# Chapter 2

## LITERATURE SURVEY

### Table of contents

<table>
<thead>
<tr>
<th>Particulars</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Introduction</td>
<td>23</td>
</tr>
<tr>
<td>2.2 Multiplication based Steganography using wavelet transformation</td>
<td>23</td>
</tr>
<tr>
<td>2.3 Secure Steganography with Scrambled Payload using Lifting Wavelet Transform</td>
<td>25</td>
</tr>
<tr>
<td>2.4 Adaptive Steganography using LWT</td>
<td>29</td>
</tr>
<tr>
<td>2.5 Hybrid domain based Steganography using BPS, LSB and IWT</td>
<td>33</td>
</tr>
</tbody>
</table>
2.1 Introduction

In this chapter a review of existing techniques of Steganography are presented. It includes a review of Wavelet based Non LSB Steganography, Secure Steganography with scrambled payload using LWT, Adaptive Steganography using Lifting Wavelet Transforms and Hybrid domain based Steganography using BPS, LSB and IWT Techniques.

2.2 Multiplication based Steganography using Wavelet Transformation

Hongmei Tang et al., [18] proposed a Combination of Encrypted image and Steganography method. The secret data is encrypted using the combination of gray value replacement and position permutation and then encrypted secret information is concealed in the cover image to fulfill steganography. Solanki et al., [19] have proposed embedding method to avoid statistical Steganalysis by hiding at high rates and also attain robustness against attacks. The secret key mutual between the encoder and the decoder determines the embedding and compensation locations. The certain percentage of host secret code is set aside for re-establishment, while the remaining are considered for embedding. The data hiding using Quantization Index Modulation (QIM) is applied for statistical restoration, which permits the embedding of huge volumes of information.

Hang ling Zhang et al., [20] proposed image based steganography using differencing the pixel value to enhance the payload capacity and to provide a stego image unnoticeable for human visualization. The
number of message bits to be embedded is estimated depending on pixel difference values between neighboring pixels. Ravuru Rakesh et al., [21] Proposed a five different randomization methodologies by adapting an embedding the data into the bits of Least Significant Nibble (LSN) pertaining to bits in Most Significant Nibble (MSN). The methodologies are (i) Embedding the data in the LSN’s according to the ranked order of MSN, (ii) uses the reversible property of XOR to implement keyless random approach. Here each 4 bits of data are XORED with MSN and then substituted in LSN, (iii) Employing random embedding lengths in each pixel. The number of information bits to be implanted in LSN is varied according to data bits in MSN, (iv) The data is embedded into LSN based on parity of MSN i.e., the number of one’s /zeros even or odd and (v) Embedding data in the LSN bits based on the MSN bits of one or zero.

Dipti Kapoor Sarmah and Neha Bajpai [22] have developed a security module by combining both Cryptography and Steganography. The Cryptography uses advanced encryption standard algorithm to encrypt a message and a part of the message is hidden in transformed coefficients of an image and remaining part of the message is used to generate a secret keys. Manjunath Gadiparthi et al., [23] have proposed a combination of Pixel Value Differencing (PVD) modulus and Least Significant Bit (LSB) method. If the PVD is 3 and the corresponding range width is 8, only 3 bits can be embedded in a pair of pixels. Where as in 3-bits LSB replacement method, the 6- bits can be embedded. The proposed LSB method is applied for smooth areas,
where as PVD modulus method is used for edge area pixel pairs based on a threshold to determine whether a pixel pair falls in smooth area or edge area. Mamta Juneja and Parvinder Singh Sandhu [24] have discussed the design of a robust steganography method using LSB addition and Rivest, Shamir, and Adelman (RSA) encryption technique and used to encrypt the secret data. The encrypted data is manipulated into a bit stream and then decomposed into number of segments. However, the cover image will also be decomposed into the same number of segments. The each segment of information data will be compared with each segment of image to find the best match segment, to obtain a new random sequence of segments to be inserted into a cover image.

Shiva Kumar et al., [25] proposed Cover image modulation approach to Steganography. The cover image is decomposed into $2\times2$ matrices and the nearby pixel intensity differences are calculated to get the threshold and same will be consider for payload embedding. The transformation matrix $H_T$ is generated based on the payload bit pair and identity matrix. The secret information is retrieve from the stego image at the destination using key obtained with first bit of secret bit pair at the sending ends.

### 2.3 Secure Steganography with Scrambled payload using Lifting Wavelet Transform

Yuan Hui Yu et al., [26] presented a Steganography technique for embedding a color or a grayscale image in a exact color image. There are three methods of hiding secrete information viz., (i) hiding a color
secret information in a true color image, (ii) hiding a palette based 256 color secret information in a true color image, and (iii) hiding a grayscale information in a true color image. The secret data are encrypted before embedding using Data Encryption Standard (DES) algorithm into the host image and at the destination the stego image is decrypted by the DES algorithm. Weiqi et al., [27] presented an edge adaptive technique to choose the embedding regions based on the size of payload information and the variation between two successive pixels in the cover image. For low embedding rates, the sharper edge regions are considered while keeping remaining smoother regions as they are. More number of edge regions can be used adaptively for data hiding in order to increase the embedding rate by adjusting few parameters.

Der Chyuan lou et al., [28] have developed a scheme of Adaptive Steganography to prevent visual degradation and also providing a higher capacity. The size of the embedding of each pixel is determined by the local complexity of the cover to maintain good image quality and larger payload embedding. The pixels are divided into three different levels depends on the difference of the local complexity of the cover image. The human vision sensitivity is considered for determining position of local complexity to a particular pixel should belong to it. Amitava Nag et al., [29] proposed Image steganography based technique using DWT. The DWT and Huffman coding is applied on cover image and secret message respectively before embedding. The Huffman code based secret information is embedded in the high
frequency coefficients obtained from transformation. The quality of the image is to be enhanced by storing the wavelet coefficients in the low frequency subband.

Souvik Bhattacharya and Gautam Sanyal, [30] developed a Pixel Mapping Method (PMM) for hiding payload message in the transform domain coefficients. The haar lifted wavelet is used on the cover image to derive subbands such as Approximation band Coefficient (CA) and detail bands are CH, CV and CD. The two bits of the secret message are mapped in the pixels of the cover image. Mohammad Ali et al., [31] developed a method of sending the secret information with encrypted image arbitrarily depending on secret key before transmission to the receiver to rebuild the transformed image and then recover the original payload. The placing positions of this information will be randomly selected. The number of horizontal and vertical blocks at the sender’s side will be obtained and then mixed with the encrypted image before transfer to the receiver. The receiver require this information to rebuilt the same secret transformation table after retrieving the secret information from the encrypted image.

Sos S. Again et al., [32] proposed an algorithm to achieve secure communication with high capacity. The secure communication of information is achieved by embedding the information bits in the noisy regions of the image so that the alter in the cover image are unnoticed. The segmentation of image into 8 - bit planes and higher number of bit planes are obtained using the concept of Fibonacci to
accumulate more information to enhance the capacity. Thanikaiselvan et al., [33] developed an embedding technique to enhance the embedding capacity, and security. The IWT is applied on cover image to generate wavelet coefficients and embedding is performed by using two keys. The first key is used to decide the coefficient in which embedding is to be performed and the second key is used to determine the number of bits of secret message to be embedded in the cover image.

Wai Wai Zin and Than Naing Soe, [34] proposed a technique for data secrecy, data verification and data reliability. The data is encrypted with Rivest Cipher 4 (RC4) encryption technique and embedding is done by using 3 - LSB replacement method. Ali Danesh Khan et al., [35] developed a technique of hiding payload in spatial domain in which two bits of pixels are permitted to modify, and also second and fourth bit planes are permitted to modify, but at one modification in one bit plane is allowed at a time. Adel Almohammad and Gheorghate Ghinea [36] have investigated the relationship between the Peak Signal to Noise Ratio (PSNR) and the quality of stego images. The PSNR is commonly used to estimate the stego image quality. However, evaluation is the most consistent method to measure the image quality. Therefore, this paper scrutinize the relationship, if there any, between the PSNR and the subjective quality of stego images. Yuh Ming Huang and Pei Wun Jhan [37] developed two different data hiding methods, one is based on Exploiting Modification Direction (EMD) data hiding algorithm and other is based on enhancement of
matrix encoding using Hamming coding to enhance the quality of stego image. Feng Pan et al., [38] developed a method of reducing embedding rate using Trellis Codes. A distortion factor is used for reducing impact for embedding in DWT.

### 2.4 Adaptive Steganography using LWT

Yicong Zhou and Agaian [39] introduced an encryption algorithm called Parameterized Logarithmic Image Processing (PLIP) addition. The secret information is scrambled to alter the image pixel locations. The scrambled payload message is embedded into the cover image using PLIP addition via specific parameters. Adel Almohammad and Chinea [40] proposed steganography methods such as JSteg and JM QT are used to investigate the pros and cons of colour and grayscale conversion of images when used as covers. It estimates the performance of grayscale and colour images used with a given steganography technique. The colour images are better than using grayscale images for hiding the data.

Ghasemi et al., [41] presented an embedding algorithm using mapping function based on genetic algorithm. The cover image is decomposed into 8 x 8 cells and transformed using Integer Wavelet Transform (IWT). The payload is embedded into transformed coefficients of cover image. The Genetic algorithm and optimal pixel adjustment provides optimal mapping function which reduces the error between the cover and stego image in order to enhance the hiding capacity with low distortion.
Yong Hong Zhang [42] implemented a digital image encryption using chaotic cryptography. The chaotic cryptography technique is used as a key cryptography. The extended chaotic sequences are obtained using-rank rational Bézier curve. The generated chaos random sequence used to encrypt the image, which is an secured way to deal with the intractable problem of highly secure image encryption. The pseudo random sequence is generated by using chaos sequencer that makes double time encryptions with enhancement of DES algorithm. 

Swain and Lenka [43] presented secure communication method by combining cryptography and image steganography. The confidential information is encrypted and embedded in sixth, seventh and eighth LSB location of darkest and brightest pixel which is randomly spread across. Weiming Zhang et al., [44] developed a binary stego codes for LSB embedding in gray-scale images, which can be obtained by the combination Hamming codes and wet paper codes.

Gopalan [45] implemented a technique of embedding data into color image for applications such as validation of an employee carrying a photo identification card. The color image is converted into red, green or blue signal. The audibly covered frequencies in one dimensional signal are determined for each segment. The confidential information is embedded by altering the spectral power at a pair of commonly occurring covered frequencies. Cui ling Jiang et al., [46] presented a steganographic technique which is based on alteration of JPEG quantization tables. The cover image is segmented into non overlapping 16 x 16 quantization table. The DCT transformed
coefficients are quantized using quantization table. The secret data is embedded into DCT coefficients of cover image.

Yan-ping Zhang et al., [47] developed a technique for information hiding into still images which is based on (n, k) Hamming Code and Wet Paper Codes. At a time seven secret bits are embedded into a pixel group of several cover pixels, if that is unsuccessful then it embeds the first three secret bits into same pixel-group. Chen Gouxi et al., [48] developed a scheme in which the cover image is marginalized and reconstructed by using mathematical morphology equations and block markers, then embedding the secret information into the cover image successfully with F5 steganographic system. The technique has benefits such as the small alters in image quality, high ability in anti attack, and the secret message can be retrieved completely from the payload image.

Cachin [49] has developed Information theory based steganography technique by interpreting the adversary’s task of differentiating between cover image and stego image as hypothesis testing problem. The entropy is used to measure the security stego image. The stego does not needs the knowledge of cover text distribution. Marghny Mohamed et al., [50] have proposed a genetic algorithm used to solve the problem of hiding data in the rightmost k-LSBs of the cover image when k is larger. However, it works inefficiently if k is greater than 3 then the number of possible keys permutations will increase exponentially as k increases. Tanmay Bhattacharya et al., [51] have
proposed DWT based Steganographic technique. The DWT is used on cover image to obtain four subbands LL, LH, HL and HH. The secret information is embedded within the HL and HH subbands. The secret images which are embedding are scattered within each subband using a pseudo random sequence and session key. The secret information is retrieved using the key and image size.

Rajkumar Yadav et al., [52] have developed a technique of data hiding using gray scale images in spatial domain. This technique uses 5th, 6th and 7th bits of pixel value and if decimal value of 5th, 6th and 7th bits are even then insert 0 at these locations and if not then add or subtract 1 at that location to make decimal value of 5th, 6th and 7th bits are even for insertion of 0. Similarly, insert 1 at a pixel location if decimal value of 5th, 6th and 7th bit at that location is odd. If decimal value of 5th, 6th and 7th bit at that location is not odd then add or subtract 1 at that location to make decimal value of 5th, 6th and 7th bits are odd for insertion of 1. For retrieval of message, again check decimal value of 5th, 6th and 7th bit. If the decimal value of 5th, 6th and 7th bit at the selected location is even then 0 is the message bit else message bit is 1. Wien Hong and Tung Shou Chen [53] proposed a data hiding technique using Pixel Pair Matching (PPM). In PPM uses the values of pixel pair as a reference coordinate, and find a coordinate in the surrounding set of this pixel pair based on the given information digit. Then pixel pair is replaced by the searched coordinate to hide the secrete digits.
2.5 Hybrid domain based Steganography using BPS, LSB and IWT

Eiji Kawaguchi and Richard Eason [54] have proposed Bit Plane Complexity Segmentation (BPCS) Steganography, which is based on human visual system. The important key for this technique is the information in the bit planes of an image is invisible. The bit planes of a image are divided as informative and noisy areas by using complexity threshold. The complex regions are replaced with secret message in the bit planes of a image without altering the image quality. Sarreshtedari and Ghaemmaghami,[55] have proposed high embedding capacity steganography in wavelet domain. The secret information is embedded into transformed coefficients of the cover image. This technique provides a higher capacity for data hiding without compromising the quality of the cover image. This is performed by retaining reliability of wavelet coefficients at high capacity embedding. Kumar V and Kumar D [56] have proposed Performance evaluation of Image Steganography using DWT. The wavelet coefficients of the cover image are altered to embed the payload information and view the effect of embedding the payload message in various bands such as CH, CV and CD of the stego image in terms of PSNR.

Shrikant S Khaire and Sanjay L Nalbalwar [57] have proposed Steganography with Bit Plane Complexity Segmentation (BPCS) technique in which the binary image is segmented into informative and noisy region. The payload information is hidden into noisy region
of the vessel image without any deterioration. Madhu Viswanatham and Jeswanth Manikonda [58] presented secure Steganography technique of LSB replacement. This technique generates random numbers and also selecting the region of interest in the cover image wherein the necessary information embedded along with the random pixels which are previously generated. The secret key is used at the destination provided by the recipient for decoding the information from the stego image. Rohini Sharma and Ekta Walia [59] have proposed a non adaptive and adaptive edge based LSB replacement for color images. These algorithms can be altered for color images and compared with the various performance parameters such as PSNR and MSE. Rupinder Kaur et al., [60] have proposed efficient approach towards Steganography. The image can be used as a shared key between sender and the receiver and image is not transmitted over the channel. The indefinite size image can be used as a key. The every character in the text is transformed into integer value and the integer value is mapped into the single pixel value of the image. The information about the index arrays are required to recover the message from the image. The image quality does not change because there is no change in any pixel value of the image.

Joyshree Nath and Sankar Das [61] have proposed steganographic technique for hiding encrypted secret information in LSB, LSB+1, LSB+2 and LSB+3 bits in cover files. The secret message is encrypted and hidden in cover files such as .exe, .com, .pdf, .doc, .xls, .ppt files using LSB replacement method. The size of secret information must
be small as compared to the cover file. Lifang Yu et al., [62] have proposed adaptive LSB steganography which is based on chaos and genetic algorithm. This method achieves higher capacity while preserving statistics and to reducing visual degradation of the stego image. The shuffle bit order of the information based on chaos and parameters are selected by using genetic algorithm. Sanjive Tyagi and Ajay Agarwal [63] have proposed multi layers security system for embedding payload in a cover image, in which the image segmentation is used to decompose cover image into two regions, i.e., foreground and background regions. Then hide encrypted text into surroundings region of cover image by using LSB replacement technique. Souvik Bhattacharya and Aparajit khan [64] have proposed Pixel Mapping Method (PMM) based Bit Plane Complexity Segmentation (BPCS) steganography. The mathematical functions are used for selecting the embedding bit planes and then use PMM in 8×8 blocks of each selected planes. The combination of PMM and BPCS produces a robust steganography technique which is independent of the information to hidden and obtain a stego image.

Anita Christaline and Vaishali [65] have proposed steganographic method with improved embedding capacity and robustness. The method uses two steganographic techniques, one is the filter method and the other one is wavelet transform method. The filter method used to embed the information into cover image and DWT is used to increase the security. Ramani et al., [66] have developed BPCS based steganography using IWT in which the data hiding is performed in bit
planes of subband wavelets coefficients. Yogendra Kumar Jain and Ahirwal [67] have proposed adaptive number of LSB replacement method with private stego key. The method embeds binary bit stream in 24 bits color image or in 8 bits gray-scale image. The method embeds the concealed information in the spatial domain of the cover image and uses ExOR operation based on digital signature using 140 bit key to check the reliability of the stego image. The embedded secret data can be retrieved from stego images without the help of original image.

Souvik Bhattacharyya et al., [68] developed a steganography method for transporting data between two areas. The secret message has been permuted, coded using integer wavelet transformation with lifting scheme and divided in different parts and finally each part is embedded through altered LSB embedding technique on different objects of the cover image to form various stego objects. Finally the stego image is formed by combining different stego objects and transmits to the receiver side. El Safy R O et al., [69] proposed a method to optimized high hiding capacity and imperceptibility. The data hiding in digital images are performed by using adaptive hiding capacity function that hides secret data in the wavelet coefficients of the cover image using Optimum Pixel Adjustment (OPA) algorithm. The coefficients are selected based on pseudorandom function generator to increase the security of the concealed data.

Sathisha et al., [70] proposed Spatial Domain Steganography technique using 1-Bit MSB with chaotic manner. The cover image is
divided into 8*8 matrix of equal size. The first block of cover image is embedded with 8 bits of upper bound and lower bound values required for retrieving payload at the destination. The mean of median values and difference between successive pixels is determined to embed payload in 3-bits of Least Significant Bit (LSB) and one bit of MSB in chaotic manner. Shiva Kumar et al., [71] proposed a technique of integrating both spatial and transform domains. The cover and payload image are segmented into two cells of each. The RGB components of cover image cell 1 are segregated and transformed individually from spatial to transform domain using DCT/DWT/FFT and then embedded into cover image. The cover image cell 2 is retained in spatial domain itself.

Kumar and Muttoo [72] proposed Steganographic algorithm based on the modified LSB method in four different wavelet transform domains. The data hiding is based on the characteristics of the Complex Wavelet Transform that provides shift invariance and offers better directional selectivity. The original information is converted into binary cell array with the help of synchronizing variable length codes, before the embedding process. The variable length code does not only compress the message but also provides synchronization at decoding end. The payload is embedded in the insensitive high subbands obtained from the cover image after applying transforms. Hu-Yu Huang and Shih-Hsu Chang [73] developed a lossless data hiding scheme using quantized transformed coefficients to embed secret information. The secret information is embedded into the succeeding
zero coefficients of the medium high frequency components in each reconstructed block for 3-level 2-D DWT of a cover medium.