CHAPTER 2
Literature Survey

2.1 Introduction

During the last few years, different Steganographic methods have been proposed. The most popular one is substitution systems which is a spatial domain technique. The exchange and gathering of information has become a central component of private and economic activities. Information is filed in documents and is transmitted by communication. If confidential information gets into the wrong hands, immense damage could be done.

Today, the protection against misuse, manipulation and eavesdropping is already considered the basic challenge of this era. There are different techniques to protect the information. The 3 main techniques are Cryptography, Watermarking and Steganography. The main goal of all these information is to hold the secret data. However, there are various differences between them. These are further discussed to establish the differences between them. Undetectability, robustness against attacks and capacity of the hidden data are the primary features of steganography which make it better than the other hiding techniques such s cryptography and watermarking.

It is one of the most popular types of steganography as an image which is the cover medium is widely used on the internet. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye. However, the image steganography techniques will exploit "holes" in the Human Visual System (HVS).

2.2 Techniques

Analog Steganography was present from the ancient world. For example writing the secret message on a table and applying wax on it so that the message is hidden. Upon removing wax the message is revealed [1]. In this digital era digital Steganography is using almost every possible carrier like text, image, audio and video etc. In image Steganography, image is used as the carrier. The earlier image Steganographic method
was simple LSB substitution, in which the LSB of each pixel is replaced by the message bit. Later on the Transform domain methods are evolved to improve the robustness. In Transform domain methods to obtain the coefficients transformation of image is done from time to frequency domain.

In Spatial domain method the simple LSB substitution method is improved to make it more secure. Cryptography is used along with Steganography to enhance the safety [7] [9]. Also Randomization techniques employed to embed the information bit randomly which makes it difficult to extract the information [9] [10]. Different randomization techniques are used such as Pseudo-Random Number Generator [PRNG] to randomly distribute the information bits in the image, Most Significant Nibble [MSN] method in which MSN of the pixels are used to select the order of pixels in which the information bits are embedded and using the pixel position and pixel intensity to embed the data into the pixels of image [8].

Then the neighborhood pixel information is used to embed the data. The four and eight neighbor methods are used to detect the sharper regions of the image where the message bits are embedded and other smoother regions are left as it is. Hence neighborhood pixel values are used to take the embedding decisions [12]. Edge detection method is improved version of neighborhood pixel value method. In this method the image edges are detected and more number of message bits is embedded onto edge pixels [15]. This is for the reason because the image edge region corresponds to the sharper regions of the image and changes in these regions are imperceptible to human eyes. Edge detection is done by different method like using Sobel operator which compares the gradient value of the pixel with a threshold value to detect edge pixels or using zero cross detectors which checks if the Laplacians passes through zero since the region where it passes through the zero has a very high chance of being an edge. These methods are equally applicable to gray-scale and color images.

Along with the development in the image Steganographic methods some work is done to embed other language characters other than English. In these efforts the other
language characters are represented by numerical value obtained by encoding the characters [18]. These numerical values are then converted to bit stream and embedded into the image pixels.

2.3 State of The Art Study

Nagham Hamid et al [1] have given nomenclature of the modern image Steganographic techniques. They also have reviewed image Steganographic methods. Most of their approach is with respect to image file format. They have validated all the approaches to the basic requirement of steganography.

Yedla Dinesh et al [2] proposed an image Steganography method in transform domain. They first transform both the original image and the secret message by employing Haar transform and Daubechies transform. This helps in effective retrieval of the secret message as the transform coefficients are required to recover the original values of pixels after they are averaged. Then they identify the capacity of each 8x8 block by splitting the original image into bit planes. Then depending on the block capacity the already transformed secret message is embedded and also a secret key is maintained to identify the blocks in which the data is embedded into. In the extraction process the Stego image is transformed again and using the key the message is extracted.

Prof. Akhil Khare et al [3] have presented software that allows even a common man with just basic computer knowledge to hide the secret data in an image and transmit it. To improve security they have employed both Steganography and cryptography. The transform domain coefficients are obtained by applying DCT, then encryption is applied here i.e. not all coefficients are used for embedding but only some sub coefficients are used. These sub coefficients are only known to the sender and receiver. Since no keys are used here, the decoder tries to find the positions the data is embedded on its own hence this leads to 2 types of errors, insertion error(decoder assumes that data is embedded in that coefficient even if it isn't) and deletion loss(decoder assumes the data is not embedded in that coefficient even if its embedded). They overcame these errors by treating insertions as errors and deletion as erasures. The sub coefficients are selected based on two methods, one is considering their entropy or energy and the second one is
considering the magnitudes of the coefficients. This method can be used to avoid distortion loss of data due to wavelet compression, image resizing.

Elham Ghasemi et al [4] their proposal integrated the use of Wavelet transform and Genetic algorithm to produce an effective image Steganography method. As usual they apply discrete wavelet transform to embed the data. After embedding they make use of genetic algorithm and optimal pixel adjustment method to reduce the difference between the original and Stego image as much as possible. They make use of Haar transform and of 4x4 masks for the embedding. In genetic algorithm they gone on increasing the data hidden in each pixel from 3-8 bit which depends on the visual quality of the image required.

Yue Wu and Joseph P. Noonan [5] have proposed the use of Wavelet transform, chaos mapping and fractal images to produce better results than the existing image Steganographic methods. Here wavelet transform is used to obtain a better representation of the signal, i.e. time-frequency representation instead of a normal frequency only representation like in other transforms. The use of chaos greatly increases the randomness, hence increases security. The chaotic mapping employed here is one dimensional logistic map which is deterministic. Finally fractal images are images which have similar segments which might be of different scales. The use of fractal images facilitates restoration.

Souvik Bhattacharyya and Gautam Sanyal [6] came up with a new transfer domain image Steganographic method in their paper. They have modified Bhattacharyya and Sanyal’s Transformation (PMM- pixel mapping method) where one seed pixel with 8 neighbors was selected. Here in a group of 8x8 DWT coefficients 4 seed pixels are selected with each having 8 (3x3 group) neighbors each. Then depending on the difference between a pair of neighbors in a 3x3 seed pixel block embedding is performed. Then inverse DWT is applied to obtain the Stego image.

Lokesh Kumar [7] has proposed the use of both Steganography and cryptography to greatly enhance the data security. The secret message is first encrypted by subjecting it to AES (Advanced Encryption Standard). AES is selected over DES (Data Encryption Standard) since it doesn't require a Feistal network and also the cipher key produced by it occupies the same space as a text message. This encrypted data is then embedded into the
cover using Alteration Component Technique. The secret data in extracted by reverse process with the help of Stego key.

Ravi Saini and Rajkumar Yadav [8], has made use of both the pixel position and the pixel intensity to determine the bit to be embedded. They employ use of logical AND between the binary value of the pixel intensity and the binary value of the pixel position. If the result is one, then bit 1 is embedded or else minor changes to the pixel intensity are made so that the result becomes 1. It is similarly done for the 0 bit. In the extraction process it’s similar to embedding process with addition of one extra step, the message bit is considered 1 if the result is greater than one and 0 if its zero.

K. Venkata Ramana et al [9] have proposed a new method in which they have introduced file hybridization along with Steganography and cryptography to improve security. Steganography is used to hide the information from the attackers eyes, incase it's been identified the next line of defense provided is cryptography. To help enhance the cryptic message the authors have employed File hybridization, so putting all three methods together they came up with Randomized Secure Data Hiding Algorithm using File Hybridization (RSDHAFH). Basically in this method 2 phases of embedding take place after encrypting the message, one is hiding the encrypted secret data into the container image and the other is the container image into supporter image. The second embedding process is nothing but file hybridization.

Ravuru Rakesh et al [10] have proposed multiple methods on image Steganography which mainly revolves around the MSN (most significant nibble) of each pixel. This paper makes use of the fact that randomization increases security in Steganography. One such method is ranked MSN method in which the LSN (least significant nibble) are loaded with the hidden data in order of increasing value of their respective MSN. Second one is embedding the data in LSN by XORing it with the data with MSN and then hiding. Other methods include variable length, parity check and also one where it involves embedding the data depending on whether the respective bit in MSN is 1 or 0.

Weiqi Luo et al[11] have proposed an image Steganographic method in which the embedding regions are selected according to the size of secret message and the difference between two consecutive pixels in the cover image instead of Pseudo Random
Number Generator [PRNG]. The sharper regions of the image are used to embed the data while the smoother regions are kept as it is. This is because the more changes in the LSB of sharper regions are less perceptible to human eyes. This will improve the visual quality of the Stego image and increases imperceptibility.

Anita Pradhan et al [12] have proposed an image Steganographic method based on two, three and four neighborhood pixels. Either horizontal or vertical neighbors of one horizontal and other vertical pixels have been used to embed the information. All the neighborhood methods have resulted in different payload capacity but four neighborhood have proved to carry the highest payload.

Po-Yueh Chen and Wei-En Wu [13] proposed an image Steganographic method based on Side-Matching. The pixels present on the edges of the images are being used. The objective is to exploit human visual system. The paper proposed three methods namely two sided side match, three sided side match and four sided side match methods. In all these methods the data is embedded into the pixels with respect to some reference pixels.

Bin Luo et al [14] have proposed an innovative way of image Steganography. They made use of the fact that changes in edges in an image have a very less probability of being perceived by the human eye. They performed this new method of multiple embedding on color images. First they identify the edges in one of the RGB planes using sobel operator, then embed the data in the corresponding position as that of the identified edges in the other two planes. Then it is repeated for the other two planes. Due to the process of multiple embedding the data hiding capacity they achieved was high.

Nitin Jain, Sachin Meshram and Shikha Dubey [15] proposed LSB substitution and edge detection in which they went for edge detection as changes to it is less susceptible to identification by an attacker. They employ zero crossing detectors to identify the edges. The zero crossing detector checks if the Laplacians passes through zero since the region where it passes through the zero has a very high chance of being an edge. Another method of identifying edges is to compare the gradient value of the pixels; if it exceeds a certain threshold then it is an edge. Then they embed the data using a modified version of LSB substitution.
Khosravi Sara et al [16] have proposed a method to hide data in BMP images. They exploited the fact that a natural image has high cross correlation between 2 neighboring pixels. This can also be applied to LSB planes in a color image. The main advantage of going to color images (3 planes) is that the data gets dispersed in the 3 planes, hence increases randomness and security. Except for the fact they go for random selection of pixels they do basic LSB substitution.

Ali Akbar Nikoukar [17] proposed a new algorithm for color image Steganography using the RGB planes. In the proposed method the author encodes the data first and converts the encoded data into bit stream. Then the bit stream is embedded into the cover image. In his algorithm, the author embeds 2bits in the plane whose value is minimum compared to other 2 planes and 3 bits in the remaining planes for each pixel. This improves the undetectability.

Kalavathi.Alla and Dr. R. Siva Rama Prasad [18] proposed a Steganography method for Hindi characters. Usually the Steganographic techniques are meant for only English characters but in this paper the authors proposed a method to hide the Hindi characters. In this method the Hindi message is first encode into a numerical value. To encode the Hindi letters and diacritics they used the Vedic Numerical Codes of Indian Theology. This method helps to hide the Hindi characters and makes Steganography more comfortable. Also the same thing can be applied for other Indian languages which are similar to Hindi.

Lifeng Zhang1 et al [19] explains the use of curvelet transform in image steganography. This technique has enhanced the availability of pixels for embedding data

Peining Tao1 and Ahmet M. Eskicioglu2 [20] describes the way in which images can be decomposed in curvelet domain transform techniques.

Rikin Nayak1 et al [21] have described angular analysis of energy distribution with respect to sub-bands in curvelet domain. Minh N. Doyand Martin and Vetterli [22] have explained use of filter banks in curvelets. Xiaoming Yao et al [23] have dealt with EMD-like (exploiting modification direction, EMD) information hiding schemes Schemes of this kind can usually achieve very high capacity of secret bits without causing
too much distortion of the cover image, but suffer from sensitivity to noise without exception.

Debnath Bhattacharyya and Asmita Haveliya [24] proposed a methodology for embedding a color image data into a PDF file and vice versa. Encryption is done at the transmitter and decryption is done accordingly at the receiver. Hassan Mathkour et al [25] have proposed an approach which is based on the LSB substitution technique applied on RGB color components of BMP images.

Geetha C.R et al [26] describes hiding data in images through geometrical figures. Hybrid of both Cryptography and Steganography, which uses LSB substitution in geometrical way of selecting pixels & secret key cryptography in providing high security for hiding the data. This paper explains the using of JPEG image as a STEGO IMAGE and dimensions of geometrical figures as CIPHER KEY. It provides a new way of approach for data hiding the images and further implementations could be done by using segmentation, In which the key becomes bit more complicated as it includes angle also to embed and extract the data.

Sujaynarayana and gaurav Prasad [27] introduces combined method of cryptography with steganography. CHAN Yan-yan et al [28] based on digital watermarking, have proposed a new visual cryptography scheme with meaningful shares. Yong Yang [29] explains a novel image fusion algorithm based on wavelet transform is presented. The images to be fused are firstly decomposed into high frequency and low frequency bands. Zhang Jiajia et al [30] proposed an idea to provide large capacity of the hidden secret data and to maintain a good visual quality of Stego-image, a novel Steganographic method based on SOM and wavelet contrast is presented.

Yi-Hui Chen et al [31] introduced an algorithm which utilized image denoising algorithm. The transformations used for the research was wavelet transform.

Zixiang Xiong et al [32] have worked on coding techniques like image and video coding. The transformation they have utilized the advantages of both Discrete Cosine Transform and Discrete Wavelet Transform.
Miss. Prajakta Deshmane and Prof. S.R. Jagtap [33] have given the taxonomy of the current image steganographic techniques for the image files. The image steganographic methods are reviewed for both loss and lossless image files such as JPEG, BMP. The different techniques include spatial domain methods, transform domain methods and those which modify the image file format. All these methods are compared with respect to three important factors of steganographic design imperceptibility, capacity and robustness. In this paper, they have discussed about various spatial domain technique and frequency domain techniques. Since the robustness is less in spatial domain algorithms, transfer domain algorithms are preferred.

Swati Kumravat[34], in her paper discusses about a steganographic scheme for text hiding and logo hiding. Here, natural images are used as cover medium for hiding secret information. Thamaraiselvi M, Tina Trueman, Rajasoundaran S[35] have explained about the biometric feature of the cover image to hide the secret data i.e. the skin region of the image that will provide an excellent secure location for hiding the data

Sunita Barve, Uma Nagaraj and Rohit Gulabani [36] have proposed a digital image steganographic technique which explores the biometric feature of skin tone region in images. This system should be capable of embedding secret images using the Discrete Wavelet Transform Anjali A. Shejul, Umesh L. Kulkarni[37] have proposed an algorithm for image hiding using skin detection and it mainly has two cases, namely with cropping and without cropping. Amritha.G, Meethu Varkey [38] proposed in their paper, a technique that uses wavelet transform which is one of the transform domain techniques. There are different transforms like DCT, DWT etc. DWT is widely preferred compared to DCT because the noise constraint is less in DWT. DWT provides better performance compared to DCT while compression. Here DWT uses transform domain technique compared to other spatial domain techniques which are more efficient.

Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath [39] explains about DWT used for digital images. Stuti Goel, Arun Rana, and Manpreet Kaur[40], in their paper compares various methods of image steganography. This paper deals with hiding text in an image file using Least Significant Bit (LSB) based Steganography,

2.4 Problem Formulation
Study of different Steganographic techniques have inferred the fact that any steganographic algorithm is considered to be strong if it attains the three main goals such as undetectability, high payload capacity and robustness. In Transform domain methods the payload capacity is low and hence the future scope is to enhance Stego image quality and payload capacity by employing adaptive Steganographic techniques. The objective of this thesis is to design and develop an efficient Steganographic algorithm against Steganalysis for Secure Communication.

2.5 Conclusion

In order to provide better security Cryptography and steganography techniques can be consider effectively for these network related applications. So both these techniques are effective method in terms of practically as well as theoretically unbreakable one. And major highlight of these approach are image can be perfectly reconstructed and the message can be retrieved without any loss.