CHAPTER 2

Literature Review

2.1 Introduction

Digital images are the most commonly used medium for steganography as they are most widely available over the Internet and on the Web. Steganography hides information in image as multimedia carriers in such a way that does not draw attention among billions of images over the internet (Chandramouli et al., 2004). Therefore, image steganography is potential for various communication applications in order to improve communication security and has become a popular topic on research. The work in this thesis is related to steganography in image files. This chapter provides a literature review of the techniques related to image based steganography and studies the methods proposed by different authors.

As this thesis focuses on the steganographic technique, firstly the requirements of a basic steganographic system is described. The three most important requirements that must be satisfied for steganographic technique are capacity, security, and robustness as in figure 2.1 (Wang and Wang, 2004). The evaluation of steganography technique is done with these three parameters and there must be tradeoffs between these parameters to have better steganographic technique (Fridrich, 1999b).

![Figure 2.1: Basic requirements of a steganographic system](image-url)
• **Capacity:** Capacity refers to the amount of secret information that can be embedded in the cover medium (Katzenbeissser and Petitolas, 2000). Steganography aims at hidden communication and therefore usually requires sufficient embedding capacity (Wang and Wang, 2004). Steganographic capacity is the maximum number of bits that can be embedded in a given cover file without affecting the quality of the cover medium and also minimizing the perception of the hidden data in the stego medium. The capacity of the secret message that is to be embedded must be less than the size of the cover medium.

• **Robustness:** Robustness is the ability to extract hidden information after common image processing operations and the embedded data to remain intact if the stego medium undergoes stego attacks (Fridrich, 1999b). The robustness requirement is required when traded with data hiding capacity. In steganography robustness is not a top priority, thus steganographic systems are either not robust against modifications or have limited robustness against technical modifications (Wang and Wang, 2004).

• **Security:** Security indicates an eavesdropper’s inability to detect embedded information. Such information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the carrier with hidden message (Fridrich, 1999b). In order to avoid raising the suspicions of attackers, the hidden contents must be invisible both perceptually and statistically (Wang and Wang, 2004). Therefore, the characteristics and attributes of cover files should not be changed and no distortions should be produced during the embedding process (Venkatraman et al., 2004).

The review on digital image steganography in this chapter is classified into two categories:

2.2 Steganography in the Image Spatial Domain.
2.3 Steganography in the Image Frequency Domain.
2.2 Steganography in the Image Spatial Domain

Steganography techniques that modify the cover image in the spatial domain are known as spatial domain methods which involve encoding at the LSBs level (Sharda and Budhiraja, 2013). The common ground of spatial steganography is to directly change the image pixel values for hiding data (Li et al., 2011). The basic concept of Least Significant Bit Substitution includes the embedding of the secret data at the bits which having minimum weighting so that it will not affect the value of original pixel (Kanzariya and Nimavat, 2013). In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message and such approach has become the basis of many techniques that hide messages within multimedia carrier data (Pavani et al., 2013). By making slight modifications to the RGB value of each pixel, a new color is produced that is so close to the original that the difference cannot be visualized and binary data can easily be hidden in the LSB values of any true color image (Hosmer, 2006). LSB based steganography technique either change the pixel value by ±1 or leave them unchanged which is dependent on the nature of the hidden bit and the LSB of the corresponding pixel value (Chandramouli and Memon, 2001).

Lin et al., (2002) proposed an image-hiding scheme in the spatial domain that embeds secret image in the pixels of a true color image. The secret image can be both a grayscale and a true color image. In case of color image to reduce the size of the transmitted data, the secret image is quantized where the red, green, and blue components of the secret image are coarsely quantized. Neeta et al., (2006) emphasize strongly on image Steganography providing a strong focus on the LSB techniques in image Steganography and explain the LSB embedding technique and present the evaluation results for various least significant bits for .png and .bmp file. A method of steganography for embedding a color or a grayscale image in a true color image is proposed by Yu et al., (2007). They described that the proposed method can hide three types of secret images: hiding a color secret image, hiding a palette-based 256-color secret image, and hiding a grayscale image in a true color image. They further claimed that the proposed method enables hiding embedding capacity and it performs better than Lin et al., (2002) scheme in terms of PSNR and image quality.
Most of previous works on steganography aimed at hiding grayscale images in grayscale host images and excluded the use of color images because of the complexity of using color images as host images. This constraint has two drawbacks. One is that only grayscale images are used to hide grayscale images. This is impractical because many valuable images are available in color. The other is the limited hiding capacity that a grayscale host image has (Yu et al., 2007).

To overcome the shortcoming of the traditional LSB embedding algorithm, a LSB watermarking algorithm is proposed by Li et al., (2009) to embed the land reorganization planning map into a remote sensing image where the LSB signal is preprocessed by the exclusive-OR (XOR) operation, and then the watermark data are inserted by bit’s XOR of watermark sequence and LSB sequence. A lossless data hiding scheme based on a combination of prediction and the prediction-error adjustment (PEA) is presented by Weng et al., (2009). For one pixel, its four surrounding neighboring pixels are used to predict it and 1-bit watermark information is embedded into the prediction-error.

A data hiding scheme by simple LSB substitution with an optimal pixel adjustment process (OPAP) is proposed by Chan and Cheng, (2004). According to them, the method requires a checking of the embedding error between the original cover-image and the stego-image. Chang and Tseng, (2004) proposed a steganographic method was based on the human visual system sensitivity to image contrast change that hides data in spatial domain of images. The method exploits the correlation between neighboring pixels to estimate the degree of smoothness or contrast of pixels. It does not replace the LSBs of pixel value directly, but changes the pixel value into another similar value. Chen and Wu, (2009) proposed an image steganography scheme to improve the side match method proposed by Chang and Tseng, (2004) by hiding more information in the edge portions. They stated that human eyes can rarely percept trivial differences in the edge regions.

A spatial domain block based steganographic algorithm is proposed which uses single digit sum function for embedding by Sur et al., (2008). They discussed that the method reduces the amount of noise added during embedding and have same payloads as other spatial domain schemes. In this scheme, a pixel is selected randomly from the
image using a shared secret key. Nithyanandam et al., (2011) presented a steganographic algorithm in spatial domain that uses matrix embedding technique to embed the secret image which is initially Huffman encoded. The Huffman encoded image is overlaid on the selected bits of all the channels of pixels of cover image through matrix embedding. An image data hiding technique by adaptive Least Significant Bits (LSBs) substitution is proposed by Mortha and Kassey, (2012) where pixels in the noise non-sensitive regions are embedded by a k-bit LSB substitution with a larger value of k than that of the pixels in noise sensitive regions. An optimal pixel adjustment process is used and also the LSBs number is computed by the high-order bits rather than all the bits of the image pixel value.

Wu et al., (2004) proposed a method based on a palette modification scheme, which can iteratively embed one message bit into each pixel in a palette-based image. At each iteration, both the cost of removing an entry color in a palette and the benefit of generating a new one to replace it are calculated. If the maximal benefit exceeds the minimal cost, an entry color is replaced. Agaian and Perez, (2004) proposed a steganographic approach for palette-based images that have the advantage of embedding secure data, within the index, the palette or both, using special sorting scheme. Firstly, the covered image is divided into block sizes. Pixels are selected using a random generated key. A stego-bit is embedded at each pixel of the selected blocks. Embedding is accomplished by selecting the closest color using a weighted distance measure that contains the desired modulus-bit. Wang et al., (2005) described an algorithm for embedding data into palette-based images via grouping similar colors together and quantizing them into one color. They used a greedy approach and with chosen risk function for achieving optimal performance. Bandyopadhyay and Maitra, (2010) proposed a method of palette based steganography based on color quantization that compresses the image from a 24-bit bitmap to an 8-bit bitmap. According to them, this slight variation in the image helps in hiding the data that are barely noticeable to the human eye.

Medeni and Souidi, (2011) proposed a steganographic method for hiding information within the spatial domain of the gray scale image. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. A
steganographic algorithm for 8bit (grayscale) or 24 bit (color image) is presented by Sharma and Shrivastava, (2012) based on Logical operation that embeds secret data into the LSB of cover image. Biswas et al., (2012) stated that dithering changes the colors of pixels in a neighbourhood so that the average color in each neighbourhood approximates the original RGB color. They used such dithering technique to hide a secret image in a cover-image.

Mielikainen, (2006) proposed a modification to the Least-Significant-Bit (LSB) matching named LSB matching revisited (LSBMR) which uses the choice to set a binary function of two cover pixels to the desired value and the value of the binary function is used to carry information. He stated that the modified method allows embedding the same payload as LSB matching, but with fewer changes to the cover image. Zhang et al., (2007) proposed a plus/minus one embedding scheme, also called as LSB Matching (LSBM) method that employs a slight modification to LSB replacement scheme. The secret data in stream of bits, based on a pseudo-random order, is matched against the LSB of the next cover pixel. On having a match, nothing is done. Otherwise the cover pixel value is incremented or decremented by 1, at random. Luo et al., (2010) proposed an edge adaptive image steganographic method (EA-LSBMR) based on least significant bit (LSB) matching revisited where the cover-image is initially preprocessed and then the embedding regions determined by a pseudo random number generator (PRNG) are selected adaptively by considering the message length and the pixel-pairs’ differences and then data hiding is performed based on LSBMR.

Cryptography can be applied to steganography to attain better security of the secret data. Song et al., (2011) proposed a communication protocol that combines steganography and cryptography techniques. It is based on the LSB matching method where the Boolean function is used for encryption and controlling the pseudo-random increment or decrement of LSB. According to them such approach is highly robust to resist regular steganalysis, such as RS analysis, GPC analysis, $\chi^2$–analysis. Swain and Lenka, (2010) proposed a technique based on both cryptography and image steganography. The secret message is encrypted and is embedded into the carrier image in 6th, 7th and 8th bit locations of the darkest and brightest pixels. The brightest pixels means having a gray value in the range 224 to 255 in 8 bit gray
scale and darkest pixels means having gray value in the range 0 to 31 in 8 bit gray scale.

Karim et al., (2011) proposed a method that hides secret data within the LSB of image where the secret information is first encrypted and then stored into different position of LSB of image depending on the secret key. Tomar, (2012) proposed a steganography based on LSB insertion and RSA (Rivest-Shamir-Adleman) encryption with the aim of providing better security about hidden data. The scheme encrypts secret data by RSA algorithm and then embedded into each cover pixels by modifying the least significant bits (LSBs) of cover pixels. Another such approach is proposed by Tyagi et al., (2012) based on the LSB (least significant bit) and encryption algorithm. In their method the secret data is first encrypted using symmetric encryption algorithm before embedding into the LSB’s. They stated that by using such approach there is less chance of an attacker being able to recover data and by their assessment the proposed algorithm is robust against attacks. According to Tomar et al., (2012) and Tyagi et al., (2012) by combining encryption and steganographic technique data security can be enhanced.

The secret data can be pre-processed before embedding and according to Jain and Kumar, (2012) this preprocessing reduces the size of the data by a significantly great amount and also improves the embedding capacity of the image because of data compression. Based on this, they proposed a steganographic approach in secret data is preprocessed first and then the preprocessed secret data is embedded into the LSBs of the cover image depending upon the intensity of the pixel values of the cover image. For pre-processing a lossless data compression technique, LZW (Lempel–Ziv–Welch) technique is used for pre-processing the data.

A steganographic method for embedding secret messages into a gray-valued cover image using pixel-value differencing (PVD) is proposed by Wu and Tsai, (2003). For embedding a difference value is calculated from the values of the two pixels in each block and is replaced by a new value to embed the value of the secret message. A data hiding method based on the least significant bit (LSB) substitution and the multi-pixel differencing (MPD) method is presented by Jung et al., (2008). First, a sum of different values for a four-pixel sub-block is calculated and the low value of the sum
can be located on a smooth block and the high value is located on an edged block. The secret data are hidden into the cover image by the LSB method in the smooth block, while the MPD method is concealed in the edged block.

According to Luo et al., (2011), based on extensive experiments it is found that some statistical artifacts will be inevitably introduced even with a low embedding capacity in most existing PVD-based algorithms. According to Mandal and Das, (2012) pixel value differencing (PVD) method can be used for secret data embedding in each of the component of a pixel in a color image. As in a color image every pixel value composed of red, green and blue component and each of which ranges from 0 to 255 in case of 8-bit representation. But when the pixel-value differencing (PVD) method is used in image steganographic scheme, the pixel values in the stego-image may exceed the range 0–255. Another approach of combining cryptographic and steganographic technique is proposed by Phad et al., (2012) where firstly secret message is encrypted using advanced encryption standard (AES) algorithm and then pixel value differencing (PVD) with K-bit least-significant-bit (LSB) substitution is used to hide encrypted message into the image.

Din et al., (2006) designed based on the least significant bit (LSB) method where each bit of the secret message picks a random red, green, or blue component in the pixel. It then sets the least significant bit in that component to the bit value it is embedding. A key is used as password for the random number generator. When the message is extracted, the program initializes the random number generator by using the same seed so that it would produce the same series of pseudorandom numbers.

Liang et al., (2007) presented a scheme for embedding secret data into a binary image by encoding the secret bits directly into boundary pixels by checking each pixel of the cover image in a pseudo-random order for embedding eligibility. A secret key is used to generate a pseudo-random pixel scanning order, which avoids concentration of pixel alterations and ensures data security. Parvez and Gutub, (2008) proposed a technique for RGB image steganography, where color intensity in each channel (values of R-G-B) is used to decide the number of bits to store in each pixel. Channels containing lower color values can store higher number of data bits. The sequence of channels is selected randomly using pixel indicator based on a shared key.
A Least Significant Bits (LSB) replacement steganography approach is proposed by Rana and Singh, (2010) that encrypts the secret message by changing position of bits using transformations and the binary representation of the encrypted data is divided into four parts. The image is also then divided into four blocks. Each part of data is hidden in each block by selecting a pixel in a random manner. They stated that the random pixel selection makes it difficult to find the sequence of the message hence resulting in a strong stego-image.

According to Amirtharajan et al., (2010) randomization is expected to increase the capacity and the security of the system. Based on randomization principle using LSB they proposed a method where the secret is hidden in the least significant bits of the pixels using pixel indicator methodology.

Baker, (2011) proposed a LSB technique that that uses geometrical mathematical for intersecting planes in random selection of the pixels for embedding. The plane is specified by setting up an equation in a frame that identifies every point that belongs to the plane. An LSB based image Steganography is proposed Pujari and Mukhopadhyay, (2012) where the secret message is divided or segmented into random number of units holding equal number of characters and the cover image is logically divided into a random number of square blocks. Each logical block of image is used to hide each unit of message in a pseudo-random fashion.

Karthikeyan et al., (2012) proposed secret key steganography based on LSB replacement approach for hiding a plaintext in a grayscale image. They stated that the embedding of the plaintext in an image is performed using a randomized matrix as key and as the key generated is randomized in a matrix, the plaintext thus gets randomized while inserting it in the original image. Such embedding is highly secured and there is no explicit change in the original image even if long plaintext is inserted in the image.

### 2.3 Steganography in the Image Frequency Domain

In the frequency domain, cover images is first transformed using a frequency-oriented mechanism such as discrete cosine transform (DCT), discrete wavelet transform
Literature Review

(DWT) or similar mechanisms to transform the pixel values in the spatial domain to coefficients in the frequency domain, after which the secret messages can be combined with the coefficients in the frequency-form images to achieve embedding (Chang et al., 2002; Li and Wang, 2007; Yu et al., 2007; Sharda and Budhiraja, 2013). The idea is to hide information in frequency domain by altering magnitude of all of discrete cosine transform (DCT) coefficients of cover image (Kanzariya and Nimavat, 2013). Each image is broken up into 8 × 8 pixel blocks, and coefficients are calculated and stored for the DCT that approximates the true color rendering for the block (Hosmer, 2006). The Discrete Cosine Transform (DCT) is applied to the given cover image to get the DCT coefficients (Chang et al., 2002). JPEG images have such compression as key advantage over other formats and using such compression high color quality images can be easily stored in relatively small files (Hamid et al., 2012; Godara et al., 2013). Embedding in DCT coefficient does not cause noticeable visible effects and detectable statistical changes (Liu and Liao, 2008; Godara et al., 2013).

Jpeg–Jsteg (Upham, 1997; Hsu and Wu, 1999) is a famous hiding-tool based on JPEG. In Jpeg–Jsteg, the secret messages are embedded in low-frequency part of quantized DCT coefficients whose values are not 0, 1, or -1. The embedding sequence employed in Jpeg–Jsteg is in the zigzag scan order.

A blind data hiding technique for hiding information in still images is presented by Alturki and Mersereau, (2001) which is based on embedding the information in the transform domain, after decorrelating the samples in the spatial domain. Chen and Wornell, (2001) introduced classes of embedding methods, termed quantization index modulation (QIM). According to them, data embedding by QIM using two different quantizers is generally carried out in such a way that in order to embed zero, one of two quantizers is used at the quantization step of DCT coefficients, and the other quantizer is used to embed one. QIM performs well in the case of noise-less channels but it is not very robust against channel noise.

A steganographic method based on JPEG is proposed by Chang et al., (2002) that embed data in the DCT coefficients. The proposed method firstly encrypts the secret message using encryption algorithm and then the secret message is hidden in the
cover-image with its middle-frequency of the quantized DCT coefficients. By comparing the method with Jpeg–Jsteg, they discussed that the proposed method provides larger message capacity and has the same security level as Jpeg–Jsteg.

Cherukuri and Agaian, (2007) introduced a switching theory based steganographic system for JPEG images which uses the fact that energy distribution among the quantized high frequency coefficients varies from block to block and coefficient to coefficient. A JPEG and Particle Swarm Optimization algorithm (PSO), based image steganography is proposed by Li and Wang, (2007) that hide secret data in the middle frequency components of the quantized DCT coefficients of the cover-image. A complementary embedding strategy based on JPEG steganography is presented by Liu and Liao, (2008) where the quantized DCT coefficients and the secret bits are divided into two parts according to a predefined partition ratio. The two parts of DCT coefficients are used to embed the corresponding parts of secret bits by subtracting one from or adding one to the non-zero DCT coefficients.

Jianquan et al., (2009) discussed a method where invariance of JPEG compression is analyzed firstly. Then, according to invariance of JPEG compression, an information hiding algorithm which can embed information in DCT median and high frequency coefficients is proposed. Information embedding capacity adaptively is determined by smooth state of sub-blocks.

A method of steganography that embeds message bits in the 4th bit of successive non-zero DCT coefficients of the low frequency of a transform domain is proposed Kafri and Suleiman, (2009) that utilizes the idea of SSB–4 technique in modifying the other bits (i.e, 1st, 2nd, 3rd and/or 5th), to obtain the minimum variation between the original and the modified coefficient. Two optimization techniques, namely, block pattern coding and dynamic programming, are proposed for hiding messages into grayscale images by Lee and Tsai, (2009) with image distortion minimization. Data embedding is accomplished by changing the block bit values so that the corresponding code of the resulting block pattern becomes just some bits of the input message data to be embedded.

Jokay and Moravcik, (2010) presented a steganographic technique based on modification of the least significant bits in JPEG images. The focus is on minimizing
of the number of modified DCT coefficients using hamming codes. They discussed that using the hamming codes for embedding and compression for preprocessing, it is possible to increase the number of inserted bits of the secret information, while reducing the number of modified DCT coefficients. A DCT based steganographic method for gray scale images is proposed by Al-Momen and George, (2010) with the objective to create a safe embedding area in the middle and high frequency region of the DCT domain using a magnitude modulation technique. The magnitude modulation is applied using uniform quantization with magnitude adder/subtractor modules on the chosen transformed coefficients in order to get a safe position to hide the secret bits sequence.

Lin and Shiu, (2010) proposed DCT-based steganography scheme based on a notation transformation concept to embed the secret data into the DCT coefficients by dividing the coefficients in the six sub-areas in the middle frequency in the DCT to adaptively embed secret data into coefficients. An Image steganography based on Block-DCT is proposed by Nag et al., (2010), where Huffman encoding is performed before embedding and each bit of Huffman code of secret message/image is embedded in the frequency domain by altering the least significant bit of each of the DCT coefficients of cover image blocks.

Kaur et al., (2011) proposed a DCT based watermarking scheme in which, the watermark is embedded in the mid frequency band of the DCT blocks carrying low frequency components and the high frequency sub band components remain unused. Watermark is inserted by adjusting the DCT coefficients of the image and by using the private key.

A method is proposed by Sheisi et al., 2012 that embed data in the DCT coefficients of the middle frequencies. By starting from the last coefficient in the middle frequencies area, the LSB of each coefficient is replaced with data bits. However the capacity in this method is less than the JSteg algorithm. A 2-D Block-DCT based steganography technique is proposed by Singh et al., (2012), where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain and the secret message is embedded in the middle and lower frequency part of the quantized DCT coefficients. Kaur and Ranade, (2012) proposed a data hiding
process in the DCT domain where the embedding algorithm is based on the quantized projection embedding method. The embedding is done on the quantized DCT coefficients using the concept of Hadamard Matrix as base vector. They stated that the process achieves high capacity as comparable to the existing techniques of DCT domain.

A steganographic technique named Inverted Steganographic Algorithm (ISA) for message embedding in the least bits of nonzero DCT of JPEG images is presented by Morsy et al., (2012). This steganographic system is based on inverting each bit flipped by message bit with the corresponding bit in the pair of values (PoVs) of the DCT coefficients. A steganography algorithm based on discrete cosine transform (DCT), Arnold transform and chaotic system is proposed by Singh and Siddiqui, (2012). The chaotic system is used to generate a random sequence to be used for spreading data in the middle frequency band DCT coefficient of the cover image.

Hsieh et al., (2001) presented a wavelet-based watermarking approach by adding visually recognizable images to the large coefficients at the high and middle frequency bands of the DWT of an image. In the proposed approach, an original image is decomposed into three levels with ten sub-bands of a pyramid structure. A DWT based steganography technique which embeds the secret messages in frequency domain is proposed by Chen and Lin, (2006) where method is divided into two modes and 5 cases. The secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality.

Reddy and Raja, (2009) proposed a DWT steganography based on fusion. The payload wavelet coefficients are encrypted and fused with wavelet coefficients of cover image to generate stego coefficients based on the embedding strength parameters alpha and beta. The cover and payload are preprocessed to reduce the pixel range to ensure the payload is recovered accurately at the destination. Al-Ataby and Al-Naima, (2010) proposed a wavelet transform based steganography that pre-adjusts the original cover-image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and thus to
recover the message correctly. Then, it uses Wavelet transform to transform both the cover-image and the hidden message.

A method of color image steganography based on discrete wavelet and discrete cosine transforms where the data hiding process takes place in one channel and in HH sub-band of the cover image is proposed by Latef, (2011). A DWT based Image steganography is proposed by Nag et al., (2011), where two-dimensional Discrete Wavelet Transform is performed on a gray level cover image and then Huffman encoding is performed on the secret data before embedding. Then each bit of Huffman code of secret data is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Dey et al., (2012) proposed a wavelet based Steganographic technique in which a color image is embedded into another color image. Both the cover image and the secret image are decomposed into three separate color planes namely R, G and B and then each plane of the images is decomposed into four sub bands using DWT.

Kumari et al., (2010) presented a framework for data hiding with the combination of steganography and encryption algorithms. The secret data is encrypted and data embedding is done in the transform domain, with a set of transform coefficients in the low and mid frequency bands selected as possible candidates for embedding. A threshold is used to determine whether to embed in a block or in a coefficient. Sarmah and Bajpai, (2010) proposed a technique in which Cryptography and Steganography are used as integrated part for enhancing security module for transmitting of secret text. Before encryption the secret data is compressed using Huffman compression technique and compressed text is encrypted using advanced encryption standard (AES). After encryption, a part of the compressed encrypted message (cipher) is hidden in DCT of an image. Marwaha, (2010) proposed a system of encrypting data that combines the features of cryptography and Visual steganography which is implemented in image files. They used traditional cryptographic techniques to achieve data encryption and then visual steganography algorithms will be used to hide the encrypted data.

Ananthan and Lakshmanan, (2012) proposed a steganographic technique to provide security for user accounts through encryption and image block based steganography.
They discussed that data theft and peer repudiation is checked by this technique of encryption and steganography. A mixed approach that applies the spatial domain with the frequency domain of steganography techniques and Asymmetric key cryptography is proposed by Singla and Syal, (2012). The idea is to utilize a significant bit of the DCT coefficients of a cover image to hide encrypted message bits. Each bit of data is embedded by altering the least significant bit of low frequency DCT coefficients of cover image blocks. Shahana, (2013) proposed a frequency domain steganography technique that uses DCT steganography and encryption for attaining security of secret data. The encryption is performed on secret image before embedding using RSA (Rivest-Shamir-Adleman) algorithm. The encrypted image is embedded in the mid frequency DCT coefficients of cover-image. An integrated approach of combining Discrete Cosine Transform (DCT) technique with LSB techniques is presented by Chhikara and Kumar, (2012). Initially the secret message is encrypted before embedding then the cover-image is transformed using DCT and LSB technique which is used to insert in pixels.

A Biometric Steganography is presented by Shejul and Kulkarni, (2011) that uses skin region of images in DWT domain for embedding secret data. They stated that by embedding data in only certain region (here skin region) enhances the security of the data. Two cases for data embedding are considered, with cropping and without cropping. The biometric feature can also be used to implement steganography in skin tone region of images and based on this a biometrics based Steganography method is proposed by Manoj et al., (2013). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Additionally the secret data is encrypted by AES (Advanced Encryption Standard) before embedding.

As transform domain steganography involves dividing cover image into 8×8 blocks, Batra and Kaushik, (2012) presented a steganographic method based on the JPEG quantization table modification where instead of dividing cover image into 8×8 blocks, the cover image is divided into non-overlapping blocks of 16×16 pixels to embed secret information. According to them, the quantization table increases that lead to the increase in number of modified quantized DCT coefficients and thus more secret data can be embedded into cover-image that results in enhancement of stego capacity. Almohammad et al., (2008) presented a steganographic approach based on
Discrete Cosine Transformation (DCT) that divides the cover image into non-overlapping blocks of 16x16 pixels. The transformed DCT coefficients are quantized by a modified 16x16 quantization table. For each quantized DCT block, the least two-significant bits (2-LSBs) of each middle frequency coefficient are modified to embed two secret bits. However, the size of the stego-images increases. A DCT based steganography is proposed by Bansal and Lamba, (2013) which is based on JPEG quantization table modification where the cover image is divided into 32*32 blocks and then DCT is applied on each block.

According to Bracamonte et al., (1997) the DCT calculation for block-sizes larger than 8x8 pixels may require much more running time and may increase the computational operations and complexity. They further stated that using block size of 16x16 pixels or more may require more computational time and this might be one of the reasons why the standard JPEG uses blocks of 8x8 pixels and most of the work present in literature uses block size of 8x8 pixels.

Steganography based on Payload Transformation (SPT) is proposed by Kumar et al., (2011) which is non LSB and non transform domain technique where the cover-image is segmented into 2*2 matrices and the matrix for payload embedding is considered based on the threshold value which is fixed by computing adjacent pixel intensity differences.

An image steganography method based on image contrast is presented by Pramitha et al., (2011) where a group of 2 × 2 blocks of non-overlapping spatially adjacent pixels is selected as the valid block for embedding the secret message. A modulo based arithmetic operation is further applied to all the valid blocks to embed a pair of binary bits using the shortest route modification scheme. Each secret message is also encrypted by RSA (Rivest-Shamir-Adleman) encryption algorithm to provide the system with more security.