng Zhang," Reversible Data Hiding in Encrypted Image" , IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011 255

[28] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012

[29] Ali Al-Ataby and Fawzi Al-Naima. "A modified high capacity image steganography technique based on wavelet transform". The International Arab Journal of Information Technology, 7:358_364, 2010.

[30] Bo Yang and Beixing Deng. "Steganography in gray images using wavelet". In Proceedings of ISCCSP 2006.

[31] Po-Yueh Chen and Hung-Ju Lin."A dwt based approach for image steganography". International Journal of Applied Science and Engineering, 4:275_290, 2006.

[32] Dr.S.T.Gandhe K.T.Talele and Dr.A.G.Keskar. "Steganography security for copyright protection of digital images using dwt". (IJCNS) International Journal of Computer and Network Security, 2:21_26, 2010.

[33] H S Manjunatha Reddy and K B Raja. High capacity and security steganography using discrete wavelet transform". International Journal of Computer Science and Security(IJCSS), 3:462_472.