Techniques for Digital Image Steganography- An Inclusive and Methodical Review

Anita paneri
M.Tech Scholar,CSE
Geetanjali Institue of Technical Studies
Udaipur

Mayank Patel
Assosciate professor,CSE
Geetanjali Institue of Technical Studies
Udaipur

Abstract : ***Advancement of technology has made people to anguish about their privacy. Steganography is the art of passing information in a custom that the very existence of the message is anonymous. The goalmouth of steganography is to circumvent drawing suspicion to the transmission of a concealed message. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the information. Original message is being concealed within a carrier such that the vicissitudes so occurred in the carrier are not apparent. Numerous unlike carrier file formats can be used, but digital images are the utmost popular because of their frequency on the Internet. The topical growth in computational power and technology has propelled it to the forefront of today's security techniques. This paper presents a review of the literature on diverse types of contemporary steganography techniques for image in spatial and transform domains and other procedures for image steganography. Furthermore, research trends, issues, performance specification and challenges are also identified.***

***Keywords*— Image steganography, Information security, Digital communication, stegaanalysis , spatial domain, transform domain, cryptography, data hiding, Survey, Review Paper.**

I. INTRODUCTION

Steganography has been developed as a new covert communication means in recent years, in order to make up for the shortcomings of cryptographic techniques. Cryptography, on the other hand, is the science of secret communication, and it aims to make the secret message unreadable. However, this may still attract attention from eavesdroppers, because it is clear that the communication is encrypted. The concept of Steganography is to hide a secret message inside an innocuous cover medium, with the aim of concealing the existence of the message in a way that makes the communication of the secret invisible.

A. Steganography concepts

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the *prisoner's problem* proposed by Simmons [1], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [2].

The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [3].

B. Image and Transform Domain

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [4]. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image [5].

Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterised as "simple systems" [6]. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format [7].

Steganography in the transform domain involves the manipulation of algorithms and image transforms [6]. These methods hide messages in more significant areas of the cover image, making it more robust [8]. Many transform domain methods are independent of the image format and the embedded message may survive conversion

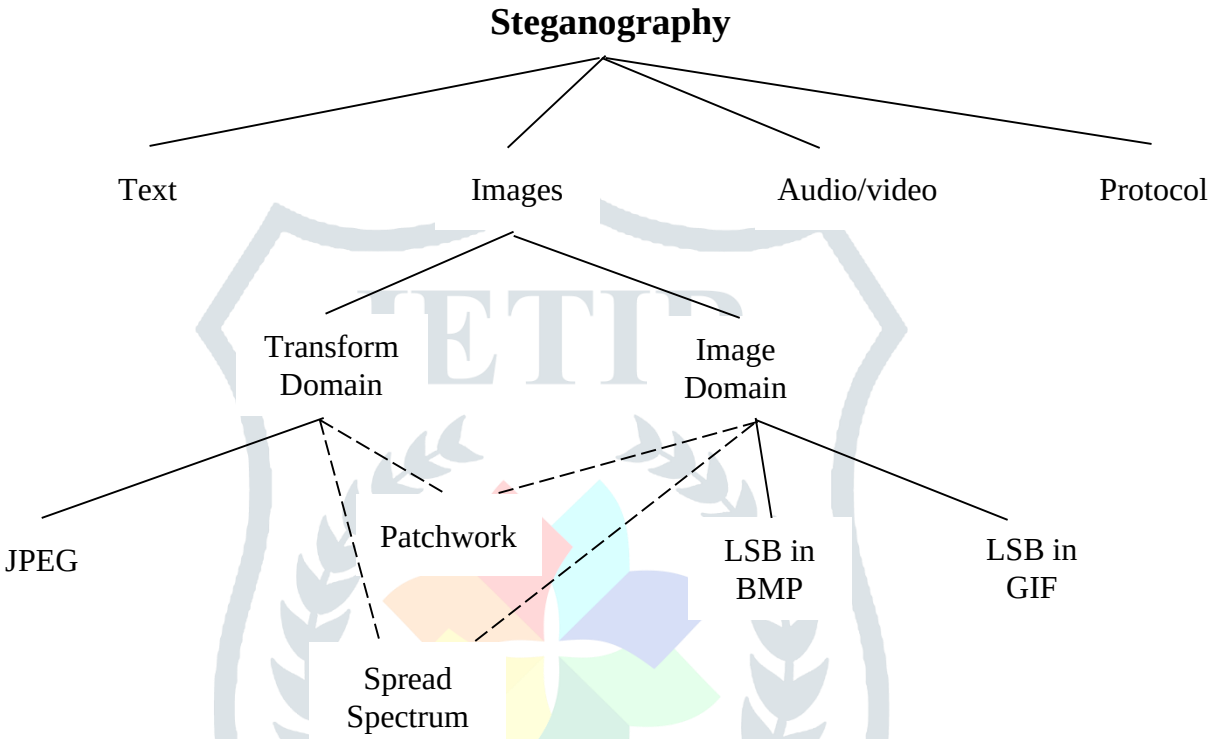

Fig. 1: Categories of image steganography

C. Era of Steganography

1. During the cold war two the Microdot technology developed by Germans which prints the clear good quality photographs shrinking to the size of a dot.
2. In Greece they select a person to send message by shaving their heads off. They write a secret message on their head and allow growing up their hair. Then the intended receiver will again shave off the hair and see the secret message.
3. During the world war two the secret message was written in invisible Ink so that the paper appears to be blank to the human eyes. The secret message is extracted back by heating the liquids such as milk, vinegar and fruit juices.

D. Steganography Types

There are two types of steganography they are Fragile and Robust,

1. *Fragile*

In Fragile steganography, if the file is modified, then the secret information is destroyed. For example the information is hidden the .bmp file format. If the file format is changed into .jpeg or some other format the hidden information is destroyed. The advantage of fragile is required to be proved when the file is modified.

2. *Robust*

In robust steganography the information is not easily destroyed as in fragile steganography. Robust steganography is difficult to implement than fragile [9].

II. BACKGROUND OF STEGANOGRAPHY

A. Image Steganography Terminologies

Image steganography terminologies are as follows: -

- *Cover-Image*: Original image which is used as a carrier for hidden information.
- *Message*: Actual information which is used to hide into images. Message could be a plain text or some other image.
- *Stego-Image*: After embedding message into cover image is known as stego-image.

- *Stego-Key*: A key is used for embedding or extracting the messages from cover-images and stegano-images.

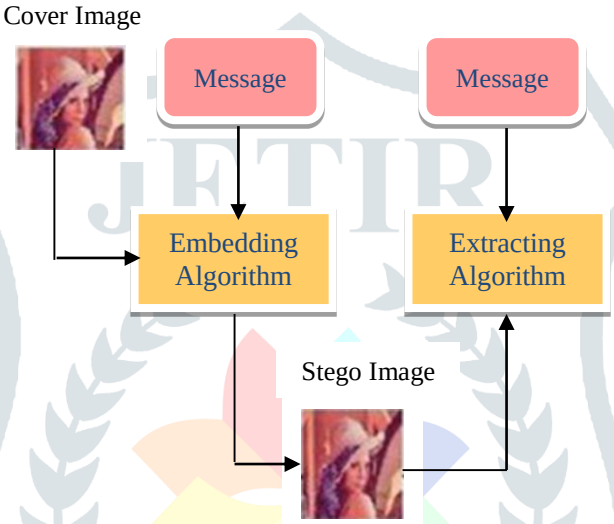

Fig. 2: Flow Diagram of Image Steganography

Generally, image steganography is method of information hiding into cover-image and generates a stego-image. This stego-image then sent to the other party by known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end [10]. Basic diagram of image steganography is shown in Figure 2 without stego-key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm unhides the message from stego-image.

B. Image Steganography Classifications

Generally, image steganography is categorized in following aspects [11] and Table I show the best steganographic measures.

- **High Capacity:** Maximum size of information can be embedded into image.
- **Perceptual Transparency:** After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to coverimage.
- **Robustness:** After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.
- **Temper Resistance:** It should be difficult to alter the message once it has been embedded into stego-image.
- **Computation Complexity:** How much expensive it is computationally for embedding and extracting a hidden message.

TABLE I. STEGANOGRAPHY ALGORITHM MEASURES

Measures	Advantages	Disadvantages
High Capacity	High	Low
Perceptual Transparency	High	Low
Robustness	High	Low

Temper Resistance	High	Low
Computation Complexity	Low	High

C. Applications of Steganography

Following are the important applications of Steganography:

- **Copyright Protection:** A secret copyright notice can be embedded inside an image to identify it as intellectual property. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified.
- **Feature Tagging:** Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.
- **Secret Communications:** In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographictechnology may be restricted or forbidden by law. However, the use of stenography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive I formation can be transmitted without alerting potential attackers or eavesdroppers.
- **Digital Watermark:** A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal.
- **Use by terrorists:** Steganography on a large scale used by terrorists, who hide their secret messages in innocent, cover sources to spread terrorism across the country. It come in concern that terrorists using steganography when the two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption" were published in newspaper.

D. Features of Image Steganography

1) *Transparency*: The steganography should not affect the quality of the original image after steganography.
2) *Robustness*: Steganography could be removed intentionally or unintentionally by simple image processing operations like contrast or enhancement brightest gamma correction, steganography should be robust against variety of such attacks.
3) *Data payload or capacity*: This property describes how much data should be embedded as a steganography to successfully detect during extraction.

III. Overview of Researches & Review of Literature

1. Least Significant Bit (LSB) Technique

The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR). In [12] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a stego -key. This private stego-key has 5 different gray level ranges of imageeach range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

Yang *et al.*, in [13] proposed an adaptive LSB substitution based data hiding method for image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the cover image to calculate the number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area k value remain small to balance overall visual quality of image. The LSB's (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. The overall result shows a good high hidden capacity, but dataset for experimental results are limited; there is not a single image which has many edges with noise region like 'Baboon.tif'.

In [14] anthers have proposed LSB based image hiding method. Common pattern bits (stego-key) are used to hide data. The LSB's of the pixel are modified depending on the (stego-key) pattern bits and the secret message bits. Pattern bits are combination of MxN size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. This technique targets to achieve security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because single secret bit requires a block of (MxN) pixels.

In the year of 2013 Akhtar, N.; Johri, P.; Khan, S., [15] implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. LSB method improving the PSNR of stegoimage. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving therobustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality.

In [16] Enhanced least significant bit method information is stored inside image but only in blue component part of each pixel to decrease distortion of image while storing of information inside image so that imperceptibility of Enhanced LSB will be low compared to simple LSB.

First information is translated into encrypted information using cryptography. In cryptography algorithm key and plain text message is translated into array of length of ascii character. After that text message is appended according to length of key. Then encrypted information is hidden inside image using pixel processing.

In [17] the Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the text messages is decided based on hash function. Hash function finds the position of least significant bit of each RGB pixel's. Then the Hash LSB technique uses the values provided by hash function to hide the data.

TABLE II. Comparison of Different Methods

Method	**Description**	**Advantages**	**Limitation**
Least Significant Bit (LSB) substitution	Data hides in least significant bit of the pixel.	1.High Capacity 2.simple to Implement	It has low robustness and pros to some attacks like low-pass filtering and compression.
Discrete cosine transform	Data is embedded by changing the coefficient of transform of image.	1. Compression is used to reduce bandwidth hence it is achieved by using quantization techniques. 2. High security and PSNR.	Large amount of Data cannot be hiding means smaller embedding capacity.
Discrete wavelet	Discrete wavelet	1.High capacity	1. The cost of

transform	transforms (DWT), which transforms a discrete time signal to a discrete wavelet representation.	2.high security and Robustness	computing DWT may be higher. 2. Low PSNR.
Spread Spectrum	In spread Spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect	In channels with narrowband noise, increasing the transmitted signal bandwidth results in an increased probability that the information received will be correct.	1. Improving the embedded signal estimation process in order to lower the signal estimation BER. 2. Medium Robustness and PSNR.
Hash-LSB	Hash function is used to find position of LSB.	Very good MSE and PSNR.	1.low robustness

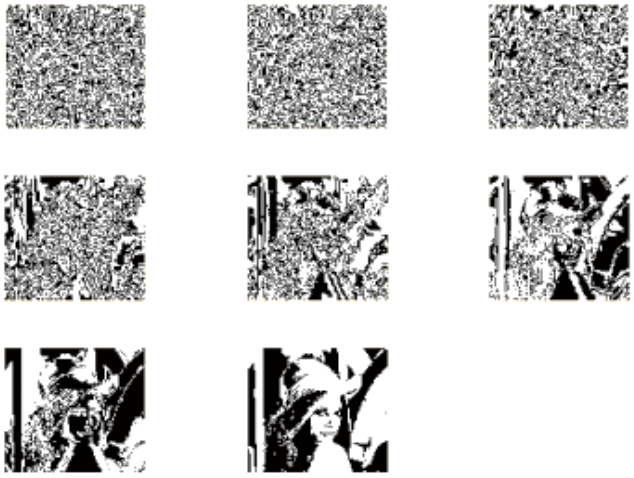

Fig. 3: Eight-bit plane slice view of an Image

As evident from Fig. 3 that shows 8-bit grayscale image when split into corresponding eight bit planes (from low order bits to higher order, in sequence) - lower order bits carry subtle (visual) details about an image in contrast to high order bits. Hence, changes made in the least order bits can seldom have an impact on image appearance in general but only when analysed in milieu of limitation of Human Visual System (HVS).

2. Pixel Value Difference (PVD)

In [18] author proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be estimated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. Proposed method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. So in this way the technique provide both larger capacity and high visual quality according to experimental results. This method is complex due to adaptive k generation for substitution of LSB.

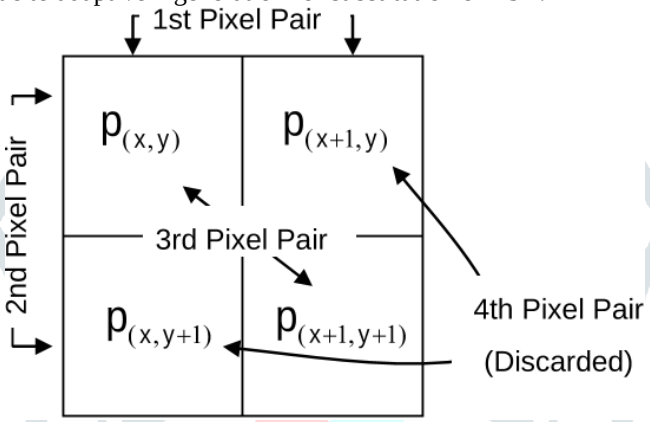

Fig. 4: PVD process (An example of Tri-way Pixel-Value Differencing)

In 2003, Wu and Tsai (2003) [19] proposed a data embedding method based on pixel value differencing (PVD). In this method, the difference of two pixels in the cover image is calculated. The number of bits to be embedded into these two pixels is determined by their absolute difference and a pre-defined range table. Since pixel pairs with larger difference are often located in complex regions, PVD embeds more data into pixel pairs with larger differences.

3. Integer Wavelet Transform (IWT)

In [20], author has proposed an image steganography technique that is based on Integer Wavelet Transform (IWT). In the proposed technique the cover is 256x256 color image, two grey scale image of size 128x128 as secret message. Single level IWT of secret message is obtained; the resultant matrix consists of LL, LH, HL, HH bands. The LL sub bands hide the secret message. The authors showed through the experiments that two secret images can be hidden in one color image. The average PSNR values obtained are much better than other methods.

Ramani, Prasad, and *Varadarajan* [21] propose an image steganography system, in which the data hiding (embedding) is realized in bit planes of *subband* wavelets coefficients obtained by using the Integer Wavelet Transform (IWT) and Bit-Plane Complexity Segmentation Steganography (BPCS).

4. Wavelet transform coefficients

In [22], author has proposed a block complexity analysis for transform domain image steganography. Author hasproposed an algorithm that is based on wavelet transform and bit plane complexity segmentation. The wavelet transform presentation of the cover is used to hide the secret message whereas the bit plane complexity segmentation is used as a measure of noisiness. The wavelet representation of an image is segmented in to 8x8 blocks and the capacity of each block is determined using BPCS. Author has also described various parameters which are associated with embedded image like PSNR, SSIM (Structural Similarity). The bit plane complexity images are obtained in embedding and extraction methods, which shows the improvement in the image quality.

A new algorithm based on WT to detect the starting point, ending point and the magnitude of the voltage sag is developed (*Gencer et al.*, 2010) [23]. DWT is used to detect fast changes in the voltage signals which allow time localization of differences frequency components of a signal with different frequency wavelets. WT is used to reformulate the recommended PQ levels (Morsi et al., 2010) [24]. The non-stationary waveforms are analyzed for the smart grid. An effective technique is proposed by using inter and inter-scale dependencies of wavelet coefficients to de-noise the waveform of PQ data for enhanced detection and time localization of PQ disturbances (Dwivedi et al., 2010) [25].

5. Discrete Cosine Transform (DCT)

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. In [26], author has proposed a robust steganography algorithm which is based on DCT, Arnold Transform and chaotic system. In embedding process , the cover image is transformed using DCT , to further increase the security data is

scrambled using Arnold transform, then the spreading is performed using chaotic sequences. The author has provided the concept of three keys, one for scrambling and two for generating chaotic sequences. In extraction process, inverse Arnold transform and inverse DCT is used. The experiment takes a host image which is first divided in to 4096 blocks of size 8x8, the cover image are 512x512 gray scale Lena, girl and Tank image . The logo is scrambled using Arnold transform. So the use of Arnold sequence increases the security level and algorithm is robust against the JPEG compression, addition of noise, low pass filtering and cropping operation as compared to other techniques. Thus the security is enhanced.

Milia Habib et. al (2015) a secure DCT steganography method is proposed. It allows hiding a secret image in another image randomly using Chaos. The chaotic generator Peace Wise Linear Chaotic Map PWLCM with perturbation was selected, it has good chaotic properties and an easy implementation. It was used to obtain the pseudo-random series of pixels in which the secret image will be embedded in their DCT coefficients. It enhances the LSB-DCT technique with threshold [27].

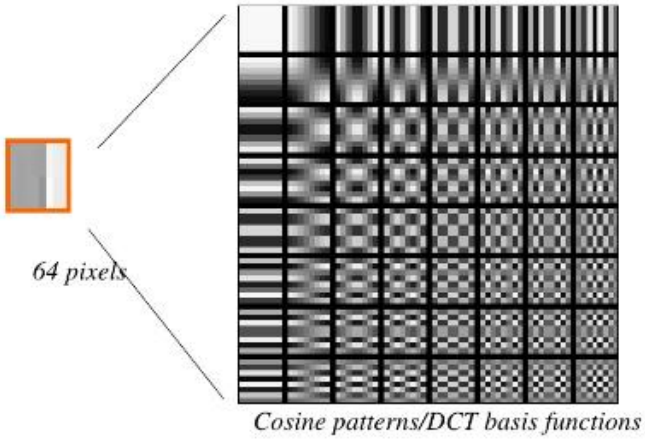

Fig. 5: Example of Discrete Cosine Transform (DCT)

6. Additional Spatial Domain Approaches

In [28], author has used various techniques like LSB, layout management schemes, only 0's and 1's are replaced from lower nibble from the byte and are considered for hiding secret message in an image. Author has also proposed various methods of data hiding based on the random bits of random pixels like replacing Intermediate bit, raster scan principle, random Scan principle, Color based data hiding, shape based data hiding. So, the techniques are analysed and it showed that the parameters responsible for noise in a cover image due to the hidden data depends on amount of data to hide, size of cover image, frequency of pixels available in an image, physical location of pixels.

In [29], a multiple base number system has been employed for embedding data bits. While embedding, thehuman vision sensitivity has been taken care of. The variance value for a block of pixels is used to compute the number base to be used for embedding. A similar kind of algorithm based on human vision sensitivity has been proposed by [30] by the name of Pixel Value Differencing. This approach is based on adding more amounts of data bits in the high variance regions of the image for example near "the edges" by considering the difference values of two neighboring pixels. This approach has been improved further by clubbing it with least significant bit embedding in [31]. According to [31], "For a given medium, the steganographic algorithm which makes fewer embedding changes or adds less additive noise will be less detectable as compared to an algorithm which

makes relatively more changes or adds higher additive noise." Following the sameline of thought Crandall [31] have introduced the use of an Error Control Coding technique called "Matrix Encoding".

7. Discrete Wavelet Transformation (DWT)

Hajizadeh et al. [33] proposed a block-based and high capacity steganographic method which is the extended form of Zhang and Wang's EMD method and it uses eight modification directions to hide multiple secret bits into a cover pixel pair at a time. In this method blocks are selected in a random order scheme of the image, to eliminate the bias between the image and the confidential data. Simulation results shows that the method can obtain various hiding capacities of 1 to 5 *bpp* and corresponding good visual qualities of either 53.68 to 30.05 dB or 52.97 to 29.40 dB in the case of 4 × 4 or 8 × 8 blocks, respectively.

TABLE 3. Comparison of Image Steganography Techniques

Lit. ref	Image Steganography technique	Description	Advantage
[20]	Integer wavelength transform	Conceal Multiple Secret Images And Keys In A Color Cover Image	Best Of PSNR Value Are Obtained And The Technique Is Simple To Implement
[22]	Wavelet transform coefficients	By Retaining The Integrity Of Wavelength Coefficients At High Capacity Embedding , Best Secret –Embedded Image Is Produced That Is Indistinguishable From A Human Eye	Bit Plain Complexity Produces The Best Quality Images
[32]	LSB, LZW(Limpel-ZivWelch, modified Kekre Algorithm(MKA)	LZW Pre-Processes The Data (Lossless Data Technique), Compression Technique Is Also Used To Increases The Efficiency. The Data Hiding Capacity Is Calculated In Bytes.	High PSNR Value And Low MSE (Mean Square Error) Value Results In To Good Quality Image
[26]	DCT, Arnold transform and chaotic sequences	Concept Of Three Keys, One For Scrambling Through Arnold Transform And Two Keys For Generating Chaotic Sequences, Along With The Concept Of DCT And IDCT For Extraction Process. Testing Is Done In The Presence Of JPEG Compression, Low Pass Filtering, Gaussian Noise Attack And Cropping Operation	Technique Is Very Secure, Provides Multilayer Security And Is Robust. Low Distortion Is Induced In The Cover Image
[28]	Spatial domain	Analysis Of Image Steganography Tools Is Performed And Parameters Of Image Are Considered Like Physical Location Of The Pixel, Intensity Value.	Noise Related Parameters Are Obtained Like Size Of Cover Image, Physical Location Of Pixel, Etc. These Parameters Can Produce More Robust And Secure Systems.

Saraireh [34] employs cryptographic algorithm together with steganography for provides high level of security, scalability and speed. In this method filter bank cipher is used to encrypt the secret text message then a discrete wavelet transforms (DWT) based steganography is employed to hide the encrypted message in the cover image by modifying the wavelet coefficients. The performance of the proposed system is evaluated using peak signal to noise ratio (PSNR) and histogram analysis. The simulation results show that, the proposed system provides high level of security. The results showed that, the PSNR of theproposed system are high, which ensure the invisibility of the hidden message through the cover image.

Shejul et al. [35] proposed a steganography method based on DWT using biometrics, the biometric feature used to implement steganography is skin tone region of images. The secret data is embedded within skin region of image that provides an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding is performed using frequency domain approach - DWT (Discrete WaveletTransform), Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding are applied by cropping an image interactively. Cropping results into an enhanced security than hiding data without cropping i.e. in whole image, so cropped region works as a key at decoding side. Also they [36] proposed a steganographic method based on biometrics and the biometric feature used to implement Steganography is skin tone region of images. Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. For data hiding two cases are considered, first is with cropping and other is without cropping. In both the cases different steps of data hiding are applied either by cropping an image interactively or without cropping i.e. on whole image. Both cases are compared and analyzed from different aspects. This is concluded that both cases offer enough security. Main feature of with cropping case is that this results intoan enhanced security because cropped region works as a key at decoding side. Whereas without cropping case uses embedding algorithm that preserves histogram of DWT coefficient after data embedding also by preventing histogram based attacks and leading to a more security.

Chen and Lin [37] embed the secret messages in frequency domain using discrete wavelet transformation. The algorithm is divided into two modes and 5 cases. Unlike the space domain approaches, 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. Some basic mathematical operations are performed on the secret messages before embedding. These

operations and a well-designed mapping Table keep the messages away from stealing, destroying from unintended users on the internet and hence provide satisfactory security.

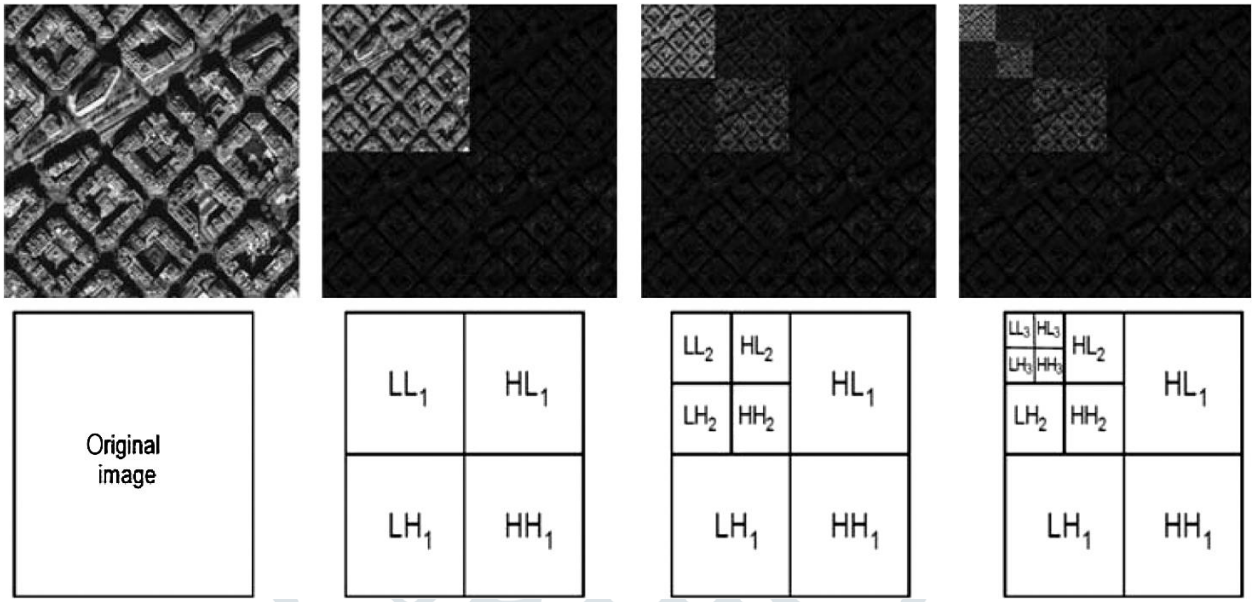

Fig. 6: Illustration of the three-level 2-D DWT decomposition of a satellite image

8. Skin color detection based Steganography

Danti et al. [38] used color quantization and chrominance-based segmentation for labeling skin pixels. Initially, a color clustering process is applied on the original image for extracting the set of dominant colors. This extracted set of colors is used to quantize the original image. Then, the quantized image is segmented according to the skin color characteristics. They used the YCbCr and the HSV color models in their experiments and obtained equivalent segmentation results from both. Another method for skin tone detection was proposed by *Lakshmi et al.* [39]. They combined YCbCr and HSI color spaces along with Canny and Prewitt edge detection for locating skin patches. They use skin tone detection prior to steganography.

Skin tone detection methods are extensively used as a preprocessing step for face detection. But their use for data hiding in skin regions is relatively new. Cheddad et al.

[40] proposed a color space that utilizes the luminance in detecting skin and non-skin pixels. The proposed color space contains error signals derived from differentiating the grayscale map and the non-encoded-red grayscale version. According to their work, *Cheddad et al.* [41] used skin tone detection for producing a skin-map which dictates the embedding process where to hide. Then, they used Discrete Wavelet Transform DWT for transforming the Y channel of the host image and then hiding in the third LSB of the coefficients of the approximation image according to the skin-map. In addition, they used Binary Reflected Gray Coding (BRGC) for representing the integer part of the coefficients during embedding.

Fig. 7: Binary results for original images (left column) and their corresponding skin detection images (right column)

Bhoyar et al. (2010) proposed a novel algorithm for region (skin) based steganography based on two output layer neurons: one each for skin and non-skin class [42]. The aim of using a single neuron network classifier is to improve the separability between these two classes.

III PERFORMANCE SPECIFICATION OF IMAGE STEGANOGRAPHY

There are several important issues to be considered when studying steganographic systems. They are steganographic robustness, capacity, and security. The relationship between them can be expressed by the steganography triangle, which is shown in Figure 2. It represents a balance of the desired characteristics associated with asteganographic method. In order to improve one element, you have to sacrifice one or both of the other two elements. For instance, in order to improve capacity, you sacrifice security. This is logical since inserting hidden information to some degree is the same as tampering with an image. The more you tamper with an image, the more probable that an observer will notice the degradation and suspect something is out of place. Each element is described below.

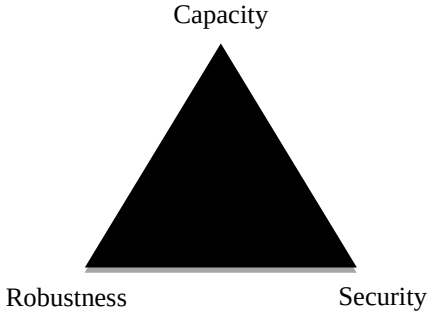

Figure 2. The steganography triangle

Robustness refers to an embedded message's ability to survive either deliberate attack by a suspecting third party or the random corruption of noise during some phase of the transmission process. If a secret message is able to survive when a carrier image

moderately degraded, then the steganographic method is said to be very robust. However, it is most desired that the embedded content be fragile so as to reduce the possibility that an interceptor would be able to reassemble the embedded message.

Capacity refers to the maximum number of bits which could be embedded in the image, while the obtained *stegoimage* remains undetectable and visually intact. The *coverimage* used to create a stego-image is acting as an information channel with which the embedded message is transferred. Like any other information channel, an important property of a stego channel is its capacity. *Shannon* defines the capacity of an information channel as the maximum achievable rate, with which error free transmission could be achieved. But capacity of steganography channel has a number of additional constraints.

Firstly, the stego channel needs to be undetectable by definition. In other words, the statistical properties of the stego and cover image need to be indistinguishable. The second constraint on the capacity of stego channel is that the stego channel should preserve the properties of the cover channel.

The fundamental characteristic of steganography is its ability to offer a means of communication without suspicion. Security is the ability of an embedding carrier to remain undiscovered. The whole purpose of steganography, unlike other forms of communication, is defeated by the detection of communication between the sender and the receiver. Therefore, the first requirement of a steganographic system is its *undetectability*. In other words, a steganographic system is considered to be insecure, if the warden is able to differentiate between cover-image and stego-image. *Cachin* has defined a steganography technique to be ε-secure if the relative entropy of the probability distribution of cover-object and stego-object is less than or equal to ε. A steganography technique is perfectly secure if ε is zero. It is demonstrated that there do exist steganographic techniques that are perfectly secure. However, it should be noted that classical definition of steganography is statistical and not perceptual.

V. Conclusion

Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate secretly. With the rapid development of digital technology and internet, steganography has advanced a lot over the past years. Accordingly, the steganalysis developed quickly. In this review paper, we present an overview and review of techniques involved in steganography and steganalysis based on digital image.

However, steganography and steganalysis are still at an early stage of research. With the rapid development of steganography, steganalysis are facing new challenge. There are several problems needed to be investigated in steganography and *steganalysis* based on digital image. Notion of security and capacity for steganography needs to be investigated deeply. Steganography and corresponding steganalysis using image models needs to be further investigated.

The paper describes a short survey on diverse types of steganography techniques for image in spatial and transform domains Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large assortment of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one system lacks in payload capacity, the other lacks in robustness. Thus, researchers can decideon which steganographic algorithm to use, depending on the type of application they want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.

VI. References

[1] Simmons, G., "The prisoner's problem and the subliminal channel", CRYPTO, 1983.

[2] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[3] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[4] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[5] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000.

[6] Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", Proceedings of the 2nd Information Hiding Workshop, April 1998.

[7] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004.

[8] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.

[9] Steganography and Digital Watermarking, Copyright © 2004, Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham.

[10] N. Johnson and S. Jajodia, exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February (1998).

[11] E Lin, E Delp, a Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS'99), Savannah, Georgia, April 25-28, (1999).

[12] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method with Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, **(2010)** March 1.

[13] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radio engineering, vol. 18, no. 4, **(2009)**, pp. 509-516.

[14] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, **(2009)**.

[15] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, vol., no., pp.385, 390, 27-29 Sept. 2013.

[16] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, "Enhanced Least Significant Bit Algorithm for Image Steganography.", International Journal of Cyber-Security and Digital Forensics 4, Volume 15, July 2012.

[17] Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique". International Journal of Computational Science & Software Engineering, Volume 3, 2013.

[18] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. **(2008)** September 3, pp. 488-497.

[19] Da-Chun Wu a, Wen-Hsiang Tsai, A steganographic method for images by pixel-value differencing, Elsevier, 2003.

[20] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, "a secure and high capacity image Steganography technique" Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, February 2013.

[21] K. Ramani Dr. E. V. Prasad Dr. S. Varadarajan, Steganography using bpcs to the integer wavelet transformed image, IJCSNS International Journal of Computer Science and Network Security, Vol .7, No.7, July 2007.

[22] Gowtham dhanarasi and Dr. A. Mallikarjuna Prasad, image steganography using block complexity analysis, International Journal of Engineering Science and Technology (IJEST) Vol. 4 July 2012.

[23] Gencer Ö, Öztürk S, Erfidan T (2010). A new approach to voltage sag detection based on wavelet transform. Int. J. Elect. Power Energy Syst. 32(2):133-140.

[24] Morsi WG, El-Hawary ME (2010). Novel power quality indices based on wavelet packet transform for non-stationary sinusoidal and nonsinusoidal disturbances. Electric Power Syst. Res. 80(7):753-759.

[25] Dwivedi UD, Singh SN (2010). Enhanced detection of power-quality events using intra and interscale dependencies of wavelet coefficients. IEEE Trans. Power Deliv. 25(1):358-366.

[26] Siddharth Singh and Tanveer J. Siddiqui, "A Security Enhanced Robust Steganography Algorithm for Data Hiding" IJCSI International Journal of Computer Science Issues, Vol. 9, May 2012.

[27] Milia Habib, Bassem Bakhache, Dalia Battikh, Safwan El Assad "Enhancement using chaos of a Steganography method in DCT domain", 2015.

[28] Dipesh Agrawal, Samidha Diwedi Sharma, "Analysis of Random Bit Image Steganography Techniques" International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013).

[29] D.C. Wu, and W.H. Tsai, "A Steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, Jan. 2003, pp. 1613–1626.

[30] S. Dumitrescu, X. Wu, and N. Memon, "On steganalysis of random lsb embedding in continuous-tone images" in Proc. IEEE International Conference on Image Processing, Rochester, New York., September 2002.

[31] Piyush Goel "Data Hiding in Digital Images: A Steganographic paradigm" Indian Institute of Technology Kharagpur, May, 2008

[32] Rahul Jain and Naresh kumar, "Efficient data hiding scheme using lossless data compression and image steganography", International Journal of Engineering Science and Technology (IJEST), Vol. 4 No.08 August 2012.

[33] Hajizadeh, Hamzeh, Ahmad Ayatollahi, and Sattar Mirzakuchaki. "A new high capacity and EMD-based image steganography scheme in spatial domain." In Electrical Engineering (ICEE), 2013 21st Iranian Conference on, pp. 1- 6. IEEE, 2013.

[34] Saraireh, Saleh. "A SECURE DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGANOGRAPHY." International Journal of Computer Networks & Communications 5, no. 3 (2013).

[35] Shejul, Anjali A., and Umesh L. Kulkarni. "A DWT based approach for steganography using biometrics." In Data Storage and Data Engineering (DSDE), International Conference IEEE, 2010.

[36] Shejul, Anjali A., and Umesh L. Kulkarni. "A secure skin tone based steganography using wavelet transform." International Journal of computer theory and Engineering 3, no. 1 (2011): 16-22.

[37] Chen, Po-Yueh, and Hung-Ju Lin. "A DWT based approach for image steganography." International Journal of Applied Science and Engineering 4, no. 3 (2006): 275-290.

[38] A. Danti, K. M. Poornima and Narasimhamurthy "Detection of multiple faces in color images using haar wavelets," in international conference on VLSI, communications and instrumentation, 2011.

[39] H. C. V. Lakshmi and S. P. Kulkarni "Face detection for skintone images using wavelet and texture features," in international journal of computing science and communication technologies, 2011.

[40] A. Cheddad, J. Condell, K. Curran, P. M. Kevitt "A new color space for skin tone detection," in 16th IEEE international conference on image processing ICIP, pp. 497 – 500, 2009.

[41] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt "A skin tone detection algorithm for an adaptive approach to steganography," in signal processing, vol. 89, pp. 2465-2478, 2009.

K. K. Bhoyar and O.G. Kakde, Skin color detection model using neural networks and its performance evaluation, Journal of Computer Science, vol. 6, no. 9, pp. 963-968, 2010