International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Image Steganography: Critical Findings through Some Novel Techniques

Farooq Nabi, M. Mazhar Afzal

Abstract: ***Word 'Steganography' is originated from Greekand has been used in several forms for 2500 years which is a art of hiding confidential data in any digital manner in such a way that no one can concealed it. It has found practise in various section like in military, government, diplomatic, medical, personal and intelligence agencies. This survey paper put the light on the basic of image steganography along with its different techniques and sub-techniques. Cover selection with recent trend ROI (region Of Interest) is highlighted. In addition, different types of Image file used in image steganography and performance parameter are discuss well.***

Index Terms: Image Steganography, Cover Selection, PSNR.

I.INTRODUCTION

Steganography is an emerging field in security which is derived from a Greek word meaning covered writing. Steganography is the study of hiding data in such a manner so that no one can predict about it except sender and receiver. It gives an alternate idea for hiding the credential data unlike cryptography (Table 1) where the messages are hiding with encryption and not visible to the world. Nowadays, using a combination of steganography and the other methods, such as cryptography, information security has improved considerably. Many intelligent algorithms based on soft computing, such as Fuzzy Logic (FL), Adaptive Neural Networks (ANN), Genetic Algorithms (GA) are being used in Steganography to achieve robust and optimal solutions.[10].

Basically Steganography contains three components i.e. carrier, data and the key. The carrier may be any medium like audio, video, digital images, TCP/IP packets etc. and it contains the secret message. A key can be any password or pattern that is used to code/decode the hidden message [33]. Steganography deals with all types of data, be it text, image, audio or video [43]. Image Stegnography, a technique for hiding data with the use of image thereby giving a secure and safe way to exchange the data over Internet. Figure 1 describes well about the discipline of security information.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Mr. Farooq Nabi, Research Scholar, Department of Computer Engineering, Glocal University, Saharanpur, Uttar Pradesh, India.
E-mail: drmir1987@gmail.com
Dr. M. Mazhar Afzal, Research Guide, Associate Professor & HOD of Computer Engineering Glocal University Saharanpur, Uttar Pradesh, India.
E-mail: mazhar@theglocaluniversity.in

Table 1. Comparison between steganography and Cryptography [5][9]

Attributes	Steganography	Cryptography
Transformation information into a form incomprehensible to third parties	Yes	Yes
Carrier	Any digital media	Usually text based, with some extensions to image file
Hiding information	Yes	No
Key usage	Yes	Yes
Hiding the fact of communication	Yes	No
Ensuring the anonymity of communicating parties	Yes	No
Flexibility	Free to choose any suitable cover	N/A
The amount of information transmitted in the communication process	Much greater than the amount of encrypted information	Comparable to the amount of encrypted information
Additional carrier needed	Yes	No

1.1. Background of Steganography

The art of steganography exist since ancient times in several forms and has a long and fascinating history. Kahn [24], S. Katzenbeisser[26] and J.C. Judge [22] has wrote a complete account of the steganography. In ancient Greece, to send message secretly they used wax-covered tablet i.e. write a message and then use wax above it. In order to receive the message, recipient removes the wax again[17]. In the 5th century BCE, Histaiacus, a Greek tyrant who was in prison of king Darius, send a message to his son-in-law by shaved a salves head, tattooed a message on his scalp and send him after hairs grew back [17][9]. In 550 A.D., the Italian mathematician Jerome Cardan [9] proposed a method, named Cardan Grille, for secret writing where he used a paper mask with holes. He kept it over a blank paper and compose his secret message through the holes then removes the mask and receiver fills the blanks in order

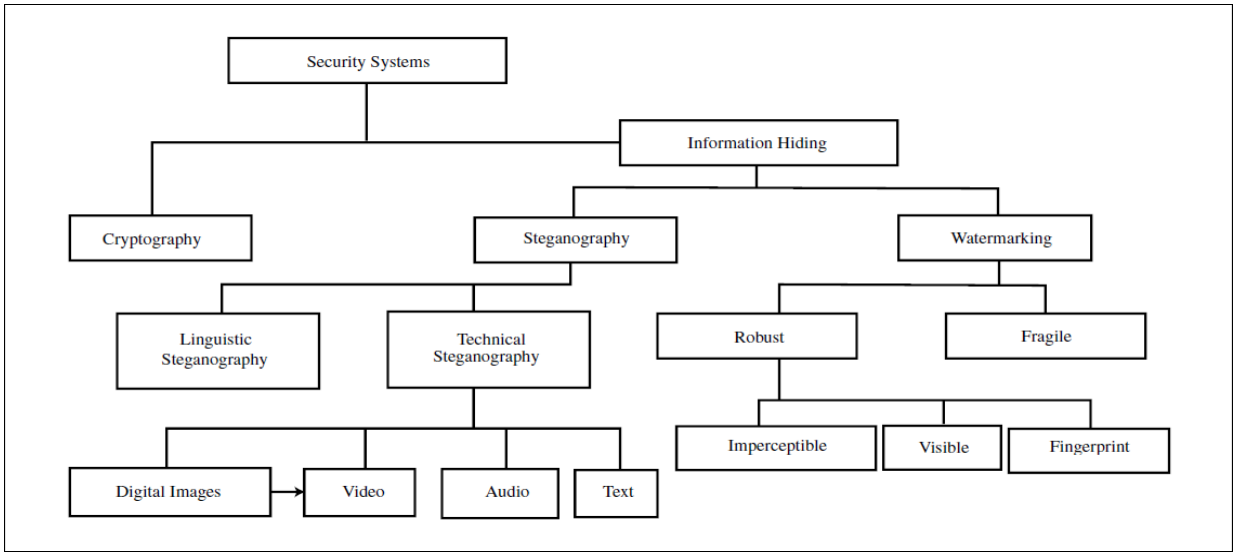

Figure 1. An overview of Security Systems [41]

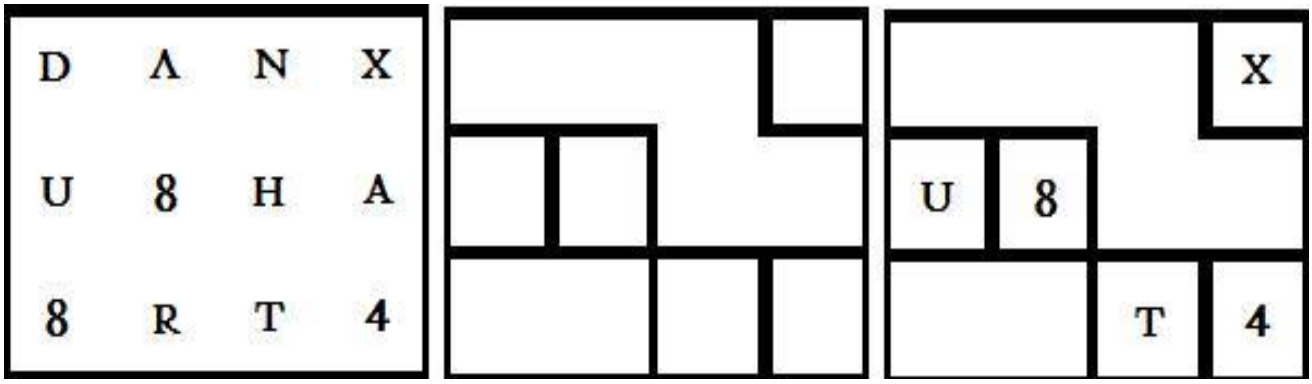

Figure 2. An illusteration of Cardan Grille method

To get text message.Figure 2 illustrate this method.

During World War I, the Germans communicated se-cretly using a sequence of characters and words referred as null cipher [11] In World War II microdot technique, which is very difficult to judge, used by German people and Invisible ink were used for hiding the data in invisible manner [17]. Linguistic Steganography were also used as a poem or stanza in which certain letters, generally the first in each line, build a motto, message or name when recite in sequence[26].

1.2. Basic Terms in Image Steganography

Cover Image: - The image in which the secret data are embedded is acknowledge as cover image.

Stego Image: - The image after embedding secret data is referred as stego image.

cover medium + embedded message = stego message

Payload: - The secret data that is embedded in coverimage is known as payload.

Payload capacity: - The embedding rate per pixel. Stegokey: - In order to get the embedded message from the stego image, some piece of secret information is needed, this is acknowledge as stegokey [13].

Figure 3 defines the generic process of embedding and extraction of secret message in image steganography.

1.3. Applications of Image Steganographic

Every Technique has its application and Image Steganography is not different from it. There exist adequate application of image steganography. Initially it was favorite to use as unobtrusive communications at military and intel-ligent agencies [26]. Later, due to its anonymity and covert nature people adopted it in their personal communication i.e. to communicate privately and secretly with a person over Internet with security such that no intruder can inspect the invisible communication [17]. Sharing of top secret or high level documents between international governments is one of the legitimate use. Government agencies use it to store critical data including illicit records. Copyrights [9] of a book or other things can be secured using image steganography. Smart Identity cards [27] contain personal information which is embedded into images and this is a emerging field in India due to Unique Identification Author-ity of India (UIDAI) program (that gather the demographic and biometric data of habitants, store them in a database, and assign a 12-digit unique identity number called Aadhaar to each habitant) Smart City etc. programs. The Commercial aspect of steganography is digital fingerprinting and water-marks that are used to track the ownership and copyright of electronic media [23].

M Ramesh et al[36] proposed an algorithm related to Quick Response Code (QR-code) that QR-code will have secret message and the QR code is hidden into Discrete Wavelet Transform (DWT) that include encoding and decoding op-erations. Preet Kamal et al [25] has explain about Medical image steganography where it has all details of patient.

It has many others authentic and legitimate uses. In same

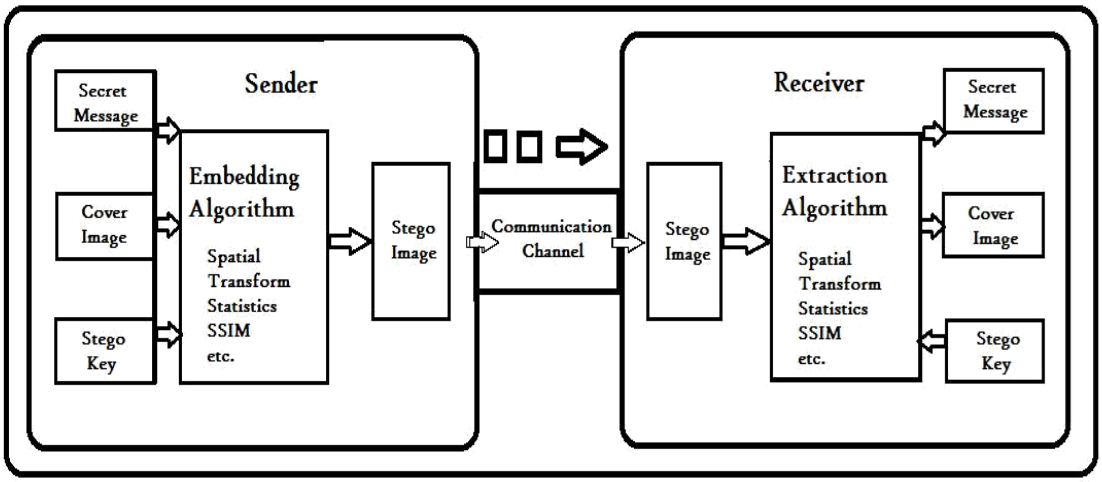

Figure 3. Generic process of Image Steganography

Manner, it may be quite nefarious and evil as some hackers can send Trojan or viruses. Also, some terrorists and sep-aratist group plan their illegal activities using hidden and covert communication process for security purpose. [33].

II.COVER SELECTION

Cover image is the basic needed element to start im-age steganography. The images used for hiding the secret message are referred as cover image and the cover image should be elect and prefer with the intelligence. It should be large enough than the message that we are going to hide in it [21]. More importantly it should be satisfy two basic goals [41]. First is that it should not reveals anything or it should provide good security so that no one can suspect about the secret message. The other goal is to maximize the payload capacity. A scads of research over cover selection for image steganography has been done to achieve these basic goals and other attributes like robustness, security etc. Region of Interest (ROI) is the concept that help better result than earlier selection method. It select a particular area in cover image for embedding the data and provide good result too. Selection of appropriate cover image and algorithm can enhance the embedding rate and payload capacity of that cover image. Edlira Martiri et.al [32] proposed a medical certificate authentication by embedding the metadata into the region of interest in the image using AES encryption technique. The metadata contains all information of patient like patient name, Id, date etc. Songtao Wu et al [47] proposed an idea that by selecting suitable cover images it is very hard to detect the stego image. To do this, they used Fisher information matrix and Gaussian Mixture model for selecting the cover image. However, ROI has not exploited much till now. Mansi et al [41] has explain ROI under future directions tag.

2.1. IMAGE FILES

Image Steganography is entirely related to selection of the type of image as cover image and each type behave differently while embedding the secret data. Some image format leave signature while some doesnt. Thus, this section is a brief overview of image file and its reflected steganogra-phy characters. The main types are JPEG, GIF, BMP, PNG, TIFF and JPEG 2000. Lossless images are preferable for the embedding of data.

2.2. JPEG

JPEG are common web friendly image type as it support about 16 million rich colors [1]. However this is lossy because many information are lost while image steganography. After compression JPEG tends to create artifacts. In spite of these, lossy compression are useful when it discards the information that are unnoticeable by human eyes and it saves storage space. Due to lossy nature of JPEG, earlier it was not considered good for steganography but F5, Outguess, JSteg/JPHide etc. are based on JPEG format and offers good hiding. DCT is used for JPEG for the transformation.

2.3. GIF

GIF are lossless image and these are 8-bit palette. It replaces redundancy/multiple occurring pattern into one. It is good for embedding as it does offer lossless compression and due to this factor we can reconstruct the original image from the compressed image [4].

1. http://1stwebdesigner.com/image-file-types/

2.4. BMP

BMP images are large and uncompressed image that of-fer high payload capacity and need good image steganogra-phy technique. For hiding small data BMP are not preferable as cover image.

2.5. PNG

PNG images are next version of JPEG but with superi-ority i.e. lossless unlike JPEG. Due to its lossless nature the image can be reconstruct back from stego image. It can't be animated and it backs RGB, indexed colors and gray-scale. [48] influence and detriment like, Spatial approach is good for embedding capacity but it is not good in security. So, we will have a look over different techniques, its advantages and disadvantages.

2.6. JPEG2000 / JPEG2K

A lot of work has been done on JPEG and JPEG2K type images. The main drawback of JPEG was its lossy nature that JPEG2K solves successfully.

JPEG2K gives both lossy and lossless image with higher quality.
Even in lossy phase it gives high quality image and keeps same level of details as original file high compression ratios [2]. JPEG2K images are based on wavelets stream and it offers Region Of Interest (ROI) i.e. the use of wavelets allow to select one region of an image and then perform all action upon it.
Lokeswara et al[37] has explain the behavior of LSB technique with various file formats, table 2 as below:-

Table 2. Comparison of lsb techniques for various file

Attributes	FORMATS[37] LSB in BMP	LSB in GIF	LSB in PNG
Percentage distortion, less	High	Medium	High
resultant image Invisibility	High	Medium	Medium
Steganalysis Detection	Low	Low	Low
Image manipulation	Low	Low	Low
Amouny od embedded data	High	Medium	Medium
Payload capacity	High	Medium	Medium
Independence of file format	Low	Low	High

III.SPATIAL TECHNIQUE

Spatial technique, also avowed as substitution technique, is the simplest technique and it deals with the change in the bit pattern of an image. The pixel value are directly embedded in the cover image. There are several methods like LSB technique, Gray level modification, Pixel Value Difference, Quantization, Multiple Base Notational System (MBNS) and Prediction based.

IV. IMAGE STEGANOGRAPHY TECH-NIQUES

As already discuss, image steganography is hiding the data through the image and various approach exist for it. Some basic approaches are spatial technique, Discrete Co-sine Transform (DCT), Discrete Wavelet Transform (DWT), Spread spectrum, Statistical based steganography, Distortion technique etc. These techniques offer different leverages,

2. http://www.verypdf.com/pdfinfoeditor/jpeg-jpeg-2000-comparison.htm

4.1. LSB Technique

This is a straightforward and uncomplicated technique for hiding the data or secret message in an image. It embed the data at right-most bit i.e. least significant bit (LSB) position. Mainly there are two kind of images 8-bit and 24-bit (RGB). The former support 256 colors and later support 256*256*256= about 16 million different colors and ordinarily LSB deals with RGB image.

E.g.Let's suppose that to hide the message bits 10101011 in an image whose pixel are 10110001 11001101 11101110 10001100 10001001 11111111 11001100 101010101. Then the output we will have 10110001 11001100 11101111 10001100 10001001 11111110 11001101 101010101. Here, the each single message bit are replacing rightmost value of the image pixel.

This method is known as Sequential LSB and it is smooth and effortless to implement. However it does not provides good payload capacity due to only one bits of message bit per pixel. Additionally, it can be detected easily by intruder. The equation 1 for embedding process of LSB is [29]

$$Y_i = 2|X_i/2| + m_i \quad (1)$$

Where m_i is the i^{th} message bit, x_i and y_i are the i^{th} selected pixel value before embedding and after embedding respectively.
Neil F. Johnson and Stefan C. Katzenbeisser [26] de-scribes the embedding and extraction algorithm for sequen-tial LSB substitution as:-

Algorithm 1 Embedding Algorithm for Sequential LSB

procedure START
For i = 1....l(c) do
$s_i \leftarrow c_i$
End for
For i = 1...,l(m) do
compute index ji where to store i^{th} message bit
$s_{ji} \leftarrow c_{ji}$ m_i
End for
end procedure

Algorithm 2 Extraction Algorithm for Sequential LSB

procedure START
For i = 1....l(M) do
compute index ji where the i^{th} message bit is store $m_i \leftarrow LSB(c_{ij})$
End for
end procedure

According to Stefan C. Katzenbeisser [26] l(C) > l(m) i.e. the cover size should be greater than message size so that the message can be embed conveniently in cover image. As embedding process is over, this particular portion of cover image gets changed and the rest part of the cover image will be unchanged. So, first portion of cover image will have different statistics than rest of the cover image due to embedding of the message bits. This is a serious security issue in Selective LSB.
An attempt is made to overcome this issue through the random selection at the cover image for embedding. This mechanism is referred as Random or scattered LSB [17] and it offers more payload capacity [29]. Neil F. Johnson and Stefan C. Katzenbeisser describes [26] the embedding and extraction algorithm for random LSB substitution as:-

Algorithm 3 Embedding Algorithm for Random LSB

procedure START
For i = 1....l(c) do
$s_i \leftarrow c_i$
End for
Generate random sequence k_i using seed k
$n \leftarrow k_1$
For i = 1...,l(m) do
$s_n \leftarrow c_n$ m_i
$n \leftarrow n + k_i$
End for
end procedure

Algorithm 4 Extraction Algorithm for Random LSB

procedure START
$n \leftarrow k_1$
For i = 1....l(m) do
$m_i \leftarrow LSB(C_n)$
$n \leftarrow n + k_i$
End for
end procedure

Loannidou et al [20] proposed a method that sharp areas can hide large amount of data if it is applied at edge image and it cannot hide more data when it works at smooth images. Odai et al [1] proposed an algorithm based on different size image segmentations (DSIS) and modified least significant bits (MLSB), where the DSIS algorithm has been applied to embed a secret image randomly instead of sequentially. There are various tools for LSB like Steghide, S-tools, steganos, stegoDos, Ez-stego, Hide and Seek etc [26].

4.2. Gray Level

As LSB uses 24-bit images and provide good embedding capacity, Gray level uses 8-bit images and it support 256 distinct shades of gray [21]. Gray level resolution refers to smallest discernible change in the shades or levels of gray in an image. The darkest color is the black and the lightest gray range is white color. The detection of grayscale is more difficult than color detection by human eyes. The main advantage of gray level method is low computational complexity and it offers good embedding capacity.
There is a close relation 2 between bits per pixel (bpp) and gray level resolution as

$$L = 2^k \quad (2)$$

Where L means number of gray levels and k is the bpp. For example consider 256 level image, we have 256 different shades and each pixel carry 8 bits. Figure 4 shows the effect of reducing the gray level of the image [3].

4.3. Pixel Value Differencing

Pixel Value Differencing (PVD) was proposed by Wu and Tsai [46] that deals with the difference between neigh-bour pixel values [41]. The pixel value difference at edge portion is more than at smooth portion. At edge portion the embedding process returns less distortion in the image and Human Visual System (HVS) is not good to judge the change at edges while at smooth portion, the disparity between neighbour pixels is less so it is not ideal for large data embedding [42][41].
This method provides better stego image respecting to LSB as it modify the pixel value of adjacent/neighbor of cover image unlike direct modification in pixel value of cover image.
There exist two different modified version of PVD [43] viz Tri-way pixel value differencing (TPVD) method [7] and Adaptive pixel value differencing (APVD) method [31]. For embedding PVD is based on single direction while TPVD is based on three dimension pixels. The three dimension are horizontal, vertical and diagonal and APVD is applicable to gray scale images.

4.4. Multiple Base Notational System

As we know binary system is the language of computer and it is of base 2 that store all information in the combi-nation of 0 and 1. In image steganography, the secret data or messages are converted into symbols in binary system. If we increment the base then we can embed more data i.e. secret data hiding capacity in the pixel can be increase with increment of base.
Secret data are transformed into symbols in a notational

3. https://www.tutorialspoint.com/dip/concept of quantization.htm

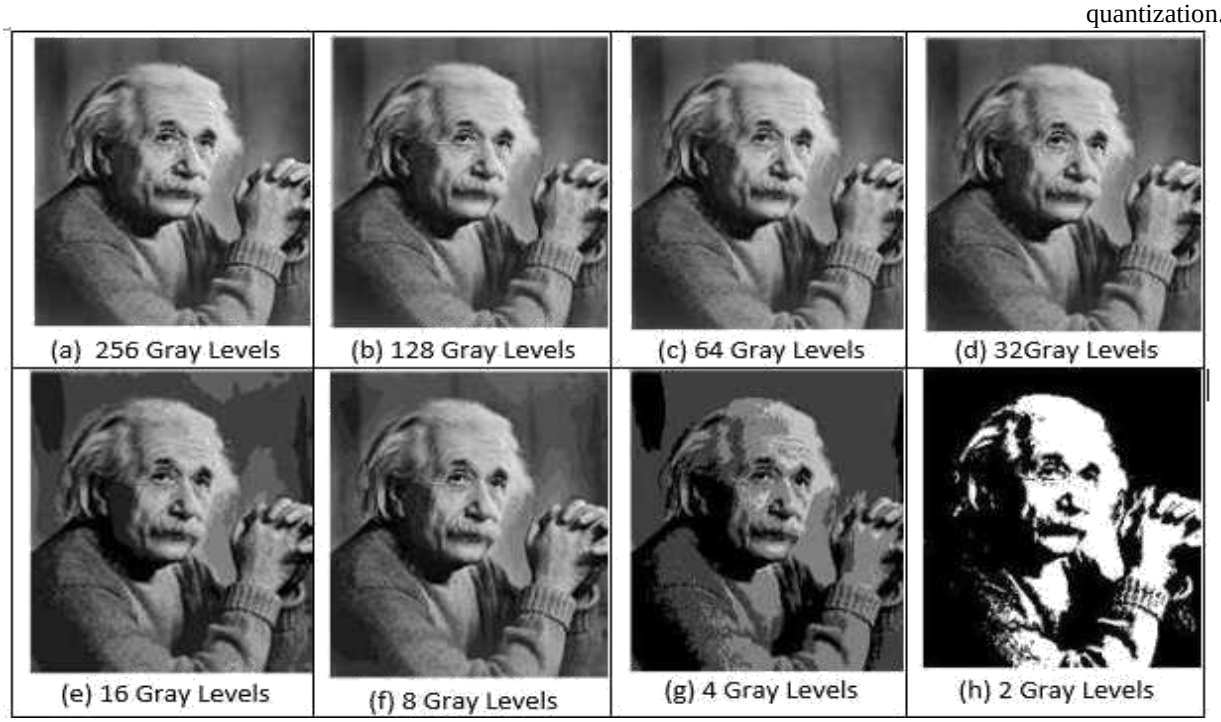

Figure 4. The image has been distorted badly by reducing the gray levels initiating from 256 levels to 2 levels which looks black and white image

System with multiple bases and in host images, the pixel are modified in such a way so that when it is divided by bases, it gives the remainder equal to the symbols [41]. Both data embedding and data extraction process are done on the basis of modulo operation, thereby also known as modulo operation based steganography [29]. It gives better Peak Signal to Noise Ratio (PSNR) value which is a quality measure metric of image after compression.

4.5. Palette Based Embedding

Palette eembedding is done mostly on GIF type images with maximum 256 colors [2] [42]. In this technique a palette table of the used colors is maintained. The palette table is used to hide the secret data. It does not depend upon size of the image so payload capacity is limited by palette size.
Jiri Fridrich [14] proposed a method of embedding one message bit into one pixel. The selection of pixel is randomly chosen using a pseudo-random number generator seeded with a secret key. After embedding one message to each pixel, the palette is used to the find out closest color and it should have same parity as the message bit and does not that of original color. This idea gives advantage that reduce the embedding effect. This method have low payload capacity and produces less distorted image after embedding [2].

4.6. Pixel Indicator Technique

Pixel Indicator Technique (PIT) was proposed by A. Gutub [16]. This is a key-less steganography approach and it uses 24 bits per pixel RGB images. This method uses two LSB bits of any one channel out of Red, Green and Blue channels as an indicator of secret data that gives the details of message existence in other two remaining channels. Considering R, G and B there will be exist six combinations as RGB, RBG, GRB, GBR, BRG and BGR. On the basis of images and its properties the indicator LSB bits will be available randomly. The relation between indicator and channel is shown in table 3 .

Table 3. Indicator values based action

Indicator Channel	Channel1	Channel2
00	No hidden data	No hidden data
01	No hidden data	2 bits of hidden data
10	2 bits of hidden data	No hidden data
11	2 bits of hidden data	2 bits of hidden data

Suppose, if we select the Red as indicator channel then Green and Blue will be channel 1 and channel 2 respectively. Same sequence will be followed for all six combinations. The first 8 bytes of the cover image delineate the com-mencement of the indicator channel sequence and will be used to store the size of the concealed message assuming that it is enough to store and will consume all LSBs of RGB component. Table 4 is used to select the indicator choice as 1st level and data hiding channel as 2nd level. All combinations of RGB are obtained from the table 4 on the basis of size of the message (N). If it is even then R is the indicator channel and GB or BG options will be chosen according to parity bit of N.

Table 4. Indicator channel selection criteria

Type of length (N) of secret message	1st Level selection, indicator channel	2nd Level selection	
		Odd Parity	Even Parity
Even	R	GB	BG
Prime	B	RG	GR
Else	G	RB	BR

Ankit Chaudhary et al [8] approaches key-less steganography to increase the confidentiality of data and and storage capacity with minimal degradation of the image by distributing the secret message throughout the image.

4.7. Distortion Technique

Distortion techniques are mainly used with text steganography. However they are also good for image steganography. It has two phases namely encoding phase and decoding phase [17]. In encoding phase, the sender marks changes in the cover image in order to get a stego image and in decoding phase, the receiver reconstruct cover image from stego image in order to get message and cover image. Now, the receiver needs original cover image so that he can make comparison between both cover images (original and extracted image). If both cover images matches then the message he got is correct otherwise message is corrupt [45][35].

V.TRANSFORM DOMAIN TECHNIQUE

In Transform steganography the pixel value of image is transformed into frequency value. The frequency value has three frequency components i.e. low frequency, high frequency and medium frequency. The low frequency area represent coarse information of the signal [21] and it is not good for embedding the message. The high frequency domain represent edge components and sharp transitions. High frequency domain are good for embedding as they are not noticeable to human eye [41]. It embed the message in such areas where message are less exposed [10]. Various transform techniques are: Discrete Cosine Transform (DCT), Wavelet Cosine Transform (WCT).

5.1. Discrete Cosine Transform

DCT coefficients [4] are used for JPEG compression. It divides the images into 8*8 matrices representing pixel values and then subtract 128 by each pixel value that will return a matrices with mostly negative values. Now use DCT formula (Equation 3) for getting a matrix of DCT coefficients.

$$D(i,j) = \frac{1}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} p(x,y) \cos\left[\frac{(2x+1)i\pi}{16}\right] p(x,y) \cos\left[\frac{(2x+1)j\pi}{16}\right] \quad (3)$$

The Quantization table, which is a default table, use it as a divisor to the DCT coefficient matrix that will produce 8*8 matrices known as Quantized DCT coefficient that gives a sparse matrix contains 44 zeros out of 64 matrix value. Zero means elimination of less important details from the high frequency region. Confidential messages are encoded in quantizes DCT coefficient followed by compression of the quantized coefficients by applying lossless method RLE (Run-Length Encoding), DPCM (Differential Pulse Code Modulation) and Huffman. The image is already compressed and lost many less important information, now there is need of lossless compression. So, RLE is used to compress the high frequency coefficients and DPCM is used to compress the first low frequency coefficient portion. Finally Huffman algorithm is implemented to compress everything [5].For an image suppose the pixel values is matrix A (4) then the following steps from matrix-equation (4) to (8) explains the procedure of DCT.

b) Values after subtracting 128 from matrix values.

$$A = \begin{bmatrix} -415 & -30 & -61 & 27 & 56 & -20 & -2 & 1 \\ 5 & -22 & -61 & 10 & 13 & -7 & -9 & 5 \\ -47 & 7 & 77 & -25 & -29 & 10 & -5 & 6 \\ -49 & 12 & 34 & -15 & -10 & 6 & 2 & 2 \\ -7 & & & -4 & & & & \\ 12 & -13 & & -2 & & 21 & -3 & 3 \\ & & & -6 & & & & \\ -8 & 3 & 2 & -2 & & 1 & 4 & 2 \\ -1 & 0 & 0 & -2 & -1 & -3 & 4 & -1 \\ -0 & 0 & -1 & -4 & -1 & -0 & 1 & 2 \end{bmatrix} \quad (6)$$

(c) DCT coefficients:- Matrix after applying DCT formula. All matrix value are in rounded form, i.e. omit the number after decimal.

$$A = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix} \quad (7)$$

(d) Quantization table.

$$A = \begin{bmatrix} -26 & -3 & -6 & 2 & 2 & -1 & 0 & 0 \\ 0 & -2 & -4 & 1 & 1 & 0 & 0 & 0 \\ -3 & 1 & 5 & -1 & -1 & 0 & 0 & 0 \\ -3 & 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (8)$$

(e) Quantized DCT coefficients.

Algorithm 5 DCT algorithm

procedure
Input: Cover image and secret message
Output: Stego Image
While end of secret image file do
read adjacent f(i,j) of cover image
if f(i,j) = 0 and f(i,j) = 1 then
get adjacent LSB of secret image
replace DCT LSB with secret image bit
end if
insert f(i,j) into stego image **end while**
end procedure

Major DCT based steganography methods are Jsteg, JPHide, F series, Outguess, YASS and Model Based.

$$A = \begin{bmatrix} 52 & 55 & 61 & 66 & 70 & 61 & 64 & 73 \\ 63 & 59 & 55 & 90 & 109 & 85 & 69 & 72 \\ 62 & 59 & 68 & 113 & 144 & 104 & 66 & 73 \\ 63 & 58 & 71 & 122 & 154 & 106 & 70 & 69 \\ 67 & 61 & 68 & 104 & 126 & 88 & 68 & 70 \\ 79 & 65 & 60 & 70 & 77 & 68 & 58 & 75 \\ 85 & 71 & 64 & 59 & 55 & 61 & 65 & 83 \\ 87 & 79 & 69 & 68 & 65 & 76 & 78 & 94 \end{bmatrix} \quad (4)$$

(a) Pixel values of the image.

$$A = \begin{bmatrix} 76 & 73 & 67 & 62 & 58 & 67 & 64 & 65 \\ 65 & 69 & 73 & 38 & 19 & 43 & 59 & 56 \\ 66 & 69 & 60 & 15 & -16 & 24 & 62 & 55 \\ 65 & 70 & 57 & 6 & -26 & 22 & 58 & 59 \\ 61 & 67 & 60 & 24 & 2 & 40 & 60 & 58 \\ 49 & 63 & 68 & 58 & 51 & 60 & 70 & 53 \\ 43 & 57 & 64 & 69 & 73 & 67 & 63 & 45 \\ 41 & 49 & 59 & 60 & 63 & 52 & 50 & 34 \end{bmatrix} \quad (5)$$

- Jsteg/JPHide:- Jsteg and JPHide are two classic tools that employ LSB embedding technique. Jsteg function, which is the first algorithm for JPEG images [28], is used to hide the secret data by replacing the LSBs of non-zero quantized DCT coefficients by secret message bits [41]. It does not replace any coefficients of 0s or 1s. Matrix (9) shows Jsteg matrix after change in coefficient values (indicating by *) in quantized DCT coefficients matrix values.

$$A = \begin{bmatrix} -26 & -4 & -6 & 2 & 1 & -2 & 0 & 0 \\ 0 & -3 & -4 & 1 & 1 & 0 & 0 & 0 \\ -4 & 1 & 5 & -2 & -1 & 0 & 0 & 0 \\ -3 & 1 & 1 & -2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (9)$$

Due to changes in values it produce abnormal histogram that help in steganalysis.
It resists visual attacks but chi-square attack, a statistical attack, thatdetect the presence of message bits. JPHide conceal the secret message with quantized DCT coefficients and these quantized coefficients are selected randomly by pseudo-random number generator. It is capable to modify the second LSB [17].

- F series (F3, F4 and F5):- F series does not change bits rather do increment / decrement of the coef-ficient values. In F series, F5 is possibly one of the most progressive and advanced program publicly available and it was introduced by Westfield [41] in 2001. It uses JPEG format and distribute messages across entire image. Table 5 shows a comparative study among F3, F4 and F5 . Figure 5 explains the encoding process of the F5.

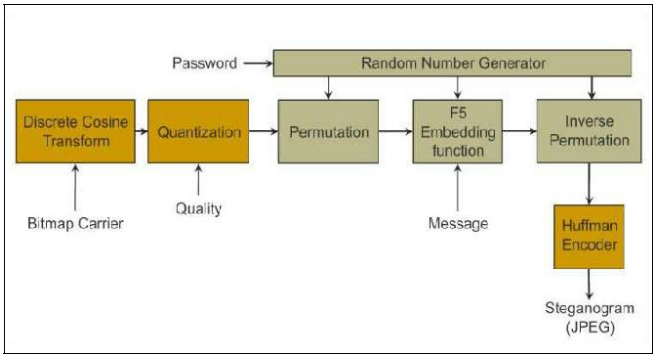

Figure 5. F5 encoding process

- Outguess: - It was introduce by Niels Provos[34] and works as 2-step procedure. First step selects the DCT coefficients randomly using pseudo-random generator and improve the embedding statistics and replaces the DCT LSB with message and while em-bedding keeps skip 0s and 1s. Second step, modifica-

Table 5. An overview of f series algorithm

No	F3	F4	F5
1	Resistant to visual attacks	Resistant to visual attacks	Resistant to visual attacks
2	Does not change Bits	Does not change bits	Does not change bits
3	Detectable by chi-square attack	Not detectable by chi-square attack	Not detectable by chi-square attack
4	Abnormal Histogram that makes steganalysis easy	Normal Histogram that makes steg-analysis difficult	Normal Histogram that makes steg-analysis difficult
5	Due to decrement to zeros, it shrinkage	Skips zeros, so no shrinkage	Skips zeros, so no shrinkage
6	It produces more even coefficient than odd	Uses inverse of negative stego values	Uses inverse of negative stego values
7	Decrement the co-efficient absolute values except zero which it can not does.	Decrement pos-itives and incre-ment negative coefficients	Decrement pos-itives and incre-ment negative coefficients

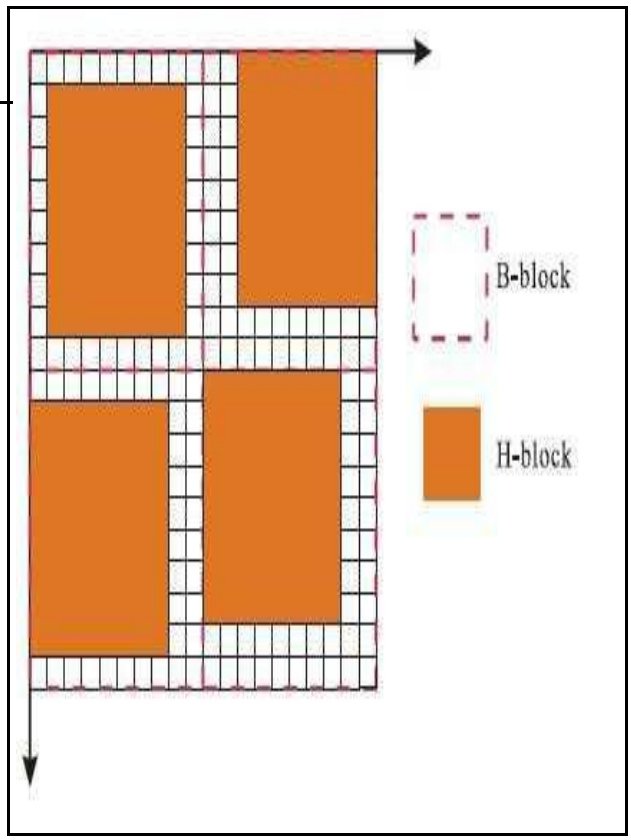

Figure 6. Design of B-Blocks and H-Blocks [29]

5.2. Discrete Wavelet Transform (DWT)

tions are made to the unselected coefficients to main-tain the DCT coefficient histogram of stego image as that of cover image [29]. Before embedding, for the first step, Outguess compute the maximum size of a randomly spread message for embedding purpose so that user can modify and adjust the values in histogram near to original values during the second step. It maintains the good histogram shape, due to which it is one of safe method that is not detectable by chi-square attack [17].

• YASS (Yet Another Steganographic Scheme) :-This is one of the least statistically detectable embedding scheme in recent years. Its working is different from F series algorithm as it does not embed the message bits directly in DCT coefficient rather it divides the whole image into fixed and large in size, non-overlapping B*B (B>8), known as Big-Block or B-Block. Figure 6 shows that In each B-block, a 8*8 sub-block known as Host Block or H-Block is selected randomly with some secret key for computing DCT [41] [29][6]. And, Next Error correction code are applied for the embedding of secret data in the DCT coefficients of the H-blocks. Finally, inverse DCT is applied to the H-blocks, the entire image is compressed and distributed as a JPEG image [17]. Due to non-overlapping H-blocks it produce good JPEG DCT coefficient instead of artifacts produced during embedding [29].

Finally, a comparison (table 6) is made among var-ious DCT techniques and Chi-square detected all previous methods before YASS successfully. For the security performance of YASS, refer to [30][19] for further study.

It is a mathematical tool for decomposing an image in a hierarchically manner. It is an application of the wavelet transform using a discrete set of the wavelet scales [6]. It is better than Fourier Transform as it captures frequency and temporal information both [7]. Also, it overcome DCT as it produce high compression ratio and avoids interferences due to artifacts. So, DWT is a better approach for hiding the secret data [3].JPEG2k is related to wavelet transform [27]. It decompose image in 4-non overlapping sub bands as LL (Low Low), LH (Low High), HL (High Low), HH (High High). This is 1st level decomposition. To get next level decomposition, we proceed LL sub-band in order to get next value of wavelets coefficients until reach some final states N (figure 7). In general or mathematically we will have total 3N+1 sub-bands with LLX, LHX, HLX, HHX where X=1 to N [21][10]. Algorithm 6 and 7 describe the process of embedding and extraction for DWT method [3][10]

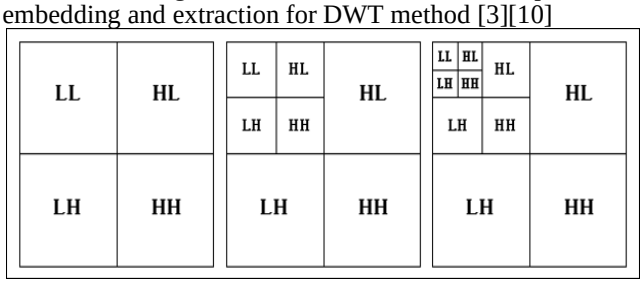

Figure 7. Single level, Two level and Three level Decomposition

6. http://klapetek.cz/wdwt.html _ _
7. https://en.wikipedia.org/wiki/Discrete wavelet transform

Table 6. Comparison among dct techniques[9][28][38][34][40]

Methods	Creator	Year	Image Format	Complexity	Random Bit Selection	Detected by
JSteg	Derek Upham	1993	JPEG	Medium	No	Chi-square, Fidirich's algorithm, Stegdetect
JPHide	Allan Latham	1999	JPEG	Medium	Yes	Chi-square, Stegdetect
F5	Andreas Westfield	2001	JPEG	High	Yes	Fidirich's algorithm
Outguess	Provos & Honeymoon	2003	JPEG	High	Yes	Chi-square extended version, Stegdetect
YASS	K Sloanki, A Sarkar, BS Manjunath	2007	JPEG	High	Yes	——-

Algorithm 6 Embedding Algorithm of DWT

procedure

input: Cover image and secret message.

Step 1: Break up the RGB cover image into three planesR, G and B.

Step 2: Decompose each plane of the cover image into 4sub-bands LLX, LHX, HLX and HHX until 3N + 1. **Step 3**: Divides the planes by Haar DWT method.

Step 4: Now decompose secret image in four sub-bandsuntil 3N + 1.

Step 5: Secret image sub-bands are embedded in thedifferent bands of the cover image.

Step 6: Apply inverse DWT to retrieve them and combinethree planes to get stego images.

end procedure

Algorithm 7 Extraction Algorithm of DWT

procedure

input: Stego Image.

Step 1: Decompose stego image in three planes i.e. R, Gand B.

Step 2:Apply 2D-DWT on each stego plane and get sub-bands.

Step 3: To get wavelet coefficients use Haar DWT.

Step 4:Now apply IDWT to combine all three planes.

Step 5: Get the secret message.

end procedure

5.3. Integer Wavelet Transform

Integer Wavelet Transform (IWT) gives lossless com-pression image while embedding. In DWT process, the floating point coefficients are generated and DWT filters it and gives lossy output but IWT does not because it maps integer to integer in the output [21]. Hemalatha et al[18] proposed a secure way to hide data in an image using the key and IWT is used to hide the key. M.Vijay et al[44] proposed a way to embed the data in gray level cover image using IWT and they got a good result with high PSNR value.

VI.SPREAD SPECTRUM IMAGE STEGANOGRAPHY

Spread spectrum Image Steganography (SSIM) is a mechanism used for generating signals [8] as the spread spectrum generates a noise in cover image and then planted secret message into it results decreasing density. The secret message is spread throughout the cover image and the message bits are embedded in such signals that have low noise than cover image that makes imperceptible and unnoticeable for human beings [21]. It is fairly robust and dont disturb the message after transformation that adds noise to the image and due to its robustness against detection it is commonly used in military communications. It is hard for intruder to know the embedded message without knowing the keys generated by pseudo random number generator during encoding phase. [13]. The general additive embedding scheme 10 can be described as follows:

$$Y_i = X_i + W_i \quad i = 1, 2, ...N \qquad (10)$$

Where Xi is a sequence of the original data from the cover, Wi is a pseudo-random sequence generated from a pseudo-random number generator (PRNG) initialized by a secret stego key, is an embedding strength parameter (gain factor), and Yi is a sequence of possibly altered data [17].

VII.STATISTICAL BASED STEGANOGRAPHY

Statistical method, also familiar as model based tech-nique, was proposed by P. Sallee [39] a special case of steganography apart from earlier both Spatial method and transform method. In LSB method the distortion in image after embedding process is generally not detectable by HVS but it changes the statistical properties of the stego image that led to the abnormal histogram followed by ease in detection while steganalysis and F5 method base on matrix was considered as first data hiding method with minimum distortion was not having freedom to select the position for embedding. So, this method first seizures the statistical prop-erties of the cover image then embedding steps are carried out accordingly by making some modifications in statistical properties of the cover image. The modifications are made by splitting the cover image, suppose X, into two distinct parts as X_A is invariant to embedding and X_B will carry the secret messages followed by 1-bit embedding method. The cover image will be change due to 1 bit embedding otherwise it remains unchanged[17].

8. https://en.wikipedia.org/wiki/Spread spectrum

Table 7. Comparison among different image steganographic techniques

Techniques	Domain	Imperceptibility	Robustness	Payload Capacity	Detectability	Image Distortion	Complexity
LSB Pseudo-rendom	Spatial	Low [42]	Low [21]	High [42]	High [27]	Medium [12]	Low [27]
LSB	Spatial	Low [21]	Medium	High [15]	medium	Medium [12]	Low [27]
PVD	Spatial	High [21]	Low [21]	High [21]	Medium [27]	Medium	Medium [2]
Palette	Spatial	High [17]	Low [17]	Low [2]	High	Low	High [2]
Distortion	Spatial	Low [17]	Low	Low	Low	Low [12]	Low
DFT	Transform	High [17]	Medium [21]	Medium [21]	Low [27]	High	Medium [27]
DCT	Transform	High [15]	Medium [21]	Medium [21]	Low [27]	High [12]	Medium [27]
DWT	Transform	High [15]	High [15]	Low [21]	Low [27]	Medium [12]	High [27]
SSIS	Spread Spectrum	High [17]	High [15]	medium [21]	Low [27]	Medium	Medium [27]
Statistics	Model based	Medium [17]	Low	Low [17]	Low	Low	High

VIII.COMPARISON AMONG IMAGE STEGANOGRAPHY TECHNIQUES

So far, we have discussed various ways to hide the secret message within an image. Table shows a summary of main techniques. These comparisons are based on differ-ent parameters and these technique will behave differently according to input. It depends upon the selection of cover image that should be enough large to hold the data. Also, the distortion of cover image depends upon the length of em-bedded message. A long message will return more distortion than a short message. However, the embedding algorithms matters more, the statistical base method offers maximum message size embedding without distortion in image while LSB method returns distortion in in images. There is no such thing as a 'best' algorithm rather it matters with cover selection, message size and users output.

IX.PERFORMANCE PARAMETER

The performance parameter is an important aspect to judge the efficiency and optimization of a technique. The performance of Image Steganography is related to the high payload capacity, imperceptibility, and robustness [17].
The different metrics to measure the efficiency of techniques are PSNR, MSE, SSIM, normalized cross relation etc. These metrics describes the robustness of stego image i.e. up to what extent the cover image has been distorted.

9.1. MSE

Mean Square Error 11 is the average of squares of the errors.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]2 \qquad (11)$$

Where I(i,j) represents original image and K(i.j) represents stego image. m and n represents the size of the image
The smaller MSE, the image quality will be higher or Image quality of stego image is inversely proportional to MSE. It gives positive values always due to squaring of the errors. And, values toward zero is better.

9.2. PSNR

Peak Signal to Noise Ratio is well known performance measurement matric that compute the peak signal to noise ratio between two images i.e. original image and the com-pressed image. The PSNR value is directly proportional to image quality i.e. the larger the value of PSNR the high will be quality of stego images. It means there is a minimum deviation in stego images from cover image [3]. PSNR is inversely proportional to MSE as given in equation 12.

$$PSNR = 10\log_{10} \frac{R^2}{MSE} \qquad (12)$$

Where R is the maximum fluctuation in the input image data type. The MSE shows the cumulative squared error between the original and the compressed image, whereas PSNR represents a measure of the peak error. A high quality stego image should have 40 dB value or above and below 30dB is referred as low quality image [9].

9.3. SSIM

Structural Similarity Index Matrix is recognized for video steganography but works well for photography. It is visible structural based perceptual metric used to ad-vance the conservative methods PSNR and MSE [3]. While processing image compression, it quantifies image quality degradation by calculating the similarity between two im-ages 13.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C1)(2\sigma_{xy} + C2)}{(\mu_x^2 + \mu_y^2 + C1)(\sigma_x^2 + \sigma_y^2 + C2)} \qquad (13)$$

Where X and Y represent cover and stego image re-spectively. σ_x and σ_y are mean intensity of x and y respectively.σ_x^2andσ_y^2 represent variance for x and y. C1 and C2 are two variables that stabilizes the division with weak denominator.

9.4. Normalized Histogram intersection

The frequency distribution of different pixel intensities of an image is said to be Histogram and it is denoted by ha(g)i.e. total number of pixels hain the image with inten-sity g. This metric is used to calculate the value of matched pixel between two histograms. Consider two histogram h(a) and h(b) of cover image A and stego image B respectively then histogram intersection is defined as 14:

$$I(A,B) = \sum_{i=1}^{N} \min((h(a), h(b)) \qquad (14)$$

A score 1 indicates both histograms are normalized and have a good match while 0 score indicates complete mismatch and no regions of histogram overlap [12].

9.5. Cross Correlation

This parameter defines the how well the neighbour pixels are co related to each other. It gives a comparison between original images and stego images. The process of data embedding may produce a disturbance in the correlation in an image.

X.CONCLUSION AND FUTURE DIRECTION

Security and covert is an important anxiety for the people over Internet and Image Steganography provide security well. It does not proposed to replace the cryptography but supplement it and appendage the security. Due to its outstanding nature of security it has infinite number of applications. This paper also introduce many techniques of image steganography with outline and each technique is has its nice impact according to conditions.
In term of adequate security, best technique is DWT with high robustness while without security LSB offers more payload capacity with simple complexity. Due to high robustness, low ease of detection and good payload capacity SSIS is very good for steganography. Distortion method carry less distortion in stego-image. For 8-bit image, Gray level method offers good payload with low complexity.
Capacity and security trade-off is an important concern in embedding the message. It has been observed that both are reciprocal to each other. Advancing or increasing in security leads to reducing in capacity factor and vice versa. A stego method is needed with optimal performance in both fields.
Many researchers has given idea to mingle it with cryptography in order to reach impregnable security. Strong encryption algorithm like 3DES (Data Encryption Standards), Twofish, AES (Advanced Encryption Standard) with image steganography can shield circumvent credential data. To make it more complicated, use Diffie-Hellman algorithm for generating key agreement between two parties for communication. As we know there are generally four type of steganography viz. Text, Images, Audio / Video and protocol. A hybrid of these methods can be seen as future work. With the rapid advancement and development of data hiding technologies aggrandize payload capacity, superlative security are perpetual demand and welcome. To improve steganography algorithm a variety of topic can be considered such as ROI, soft computing algorithm, etc.

Image steganography works rely mostly on RGB or the gray scale images. The other color spaces like CMY (Cyan Magenta Yellow) YCbCr (Yellow Blue-Chromaticity Red-Chromaticity), HSV (Hue, Saturation,Value) share very less amount of work related to it.

It has been notice that Hue component of HSV returns less image distortion while embedding. So the use of these color spaces are yet to be dig in more depth for image steganography.[38]

However image steganography is not optimal in each and every aspects and it has its certain limitations that makes researcher to do more work and extend its shielding power.

REFERENCES

1. O. M. Al-Shatanawi and N. N. E. Emam, "A new image steganography algorithm based on mlsb method with random pixels selection," *International Journal of Network Security & Its Applications*, vol. 7,no. 2, p. 37, 2015.
2. D. Anandpara and A. Kothari, "Working and comparative analysis of various spatial based image steganography techniques," *InternationalJournal of Computer Applications*, vol. 113, no. 12, 2015.
3. D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel dwt based image securing method using steganography," *Procedia Computer Science*, vol. 46, pp. 612–618, 2015.
4. K. Bailey and K. Curran, "An evaluation of image based steganography methods," *Multimedia Tools and Applications*, vol. 30, no. 1, pp. 55–88, 2006.

A. Bhardwaj and S. Som, "Study of different cryptographic technique and challenges in future," in *Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on*. IEEE,2016, pp. 208–212.

5. V. H. Bhat, S. Krishna, P. D. Shenoy, K. Venugopal, and L. Patnaik, "Steganalysis of yass using huffman length statistics," *InternationalJournal of Hybrid Information Technology*, vol. 4, no. 3, pp. 15–30,2011.
6. K.-C. Chang, C.-P. Chang, P. S. Huang, and T.-M. Tu, "A novel image steganographic method using tri-way pixel-value differencing," *Journal of multimedia*, vol. 3, no. 2, pp. 37–44, 2008.

A. Chaudhary and J. Vasavada, "A hash based approach for secure keyless image steganography in lossless rgb images," in *Ultra ModernTelecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on*. IEEE, 2012, pp. 941–944.

7. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signalprocessing*, vol. 90, no. 3, pp. 727–752, 2010.
8. J. Desai, S. Hemalatha, and S. Shishira, "Comparison between dct and dwt steganography algorithms," *International Journal of AdvancedInformation Science and Technology (IJAIST)*, vol. 24, no. 24, pp.51–55, 2014.
9. Desoky, "Normals: normal linguistic steganography methodology," Journal of Information Hiding and Multimedia Signal Processing,vol. 1, no. 3, pp. 145–171, 2010.
10. S. Dhall, B. Bhushan, and S. Gupta, "An in-depth analysis of various steganography techniques," *International Journal of Security and ItsApplications*, vol. 9, no. 8, pp. 67–94, 2015.
11. M. Fortrini, "Steganography and digital watermarking: A global
12. view," *University of California, Davis. Available: http://lia.deis. unibo. it/Courses/RetiDiCalcolatori/Progetti00/fortini/project. pdf.[June 2011]*, 2000.
13. J. Fridrich, "A new steganographic method for palette-based images," in *PICS*. Citeseer, 1999, pp. 285–289.
14. S. Goel, A. Rana, and M. Kaur, "Comparison of image steganography techniques," *International Journal of Computers and DistributedSystems*, vol. 3, no. 1, pp. 20–30, 2013.
15. A.-A. Gutub, "Pixel indicator technique for rgb image steganography," Journal of Emerging Technologies in Web Intelligence, vol. 2, no. 1, pp. 56–64, 2010.
16. N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *International Journal ofComputer Science and Security (IJCSS)*, vol. 6, no. 3, pp. 168–187,2012.
17. S. Hemalatha, A. Renuka, U. D. Acharya, and P. R. Kamath, "A secure image steganography technique using integer wavelet transform," in *Information and Communication Technologies (WICT), 2012 WorldCongress on*. IEEE, 2012, pp. 755–758.
18. F. Huang, Y. Q. Shi, and J. Huang, "A study on security performance of yass," in *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on*. IEEE, 2008, pp. 2084–2087.
19. Ioannidou, S. T. Halkidis, and G. Stephanides, "A novel technique for image steganography based on a high payload method and edge detection," Expert systems with applications, vol. 39, no. 14, pp. 11 517–11 524, 2012.
20. N. Jambhekar, C. Dhawale, and R. Hegadi, "Performance analysis of digital image steganographic algorithm," in *Proceedings of the2014 International Conference on Information and Communication Technology for Competitive Strategies*. ACM, 2014, p. 82.
21. James, "Steganography past, present, future," *URL: http://www.sans. org/reaing room/whitepapers/steganography/steganogaphy past*
22. *present future 552. pdf (: 12.12. 2009)*.
23. N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.
24. Kahn, *The codebreakers*. Weidenfeld and Nicolson, 1974.
25. P. Kamal and G. Jindal, "Review of different steganographic techniques on medical images regarding their efficiency," 2005.
26. S. Katzenbeisser and F. Petitcolas, *Information hiding techniques forsteganography and digital watermarking*. Artech house, 2000.
27. H. Kaur and J. Rani, "A survey on different techniques of steganog-
28. raphy," in *MATEC Web of Conferences*, vol. 57. EDP Sciences, 2016.
29. J. Kodovsky and J. Fridrich, "Quantitative structural steganalysis of jsteg," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 681–693, 2010.
30. B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," *Journal of Information Hiding and MultimediaSignal Processing*, vol. 2, no. 2, pp. 142–172, 2011.
31. B. Li, J. Huang, and Y. Q. Shi, "Steganalysis of yass," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 369–382, 2009.
32. J. Mandal and D. Das, "Steganography using adaptive pixel value differencing (apvd) of gray images through exclusion of overflow/underflow," *arXiv preprint arXiv:1205.6775*, 2012.
33. Martiri, A. Baxhaku, and E. Barolli, "Steganographic algorithm injection in image information systems used in healthcare organizations," in *Intelligent Networking and Collaborative Systems (INCoS),2011 Third International Conference on*. IEEE, 2011, pp. 408–411.
34. N. Nabavian, "Cpsc 350 data structures: Image steganography," *nabavl00@ chapman. edu*, 2007.
35. N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, 2003.
36. R. Radhakrishnan, K. Shanmugasundaram, and N. Memon, "Data masking: a secure-covert channel paradigm," in *Multimedia SignalProcessing, 2002 IEEE Workshop on*. IEEE, 2002, pp. 339–342.
37. M. Ramesh, G. Prabakaran, and R. Bhavani, "Qr-dwt code image steganography," *International Journal of Computational Intelligenceand Informatics*, vol. 3, pp. 9–13, 2013.
38. V. L. Reddy, A. Subramanyam, and P. C. Reddy, "Implementation of lsb steganography and its evaluation for various file formats," *Int. J.Advanced Networking and Applications*, vol. 2, no. 05, pp. 868–872,2011.
39. R. Roy, S. Changder, A. Sarkar, and N. C. Debnath, "Evaluat-ing image steganography techniques: Future research challenges," in *Computing, Management and Telecommunications (ComManTel),2013 International Conference on*. IEEE, 2013, pp. 309–314.
40. P. Sallee, "Model-based steganography," in *International workshopon digital watermarking*. Springer, 2003, pp. 154–167.
41. K. Solanki, A. Sarkar, and B. Manjunath, "Yass: Yet another steganographic scheme that resists blind steganalysis," in *International Workshop on Information Hiding*. Springer, 2007, pp. 16–31.
42. M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer science review*, vol. 13, pp. 95–113, 2014.
43. P. Thomas, "Literature survey on modern image steganographic techniques," in *International Journal of Engineering Research andTechnology*, vol. 2, no. 5 (May-2013). ESRSA Publications, 2013.

44. M. C. Trivedi, S. Sharma, and V. K. Yadav, "Analysis of several image steganography techniques in spatial domain: A survey," in *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*. ACM,2016, p. 84.
45. M. Vijay and V. Vignesh, "Image steganography method using integer wavelet transform," in *International Journal of Innovative Research inScience, Engineering and Technology, IEEE International Conference on Innovations in Engineering and Technology (ICIET14)*, vol. 3,no. 3, 2014, pp. 1207–1211.
46. M. Weiss, "Principles of steganography," 2012
47. D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9, pp. 1613–1626, 2003.
48. S. Wu, Y. Liu, S. Zhong, and Y. Liu, "What makes the stego image undetectable?" in *Proceedings of the 7th International Conference onInternet Multimedia Computing and Service*. ACM, 2015, p. 47.
49. W. W. Zin, "Message embedding in png file using lsb steganographic technique," *International Journal of Science and Research (IJSR)*, vol. 2, no. 1, pp. 227–230, 2013.

AUTHORS PROFILE

Mr. Farooq Nabi, received his Bachelors Degree [BCA] from university of Kashmir Srinagar J&K, India, and Master of Computer Application [MCA] from university of Kashmir, Srinagar, India, he also holds a post graduate diploma in cyber law from university of Kashmir, he also authored a book on e-commerce, He has done his Master of Philosophy [M.PHIl] and now currently pursuing doctorate of philosophy [PHD] In computer science from Glocal university Saharanpur, UP, India. his research interests include survey on image steganography, cryptography and encryption algorithms, Internet on things (IOT), Information security and cyber laws.

Dr. M. Mazhar Afzal, is an Associate Professor and head of the Computer Science Department at Glocal University, where he has been since 2015. From 2008 to 2013 he served at a Government University at KSA. After Completing his Masters in Computer Science in Year 1997 he served at Department of Computer Science Maulana Azad college, Aurangabad for nearly a decade. He received his PhD from Dr. Babasaheb Ambedkar Marathawada University Aurangabad (MS). His research interests span both Internet Governance and Network Security. Much of his work has been on improving the understanding, design, and performance of Security systems and various cryptographic techniques. In the networking arena, he has worked on characterizing the Internet and the World Wide Web. In addition he is always keen on improving and imparting modern methods of teaching and imparting knowledge. He also Served various academic bodies at different capacities. Additionally he is also working as Director (IQAC) at Glocal University.