© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A New Approach for Image Steganography Using Edge Detection Method for Hiding Text in Color Images Using HSI Color Model

Vandana Yadav, Sanjay Kumar Sharma
Department of Computer Science & Engineering Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

ABSTRACT

The objective of the present project is to uses a new techniques for steganography in a HSI color cover images, which hides secret message in the edges of the carrier images using 2-bit LSB substitution for embedding. To get true edges, canny edge detection technique has been used. Amount of data to be embedded plays an important role on the selection of edges. The main advantage of using HIS color mode is that it produces a image with a significantly larg file size hence we hide large amount of secrete message Experimental results have shown that the proposed technique performs better and higher embedding capacity.

Keywords: HSI colo Model, True Edge, 2-bit LSB, Image Steganography, Edge Detection, Hiding Text.

I. INTRODUCTION

Steganography word is derived from the Greek words, the stegos importance cover and grafia significance composing both are characterizing it as secured composition. Image steganography is only to hide the data in images. The science and art of secret communication is by steganography. The secret communication is finished by encoding or embedding secret data in such a way such, to the point that the invisibility of presence of data is there.

The original files is referred as cover image, cover text or the cover audio. After secret message insertion it is alluded as stego-medium. By the use of stego-key, the process pf hiding or encoding to confine location or the extraction of embedded data.Nowadays, digital communication needs has been increased tremendously and this helps to come about the web has turned out to be extremely fundamental means for more effective and faster communication to digital communication. In the meantime, the data which are accessible in the web has turned out to be more powerless to make it copyright infringement, protection, espionage, and so forth. Which requires secret communication. Hence, a new domain dedicated to data security has evolved and this also called data hiding. The novel idea steganography in the field of information hiding which traces its previous history from its origin.

In present, steganography categorize in different medium such as audio, video, images, or text file to secretly hide any information in it therefore it does not illustrate any interest and hence looks like a safe medium. Digital image, video, audio and photo become the first choice as cover medium. Stego is the media that helps to contain secret data whereas the cover media are the plain file.

These days, the images turn into a most mainstream decision as a methods for cover medium primarily due to its excess to speak to and the capacity to get over applications in our day by day life. In most recent couple of years, numerous calculations are as subject of research. In our work, we have built up another system for steganography in RGB images. Data are covered up into the images in vector space. The cover picture is chosen and the secret message is inserted in it.

Information are secretly covered up into edges which are progressively chosen in light of content size. The proposed strategy is free from auxiliary draw in as it uses 2LSB procedure. The 2LSB strategy is free from basic

assault. The most vital three classes of steganography strategies are spatial area strategy, recurrence space technique and versatile strategies.

The adaptive strategy can be utilized in both spatial area and recurrence space and furthermore it is considered as extraordinary area. The two wide grouping in picture steganography is spatial area and recurrence space. In spatial space, the concealed data is utilized to straightforwardly embed in the power of the pixels which is in spatial area technique, with the assistance of a stenographer made the alteration of the secret hidden message and the cover document, which demonstrates change at the phase of least significant bit.

This approach is less convoluted and additionally best when contrasted with the other two sorts of techniques, while on account of recurrence area, the picture is first changed into recurrence area or exchange space and afterward the secretly covered up message is embedded in the change coefficients. There are different sorts of record organization of picture which are utilized as a part of investigation of picture steganography, for example, bmp, gif and jpeg.

If there should be an occurrence of digital image, commonly put away in either 8-bit or 24-bit records. 8-bit for the little size picture and 24-bit is utilized for the high payload they offer and furthermore the way that the huge number of colors present roll out the improvements from the concealed mystery message which is imperceptible from the human visual framework. Lately, there are numerous applications for information hiding.

Data hiding methods cannot be easily classified in either category of watermarking or steganography, and therefore there are so many similarities between watermarking or steganography terms. Hence different application of these two terms based upon application of the algorithm. Therefore instead of classifying between them, the most common data hiding applications are: cover communication, fingerprinting, copyright protection, secure storage and secret communication.

II. METHODS AND MATERIAL

1) Classification

In image steganography systems, the following classifications are used frequently irrespective of the algorithm by which they are executed.

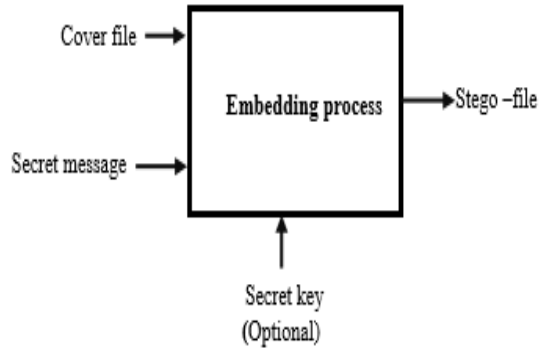

Figure 1. A Generic Scheme of Steganography Embedding Model

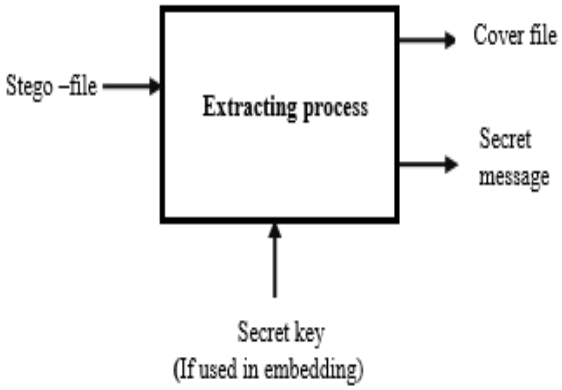

Figure 2. A Generic Scheme of Steganography Recovery Model

Image: A picture is a variety of numbers that speak to light powers at different pixels also, numerically a picture c is a discrete capacity relegating a color vector c(x,y) to each pixel (x,y).

Cover image: The cover image is the carrier of the secret message. A cover is usually chosen in a way that seems more common and harmless and not arouse suspicion.

Stego Image: A hidden secret message inside the cover image is known as the Stego image.

It is engaged at the receiver place to pull out the secretly hidden message.

Stego Key: Stego key is a key to open up the data which is available inside the cover medium and the extraction of a similar data is finished with the assistance of stego medium. It can be a number created by a pseudo-arbit ary numbers or might be just a secret word is utilized to interpret the embed site.

Embedding Domain: The Embedding area means the cover medium qualities that are make utilization of in inserting message into it. There might be spatial area when coordinate change is required of the occupant components of the cover is modified (e.g. pixels in a picture) or it can be the change area or recurrence space if numerical alterations are done on the medium before implanting.

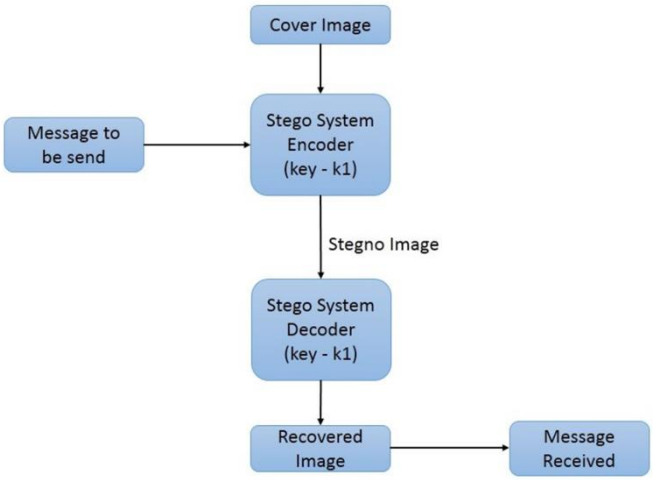

Figure 1.3: Basic block diagram of Stenographic System

Types of Steganography

Information hiding methods are classified mainly into three different classes such as: steganography, watermarking, and cryptography. The two different class i.e., Steganography and watermarking are comes under one subclasses as we can say that there is no clear boundaries between them. Fig. 1.4 illustrating the classifications of all these three classes of information hiding methods.

Steganography is the art and science of hiding data in such a manner by which forbid the detection of secret data. Steganography exactly means "covered writing" and therefore generally employed to hiding the secret information inside some cover medium.

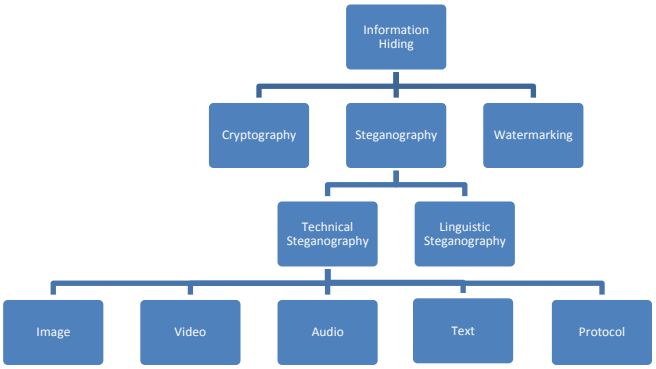

Figure 1.4: Diagram illustrating classification of Information hiding

The encryption and decryption process of a message is done with the help of cryptography. The main advantages of steganography over cryptography in such a manner that in steganography message may not able to attract the attention itself but in cryptography, there is plainly visible encrypted messages, and also it does not matter that how unbreakable will arose the suspension. Steganography may be useful for secret communication to hide the message in countries and regions where public use of cryptography is prohibited or restricted as well as cryptography never uses complex algorithms and arithmetic.

The process of inserting a message on a host signal is known as Watermarking. As we compare the watermarking and the steganography has a distinct necessity of robustness against public attack. A watermarking technique may be visible or invisible. A Digital Watermarking focuses essentially on the protection of authentication of digital media as well as intellectual property rights. Hence it holds data which is hide regarding to its author, its buyer and the helps to maintain the integrity of content. Therefore, this method helps to keep the track of the quick and inexpensive classification of the digital information over the Internet. As Steganography communication are usually point-to-point which means the communication is in between sender and receiver site while watermarking technique are usually one-to-many which means the communication is with a single sender and n number of receivers.

2) **2. Edge Detection Method**

2.1 Introduction

An edge is illustrate as the points in an image where brightness changes rapidly. Edges are substantial local modification in intensity of an image. They are treated as the boundaries between various image segments.

Image processing, computer vision and machine vision generally need edge detection process as a very important tool, mainly in the area of feature detection and feature extraction as edges are the main features for analysis of the most necessary contained information in an image. The methodology of acquiring meaningful transitions in an image, is known as edge detection. The points where sharp changes in the brightness takes place usually from the boundaries between different separate objects. Many classical edge operators are now available in the literature of image processing. Such as

1. Sobel Edge Detector
2. Prewitt Edge Detector
3. Robert Edge Detector
4. Laplacian of Gausian (Log) Edge Detector
5. Canny Edge Detector
6. Fuzzy Edge Detector

(a) Lena (b) Pepper

Figure 2.1. Two 128 X 128 test images for experiment (a) Lena (b) Pepper

Among the above all edge detection methods, the most efficient, popular and widely used edge detection is the canny edge detection method. Good detection, good localization, and single response to an edge are the three most important attributes of canny edge operator, for which it selected as the best among the other available operator. Here are the four 128 × 128 grayscale image are used for experiment in fig.2.1 such as: lena, pepper.

2.**2 Canny Edge Detector**

The main aims of the Canny Edge Detector are as follows:

- Good detection - There should be a less probability of fail to mark real edge points, and also less probability of false marking non edge points. Therefore, both these probabilities are predictability decreasing functions of the output signal-to-noise ratio, this criteria signifies to maximizing the signal-to-noise ratio. Hence, we require to mark as many real edges as possible.
- Good localization - The points marked out as edge points by the operator should be as close as possible to the center of the true edge. In essence, the marked out edges should be as close to the edges in the real edges as possible.

Single response - Only one single response to a certain edge. That isimplicitly captured in the first criteria therefore when there are two major responses to the same edge, one of them must be considered as false. Therefore, the idea is that a particular edge should be marked only once, and image noise should not create the detection of false edges.

The most important thing about canny edge detector is that it has specifically three characteristics for which it is mostly deployed in machine vision, computer vision and image processing to search the sharp intensity conversion and the object boundaries in an image. They are:

- All the most necessary edges are preserved, no false edges are taken into consideration and at the mean time the magnitude of error detection should be low.
- Least distance should be maintained between the located and real position of the edge.
- There is only one response to a particular edge.

In case of canny edge detector operator, a pixel is taken into consideration to be an edge pixel, if the gradient magnitude of that a particular pixel is more than important those of the pixels on either sides of it and in the direction of utmost intensity modification. The procedure for Canny Edge Detector implementation is summarized in the following steps [16]:

- Firstly, the image is smoothed by implementing Gaussian filter with a fixed standard deviation, to decrease the noise. (ρ) .
- The gradient magnitude g2 x + g2 y and edge direction tan−1(gx gy) should be calculated at each

and every point. A point whose strength is nearby maximum in the direction of gradient is defined as an edge point.

The performance of Canny Edge Detector, in the simulation of "Lena" and "Pepper" as the test images are defined here. Fig 2.1 illustrate the visual quality of original image and edge image shown by the canny edge detector and the number of edge pixel present in it.

3. Problem Identification

This section provides description of Existing approach available for image steganography and later in this section, Problem identification are discussed.

3.1 Objective

A new technique for steganography in HIS color image using canny edge detection operator has been proposed. Processing an image in HSI color model is relatively easier and less time consuming to other color model.

The brightness information in HIS color space is not embedded in its each layer, which indicates that all the three layers are not strongly correlated to one another and any changes to one of its layer will not have its corresponding effect on other layer.

In HSI color model we can wide large amount of data as compare to gray scale image. Data is hidden at the edges of the cover image and the edges are dynamically selected based on the length of the message.

Edge adaptive image steganography it fails to discriminate(separate) between prominent(rough) edges and smothered area for a given threshold value. Hence, there is a possibility of embedding in smoother parts of image. The proposed technique uses two-bit LSB substitution for embedding, and as a result, it reduce the number of pixels to be distorted.

Modification of two bits of the selected pixels leads to significant change in intensity of pixel, but this change does not lead to detect ability due to sharp difference in intensity of edge and non-edge pixels. Hence, embedding in edges does not produce any visible distortion in stego images.

Canny edge detection method uses Gaussian filter to remove noise present in an image. Gaussian filter perform first order differentiation to filter noise from image.

The next advantage is enhancing the signal with respect to the noise ratio. This is done by non-maxima suppression method as it results in one pixel wide ridges(hills) as the output. The third advantage is better detection of edges especially in noisy case by applying thresholding method.

The effectiveness of Canny method is affected by adjustable parameters i.e.small filter and large filter. Small filters are desirable for detection of small, sharp lines, since it causes fewer instances of blurring. Large filters are desirable for detecting larger, smoother edges. However, it causes higher instances of blurring.

We will propose a new HIS color model edge detection technique based on the mixture of hue factor and principal component analysis to resolve the problem with exiting method.

Canny edge detector has many favorable features such as smoothing effect to remove noise, and improving signal to noise ratio through a process known as non-maximal suppression. Complex algorithms used in Canny method makes it time consuming and difficult to implement to reach real time response speeds.

3.2 Limitations of the Present Investigations

Gray scale color model is a method of representing black and white images on computer. Gray images are represented using only 256 shades of gray rather than the full pallet of HSI color model. HSI color model uses the 255x255x255 shades.

Gray scale refers to a photo which has only intensity (or lightness) value, rather than full HSI color values for each pixel.

The main problem of using gray scale color mode is that it produces a image with a significantly smaller file size hence we cannot hide large amount of secrete message in a gray scale images. Gray scale color mode is in flexible and does not necessarily produce the best result image.
Edge adaptive image steganography it fails to discriminate between prominent edges and smothered

area for a given threshold. Hence, there is a possibility of embedding in smoother parts of image.

4.3 Problem Identification

Steganography is an ancient subject. Many authors has proposed various solution to the problem of encrypting secret messages into image so that intermediate person cannot able to read it. Consider two person Alice and Bob. They want to communicate with each other so that the third person cannot able to understand that about what topic they are talking. So they used method steganography, hiding secret messages into Images or any other form.

There were many problem found on various research papers. Hiding Information using LSB technique is not efficient as the output image quality is significantly decreases. The PSNR also plays very import role in encrypting the text messages. The higher is the PSNR will be, the higher will be the image quality. So we will also focused on the quality of image after the embedding process. Next, to hide text messages many paper uses Random Pixel Steganography. The random pixel steganography has many drawbacks as it is based on pixel value as the name suggests. The area are not sufficient to hide text data into images due to pixel based transformation. This problem is also addressed in our project. Majority of the existing image security systems are not up to date to protect against the latest breaching attacks. So, we have proposed an effective and robust image security framework particularly designed for the images. So, to sum of everything there are many problems earlier in steganography method. They need to seriously address. In this project, we demonstrate image steganography with Threshold selection algorithm based on Canny Edge Detection.

4. Methodology

This section presents a new Edge Based Steganography architecture. Various steps involved in processing and hiding text into images are described in this section. Section 5.1 describes about whole system architecture of the text hiding process.

4.1 Methodology

This section describes different phases of implementation of Image Steganography. Various steps involved in image steganography such as image pre-processing, threshold selection, secret message hiding or embedding and decoding of secret message. These steps are illustrated in fig.5.1.

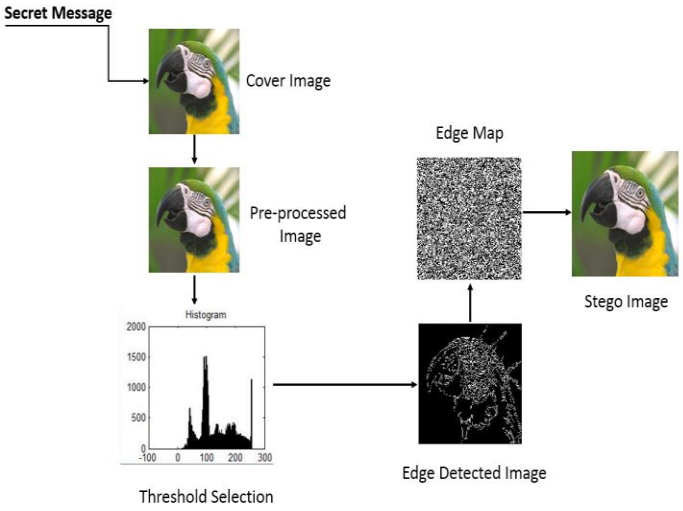

Figure 4.1. Shows the sender side image steganography system architecture

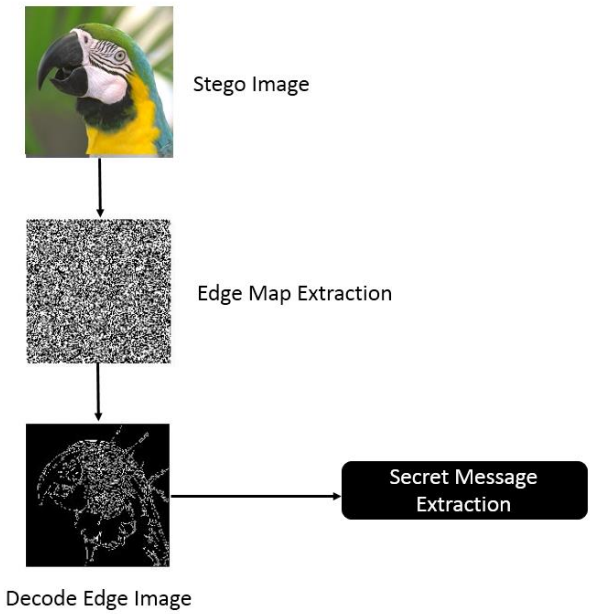

Figure 4.2. Shows the receiver side image steganography system architecture

Various steps involved in performing image steganography. The steps are described in later sections. For threshold selection getThreshold() is used and edge detection is based on Canny Edge Detection algorithm.

4.2 Cover Image

Cover Image are the image in which the information is hided. The information can be of any size. The higher is the image quality the higher information can be

stored. The capacity of the images also depends on the edge. The number of edges are more the hiding capacity of images increases. Cover Image is the input to our process. The peacock image is taken as input. It is of TIF format.

Figure 4.3. Peacock RGB Image, TIF format, 256 X 256 size

4.3 Secret Message

Secret message is the information which is to be secretly stored for transfer to another person so that third person cannot read it. The length of secret message depends on the edge and quality of image. More the quality of the image more will be the storing capacity.

Hiding of information is also depended on Edge Detection Algorithm. If there lots of edges present, then obviously the capacity to hold information also increases.

Figure 4.4. Shows the message to embed into image

4.4 Pre-Processing

There were various method used for conversion of RGB to HSI image. It is simplest one. Conversion takes place by applying below 6 steps algorithm

Steps to be followed:

1. Read a RGB image
2. Represent the RGB image in the range [0 1]
3. Find HSI components

$$\theta = \cos^{-1}\left\{\frac{\frac{1}{2}\left[(R-G)+(R-B)\right]}{\left[(R-G)^2+(R-B)(G-B)\right]^{1/2}}\right\}$$

4. $H(\text{Hue}) = \begin{cases} \theta & \text{If } B<=G \\ 360-\theta & \text{If } B>G \end{cases}$

5. $S(\text{Saturation}) = 1 - \frac{3}{(R+G+B)}\left[\min(R,G,B)\right]$

6. $I(\text{Intensity}) = \frac{1}{3}(R+G+B)$

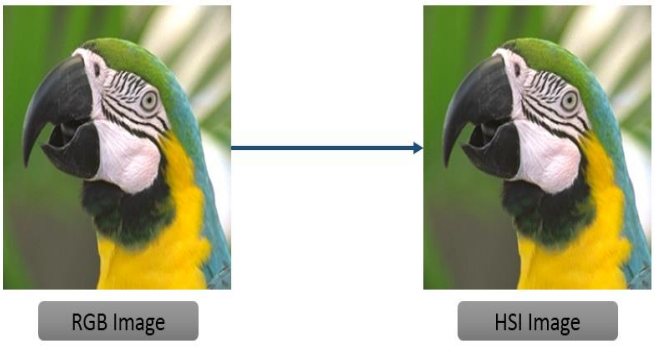

Figure 4.5. Shows the conversion of RGB to HSI Image using 6 Steps Algorithm

4.5 Threshold Selection

The threshold value is returned by the Canny Edge Detection algorithm namely, high threshold, low threshold.All these parameters are used to identify the edges in the cover images. The high threshold parameter describes that there is strong edges present and low threshold describes that there is relatively low edges are present in an Image. Based on the secret message size, the threshold is adjusted. If the message is too log then high threshold value is selected so that message can be accommodated in edges effectively. Various effect of change in threshold value is shown in fig. 5.6.

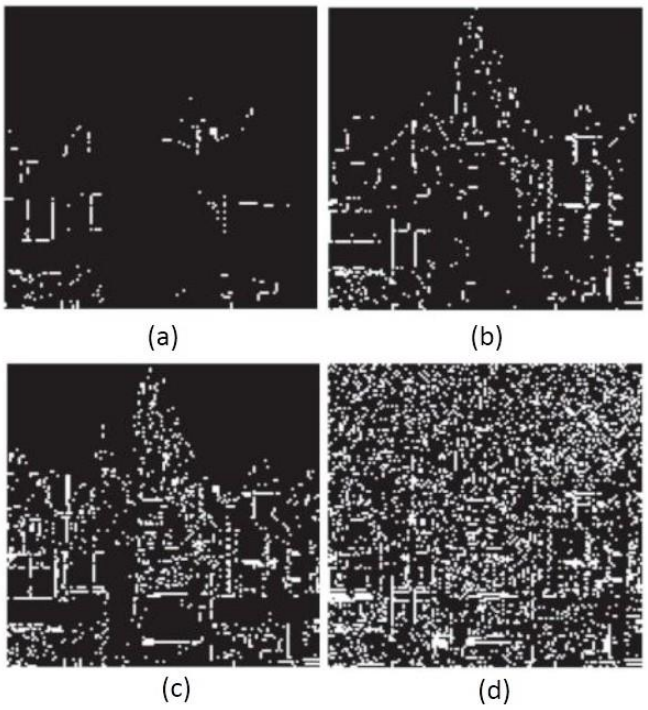

Figure 4.6. Effects of threshold. **(a)** Threshold 0 **(b)** Threshold .25 **(c)** Threshold .50**(d)** Threshold .75

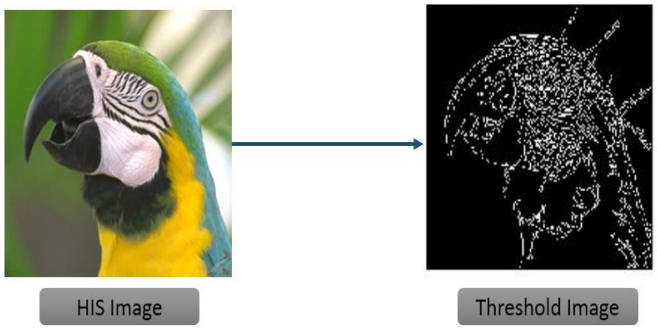

Figure 5.7. Shows the extraction of threshold form HSI image

Algorithm for Getting Threshold:

getThresholdValue(I, N, w)

Data: I: Image, N: Length of augmented message to beembedded, w: width of the Gaussian Kernel

Result: threshold: threshold th for Canny to get N pixels

// limit is set to 1% of the messagelength

// no. of edge pixels,ne ≤ N + 0.01 × N

and ne ≥ N

// ne = number of edge pixels in I, whenCanny edge detector is used on I withhigh threshold th and low threshold

tl = 0.4 ∗th and w

limit ←- 0.01 × N;

threshold_max ←- 1;

threshold_min ←- 0;

set ←- false;

repeat

th ←- [(tmax + tmin)]/2;

ne ←- getEdgePixelCount(Canny(I, th, tl, w));

// it returns the number of pixels inthe edges obtained through Cannyedge detector

diff ←- ne-N;

if diff >limit **then**

threshold_min←- th;

end

else if diff <0 **then**

threshold_max←- th;

end

else

set ←- false;

end

until set = true;

return threshold (th)

4.6 EDGE MAP

Edge map is used to represent the vector fields of an image. The vector fields can be represented in Edge Map using getEdgeMap method. It provides the continuous flow of vector mapping entry in sequence order. It provides entry as well as exit points which can be useful in determining the image contents. Edge Mapping is very robust and error free technique for storing points of image into it.In our work, we have used edge map to store the edges of images to hide secret message into it. This will help to utilize the full capacity of image to store information which is transfer to other person secretly. Fig. 5.8 shows the construction of edge map.

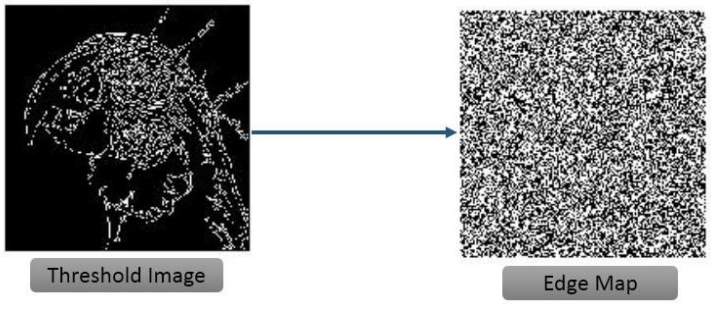

Figure 4.8. Shows the construction of Edge Map

4.7 Embedding of Message

Most of the steganographic techniques described uses LSB technique. But LSB technique is not so efficient in performing data hiding into images. So we have used 2 bit LSB technique to ensure the data hidden into images efficiently. Structural detectors can easily detect LSB

text, but with the help of 2LSB technique we can minimize the attach perform by structural detectors.

Embedding of Secret Message: embedding(I, M, P, w)
Data: I: Image, M: Augmented message in binary, P: Stegokey, w: width of the Gaussian kernel
Result: S: Stego image

S ←- I;
I ← bitand(I,252);
L ← |M|;
threshold ←- getThreshold(I, L, w);
e ←- CannyEdgeDetection(I, th, tl, w);
// Shuffle eand **S** using Stego key P
e ←- randomPermutation(e,P);
S ←- randomPermutation(S,P);
index ←- 0;
for each edge pixel **i** in **e do**
Sx,y = bitand(Sx,y,252); // x,y are co-ordinates of pixel i
Sx,y = Sx,y + 2*Mindex+1 + Mindex;
index ←- index + 2;
end
// Embed threshold and width in non-edgepixels of S
e ←- CannyEdgeDetection(I, 0, 0, 0.1); // Pixels in e aremaximum number of edge pixels for a given image
e' ←- complementOf(e); // Pixels in e' arenon-edge pixels
for i = 1: 16 in **e**' **do**
S (x,y)= bitANDoperation(Sx,y,254);
S(x,y)= Sx,y + threshold(i);
end
for i = 17: 32 in **e**' **do**
S(x,y)= bitand(Sx,y,254);
Sx,y = Sx,y +w(i-16);
end
Stego_Image←- randomPermute(S,P); // Reshuffle S toget Stego Image: S
return Stego_Image;

4.8 STEGO IMAGE

After embedding of secret information into the image, it is ready for transmission to the receiver. It can be transferred over internet, email and by other means also. The stego image is similar to the original image. There is no loss in the quality of image. Fig. 4.9. Shows the original image and stego image.

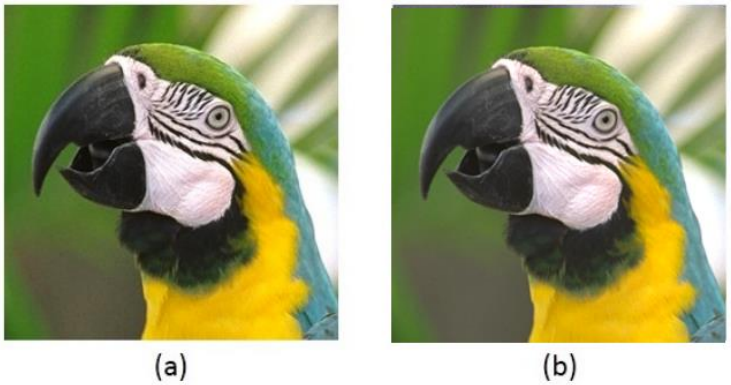

Figure 4.9. Shows **(a)** Cover Image and **(b)** Stego Image

4.9 Receiver Side Decoding

After encoding of secret message into the image, the receiver side decoder requires. The decoder construction is same as the encoder side algorithm. If there is mismatch with any of the algorithm used on encoder side, than the decoding process cannot be successfully carried out. Fig. 4.10. Shows the reverse engineering approach in which stego image is converted and processed using Edge Map Extraction.

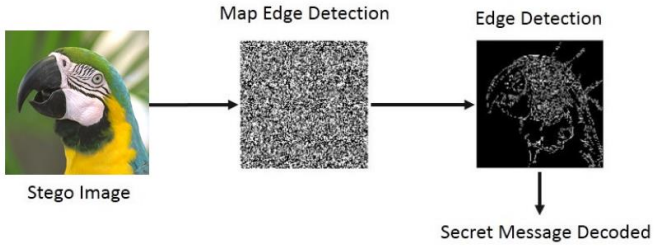

Figure 4.10. Shows the decoding process of stego image

The algorithm involved in decoding of secret message is described in algorithm below.

Decoding of Secret Messages: decode: retrieve secret message
Data: I: stego image, T: Threshold, P: stego key, w: Kernelwidth
Result: Message: Secret message

S ←- I;
S ←- bitand(S,252);
threshold ←- T;
tl ←- 0.4 ∗th;
e ←- Canny(S',th, tl, w);
e ←- randomPermutation(e,P);
// Shuffle S to get order of embedding
S ←- randomPermutation(S, P);

```
index ←- 0;
for each edge pixel i in e do
val ←- bitand(Sx,y,3); // x, y are co-ordinates
of pixel i
Mindex+1 ←- val mod 2;
val ←- val/2;
Mindex = val;
index ←- index + 2;
end
// extract first C bits to get message
size
msg_size ←- Message[1:C];
Message←- Message[C + 1 : msg_size];
return (Message);
```

III. RESULTS AND DISCUSSION

5.1 Environment Setup

We have used MATLAB for evaluation and validation of our project. Image processing tool is used to pre-process and implement Canny Edge Detection algorithm.

TABLE II. Presents Various Tools and Method Used

Simulation Software Used	**MATLAB**
Simulation Software Version	Version 2010b
Tools Used	Image Processing Tool
Algorithm Used	Canny Edge Detection
Stego Key Algorithm	Symmetric Key Algorithm
Cover Image Format	JPEG, TIF
Image Type	RGB to HIS

5.2 Experiment Results

The Proposed methodology is tested and run successfully on MATLAB software. The input dataset is peacock.jpg file which is taken from the web. Various other images with different format are analyzed. The description are provided in subsequent sections. We have performed experiment and analyzed performance using PSNR metrics and time required for algorithm to run. The attributed of images are shown in fig. 5.1 and fig. 5.2.

Figure 5.1. Shows various attributes of peacock image.

Figure 5.2. Shows various attributes of baby girl image.

We have analyzed image baby girl and peacock image using Canny Edge detection method by varying the threshold level. We have adjusted threshold in three levels. The output of threshold generated are given in TABLE II presents various metrics for validating

performance of proposed steganography method.

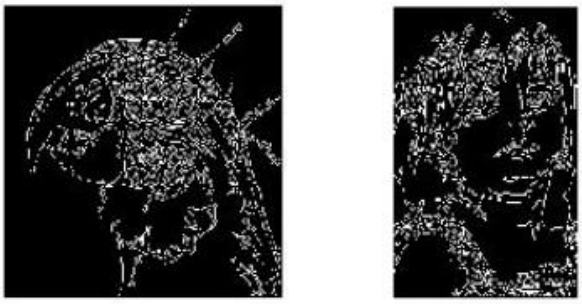

Figure 5.3. Shows the threshold selection of two images peacock and baby girl respectively

5.3 Metrics for Measuring Quality of Image

Comparing restoration results requires a measure of image quality. Commonly used measures isPeak Signal-to-Noise Ratio. The formula is presented below for calculating PSNR value.

$$e_{MSE} = \frac{1}{MN}\sum_{n=1}^{M}\sum_{m=1}^{N}\left[\hat{g}(n,m) - g(n,m)\right]^2$$

$$\text{PSNR} = -10 log_{10}\frac{e_{MSE}}{S^2}$$

Where S is the (max) pixel value. PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image. The more is the dB the more will the quality of image. Hence 30 dB image look much better than 10 dB image. Table shows the comparative analysis of two images on the basis of time of execution and PSNR value.

TABLE III. Shows PSNR value and time required for execution of algorithm

Image	Size	Execution time	PSNR
Peacock.tif	256 X 256	20.191 sec	37.9908 dB
Baby-girl.jpg	256 X 256	20.54 sec	71.0068 dB

5.4 Discussions

We have discusses various method for hiding information into images. The experimental results shows that our proposed algorithm effectively process our images and transform it into another form where the secret message are hidden. We also have computed the computation time of our algorithm to show how much time is required for processing of job. We have validated our work with PSNR value. The PSNR describes about image quality. The higher is the PSNR value, the higher will be the quality of image.

IV. CONCLUSION

In our work, we have developed a new technique for steganography in RGB images. Information are hidden into the images in vector space. The cover image is selected and the secret message is embedded in it. Data are secretly hidden into edges which are dynamically selected based on text size. The proposed method is free from structural attract as it uses 2LSB technique. The 2LSB technique is free from structural attack. Canny Edge detection is used to detect the edges based on threshold. We have defined various threshold levels for an image. For example low and high threshold value. The higher will be the threshold value the higher is the space allocated by an image. Means with higher threshold value we can hide more umber of textual information into image.

V. SCOPE OF FUTURE WORK

Due to the time limit, several interesting ideas have not been implemented yet. However, it will be worthwhile trying them in the future.One of the foremost thing I would like to improve is to apply steganography for 3D images using Canny Edge Detection algorithm.

VI. REFERENCES

[1]. Song, S., Zhang, J., Liao, X., Du, J., and Wen, Q., "A novel secure communication protocol combining steganography and cryptography," Procedia Engineering, vol. 15, pp. 2767–2772, 2011.

[2]. Benlcouiri, Y., Ismaili, M., Azizi, A., and Benabdellah, M., "Securing images by secret key steganography," Applied Mathematical Sciences, vol. 6, no. 111, pp. 5513–5523, 2012

[3]. Anand, D. and Niranjan, U., "Watermarking medical images with patient information," in Engineering in Medicine and Biology Society, 1998. Proceedings of the 20th Annual International Conference of the IEEE, vol. 2, pp. 703–706, IEEE, 1998.

[4]. Judge, J. C., "Steganography: Past, present, future," tech. rep., Lawrence Livermore National Lab., CA (US), 2001.
[5]. Bin Sahib, S. and Zamani, M., "An introduction to image steganography techniques,"
[6]. Roy, R., Changder, S., Sarkar, A., and Debnath, N. C., "Evaluating image teganography techniques: Future research challenges," in Computing, Management and Telecommunications (ComManTel), 2013 International Conference on, pp. 309–314, IEEE, 2013.
[7]. Chanu, Y., Tuithung, T., and Manglem Singh, K., "A short survey on image steganography and steganalysis techniques," in Emerging Trends and Applications in computer Science (NCETACS), 2012 3rd National Conference on, pp. 52–55, IEEE, 2012.
[8]. An overview of image steganography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa
[9]. Johnson, N.F. Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998
[10]. Li, Y., Li, C.-T., and Wei, C.-H., "Protection of mammograms using blind steganography and watermarking," in Information Assurance and Security, 2007. IAS 2007. Third International Symposium on, pp. 496–500, IEEE, 2007
[11]. "Detecting LSB Steganography in Color and Gray-Scale Images" Jessica Fridrich, Miroslav Goljan, and Rui Du State University of New York, Binghamton
[12]. K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images",Technical Report, Department of Computer Science and Engineering, University Visvesvarya College of Engineering,Bangalore University, December 2004
[13]. P. Kruus, C. Scace,M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal.
[14]. M.M. Amin, M. Salleh, S. Ibrahim, et al., "Information Hiding Using Steganography", 4th National Conference on Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, 2003
[15]. A Review of Data Hiding in Digital Images by E Lin, E Delp Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, IN 47907-2086
[16]. Gonzalez, R. C., Woods, R. E., and Eddins, S. L., Digital image processing using MATLAB. Pearson Education India, 2004
[17]. Akash Modi, Manu Bansal, "An Enhanced LSB Steganography Algorithm for Data Hiding",International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 5, May 2015.
[18]. Yojna Chandel and Sunil Chhillar, "A Review on Reversible Data Hiding",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 9, September 2015.
[19]. Arun Kumar Singh, Juhi Singh and Dr. Harsh Vikram Singh., "Steganography in Images Using LSB Technique",International Journal of Latest Trends in Engineering and Technology (IJLTET),Vol. 5 Issue 1 January 2015.
[20]. S. Raveendra Reddy and Sakthivel S M, "A Fpga Implementation Of Data Hiding Using Lsb Matching Method",IJRET: International Journal of Research in Engineering and Technology,Volume: 04 Issue: 03.
[21]. Sandipan Dey , Ajith Abraham and Sugata Sanyal ,"An LSB Data Hiding Technique Using Prime Numbers".
[22]. Kede Ma, "Objective Quality Assessment for Color-to-Gray Image Conversion", International Electrical and Electronics Engineering (IEEE),Volume:24 Issue:12 2015.
[23]. Arun Navjot Kaur and Manpreet Singh, "Modified Approach Using Lsb In Image Steganography", International Journal Of Research –Granthaalayah,Vol.3(Iss.5):May,2015.
[24]. Deepak Tomarand S. Vijaylakshmi, "Steganography Based On Singal Bit Data Hiding", International Journal of Innovative Research and Studio (IJIRS),Vol. 3 Issue 4May 2014.
[25]. Mukesh Garg and A.P. Gurudev Jangra, "An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques",International Journal of Advanced

Research in Computer Science and Software Engineering,Volume 4, Issue 1, January 2014.

[26]. Saiful Islam,MangatRModi and PhalguniGupta, "Edge-basedimagesteganography", EURASIPJournalonInformationSecurity a Springer open Journal,2014.

[27]. Krati vyas and B.L.Pal,, "A Proposed Method In Image Steganography To Improve Image Quality With Lsb Technique", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2014.

[28]. Mamta Juneja and Parvinder S. Sandhu, "An Improved LSB Based Steganography Technique for RGB Color Images",International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013.

[29]. Deepesh Rawat and Vijaya Bhandari, "Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method", International Journal of Computer Applications (0975 – 8887) Volume 67– No.1, April 2013.