

Image Steganography using LSB and Edge – Detection Technique

Nitin Jain, Sachin Meshram, Shikha Dubey

Abstract: *Steganography is the technique of hiding the fact that communication is taking place, by hiding data in other data. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Steganalysis, the detection of this hidden information, is an inherently difficult problem and requires a thorough investigation so we are using “Edge detection Filter”.*

In this paper search how the edges of the images can be used to hiding text message in Steganography .It give the depth view of image steganography and Edge detection Filter techniques.

Keywords: *Steganography, Steganalysis, edge detection, digital image, gray image, RGB image, Binary image, 8 pixel connectivity.*

Method: *In this paper search how the edges of the images can be used to hiding text message in Steganography. For that gray image has been presented. In this method tried to find binary value of each character of text message and then in the next stage, tried to find dark places of gray image (black) by converting the original image to binary image for labeling each object of image by considering on 8 pixel connectivity. Then these images have been converted to RGB image in order to find dark places. Because in this way each sequence of gray color turns into RGB color and dark level of grey image is found by this way if the Gary image is very light the histogram must be changed manually to find just dark places. In the final stage each 8 pixels of dark places has been considered as a byte and binary value of each character has been put in low bit of each byte that was created manually by dark places pixels for increasing security of the main way of least Significant bit steganography. Steganalysis then used to evaluate the hiding process to ensure the data can be hidden in best possible way.*

I. INTRODUCTION

The growing possibilities of Modern communication need the special mean of security on computer network. In the computer world, it is very important to keep secret information secret, private information private and protect the copyrights of data. To accomplish this task, new methods based on the principle of Image processing are being developed and used.

A. Image Processing

Image processing is any form of signal processing for which the input is an image, such as photographs or frames

Manuscript received on July 2012.

Mr. Nitin Jain, Assistant Professor, Department Of Electronics & Telecommunication, Chouksey Engineering College, Bilaspur, C.G., India.

Mr. Sachin Meshram Assistant Professor, Department Of Electronics & Telecommunication, Chouksey Engineering College, Bilaspur, C.G., India.

Shikha Dubey, M.tech research scholar, Department Of Electronics & Telecommunication, Chouksey Engineering College, Bilaspur, C.G., India.

of video, the output of image processing can be either an image or a set of characteristics related to the image. Now, an image is an array of numbers that represent light intensities at various points (pixels). These pixels make up the image raster data [1].

In computer vision, image processing can be done through digital images. A digital image is composed of *pixels* which can be thought of as small dots on the screen. A digital image is an instruction of how to colour each pixel. Each image can be divided in to number of pixels.

B. Image steganography

Image steganography, the covert embedding of data into digital pictures, represents a threat to the safeguarding of sensitive information and the gathering of intelligence. Steganalysis, the detection of this hidden information, is an inherently difficult problem and requires a thorough investigation. Conversely, then hider who demands privacy must carefully examine a means to guarantee stealth. A rigorous framework for analysis is required, both from the point of view of the steganalyst and the steganographer. The research concerning the technique of hiding secret message into information is usually named *steganography*. This is because the word “Steganography” comes from the Greek root meaning “covered writing”.

An *image* steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method. Someone can then use a proper embedding procedure to recover the hidden message from the image. The original image is called a *cover image* in steganography, and the message-embedded image is called a *stego image* [2].

C. Data hiding Background

As long as people have been able to communicate with one another, there has been a desire to do so secretly. Two general approaches to covert exchanges of information have been: communicate in a way understandable by the intended parties, but unintelligible to eavesdroppers; or communicate innocuously, so no extra party bothers to eavesdrop. Naturally both of these methods can be used concurrently to enhance privacy. Naturally both of these methods can be used concurrently to enhance privacy. The formal studies of these methods, cryptography and steganography, have evolved and become increasingly more sophisticated over the centuries to the modern digital age. Methods for hiding data into cover or host media, such as audio, images, and video, were developed about a decade Steganography generally is subjected to less vicious attacks, however much data as possible has is to be inserted.

The general motivation for

steganalysis is to remove the veil of secrecy desired by the hider. Typical uses for steganography are for espionage, industrial or military. A steganalyst may be a company scanning outgoing emails to prevent the leaking of proprietary information, or an intelligence gatherer hoping to detect communication between adversaries.

Steganalysis is an inherently difficult problem. The original cover is not available, the number of steganography tools is large, and each tool may have many tenable parameters. However because of the importance of the problem there have been many approaches. Typically an intuition on the characteristics of cover images is used to determine a decision statistic that captures the effect of data hiding and allow discrimination between natural images and those containing hidden data. We have therefore seen an iterative process of steganography and steganalysis: a steganographic method is detected by a steganalysis tool, a new steganographic method is invented to prevent detection, which in turn is found to be susceptible to an improved steganalysis.

II. PROPOSED WORK



In this paper edge pixels were selected in order to hide the data. One common way to hide the data is “Least Significant Bit Insertion”. This method modifies the low order bit of each pixel to match the message to hide [4]. The selection of pixels in which the message will be embedded is very important because modified pixels in areas of the image where there are pixels that are most like their neighbors are much more noticeable to the naked eye. A single modified pixel stands out among its uniform neighbor pixels thus making the image suspicious. One possible solution for this problem is to select the edge-pixels of the image to hide the message. It is not noticeable when a single pixel is modified when its surrounding pixels are least like it. Once the edge pixels are selected, the edge pixels are selected randomly.

III. ALGORITHM AND TECHNIQUE

A. Connectivity of Image

- 1) Pixel Connectivity: A morphological processing starts at the peaks in the marker image and spreads throughout the rest of the image based on the connectivity of the pixels. Connectivity defines which pixels are connected to other pixels. A group of pixels that connected based on Connectivity types called an Object.
- 2) Selecting Connectivity: The type of neighborhood that may choose affects the number of objects found in an image. For example (Table.1), if you specify a 4-connected neighborhood, this binary image contains three objects; if you specify an 8-connected neighborhood, the image has one object. The gray thresh function which chooses the threshold to minimize the interclass variance of the black and white pixels.

TABLE I
SUPPORTED CONNECTIVITY

Two-Dimensional Connectivities		
4-connected	Pixels are connected if their edges touch. This means that a pair of adjoining pixels are part of the same object only if they are both on and are connected along the horizontal or vertical direction.	
8-connected	Pixels are connected if their edges or corners touch. This means that if two adjoining pixels are on, they are part of the same object, regardless of whether they are connected along the horizontal, vertical, or diagonal direction.	

B. Edge Detection

Edge detection is a problem of fundamental importance in image analysis. In typical images, edges characterize object boundaries and are therefore useful for segmentation, registration, and identification of objects in a scene. Edge detection of an image reduces significantly the amount of data and filters out information that may be regarded as less relevant, preserving the important structural properties of an image. A theory of edge detection is presented. The analysis proceeds in two parts:

- 1) Intensity changes, which occur in a natural image over a wide range of scales, are detected separately at different scales. An appropriate filter for this purpose at a given scale is found to be the second derivative of a Gaussian. Intensity changes at a given scale are best detected by finding the zero values of image. The intensity changes discovered in each of the channels are represented by oriented primitives called zero-crossing segments.
- 2) Intensity changes in images arise from surface discontinuities or from reflectance or illumination Boundaries and these all have the property that they are spatially localized. Because of this, the zero crossing segments from the different channels are not independent, and rules are deduced for Combining them into a description of the image. This description is called the raw primal sketch.

C. Edge Detection Techniques

Edge detection aims at identifying points in a digital image at which the image brightness changes sharply or more formally has discontinuities. Following edge detectors are handy:

- 1) Sobels Edge Detector - 3×3 gradient edge detector
- 2) Prewitt Edge Detector - 3×3 gradient edge detector.
- 3) Canny Edge Detector - non-maximal suppression of local gradient magnitude.
- 4) Zero Crossing Detectors - edge detector using the Laplacian of Gaussian operator.

In this paper work we are using Zero crossing detector.

Zero Crossing Detector

The zero crossing detector looks for places in



the Laplacian of an image where the value of the Laplacian passes through zero --- i.e. points where the Laplacian changes sign. Such points often occur at 'edges' in images --- i.e. points where the intensity of the image changes rapidly, but they also occur at places that are not as easy to associate with edges. It is best to think of the zero crossing detectors as some sort of feature detector rather than as a specific edge detector. Zero crossings always lie on closed contours, and so the output from the zero crossing detector is usually a binary image with single pixel thickness lines showing the positions of the zero crossing points. The starting point for the zero crossing detectors is an image which has been filtered using the Laplacian of Gaussian filter. The zero crossings that result are strongly influenced by the size of the Gaussian used for the smoothing stage of this operator. As the smoothing is increased then fewer and fewer zero crossing contours will be found, and those that do remain will correspond to features of larger and larger scale in the image.

D. Obtaining Image Edge

The most important features of objects in images are edges. There are several edge detection algorithms. It uses its zero-crossing property to find the location of edges. Let's suppose that we have the following image signal ($f(t)$) as its describing function, with an edge it is quite clear that the gradient has a large peak centered around the edge. By comparing the gradient to a threshold value which in this case is 10 percent of the peak value, an edge can be detected if the threshold exceeds. In this case the edge has been found, but it becomes broad" due to the threshold.

However, since we know the edge occurs at the peak, we can localize it by computing the one dimension and the second derivative with respect to t .

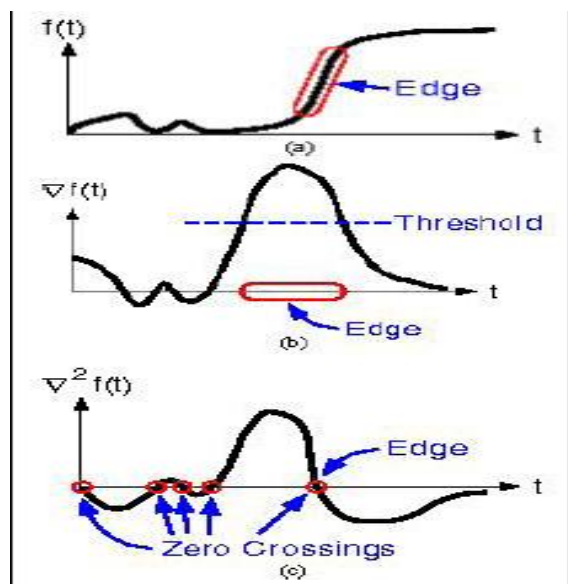


Fig. 3.1 Binary Image

IV. IMAGE EMBEDDING AND EXTRACTING

Most steganographic systems follow the same general process for hiding and recovering data. Typically, the input for a system consists of a cover medium that is image and a

secret message. Several classes of steganographic methods have emerged are following:-

A. Least Significant Bit Embedding

Embedding is defined as the mapping secret message to pixel's steganography is the most classic steganographic techniques, which embeds secret messages in a subset of the LSB plane of the image. A large number of popular steganographic tools, such as S-Tools 4, Steganos and StegoDos, are based on LSB replacement in the spatial domain.

LSB steganography can be described as follows: if the LSB of the pixel value $I(i, j)$ is equal to the message bit m to be embedded, $I(i, j)$ remain unchanged; if not, set the LSB of $I(i, j)$ to m . The message embedding procedure can be described using an Equation as follows;

$$I_s(i, j) = \begin{cases} I(i, j)-1 & \text{LSB}(I(i, j))=1 \text{ and } m=0 \\ I(i, j) & \text{LSB}(I(i, j))=m \\ I(i, j)+1 & \text{LSB}(I(i, j))\neq 0 \text{ and } m=1 \end{cases}$$

In general, a p -by- q image is simply a p -by- q matrix, where each entry in the matrix is a positive integer called the pixel value, which determine the color of that pixel. For an n -bit image, these pixel values range from 0 to $2^n - 1$. In other words, the possible color values for each pixel in an n -bit image are the colors corresponding to the bit strings of length n . Unless there is a specific need to use the bit string representations of pixel values, we will typically use the decimal representations. In this paper, we talk primarily about 8-bit grayscale images. These images are thus p -by- q matrices of integers ranging from 0 to 255, where 0 corresponds to black, 255 to white, and the values in between form a spectrum of varying shades of gray (i.e., darker shades nearer 0 and lighter shades nearer 255). The least significant bit (LSB) is the bit corresponding to 1, that is, the bit that makes a value even or odd. Since these grayscale values form a spectrum ranging in order from dark to light, each gray value varies little from the values on either side of it. For example, the gray value 100 varies little from the gray values 99 or 101. Therefore, changing the LSB creates an imperceptible change in the image.

```

If pixel value = odd
  Then increment by 1
  Else if the pixel value = 255
    then decrement by 1
If pixel value = even
  if bit = 0
    then add 1
  else if pixel value = 255
    if bit value = 0
      then decrement by 1
  else if pixel value = even
    if bit = 1
      then increment by 1
    
```

1

Image Steganography Using LSB and Edge – Detection Technique

Select the pixels of the image using the key. Increment the grey level value of the pixel by 1 if the pixel value is odd and if the value is 255 subtract it by 1. Convert the data into bit stream and compare this bit stream with the pixel values.

increment pixel values by one if bit is 0 and pixel values is odd, and increase by one if bit is 1 and pixel value is even. Decrement pixel value by 1 if bit is 0 and pixel value is 255.

B. Least Significant Bit Extracting

Extracting is defined as the mapping pixels to image. In the image steganography the extracting process can be done on message which is the stego image. The recipient inputs the stego image, and when applicable, the steganographic key, into an extraction algorithm, which outputs the secret message. This extraction algorithm is considered the inverse of the embedding algorithm, although the embedding and extraction algorithms may be created such that the extraction algorithm is not actually the mathematical inverse of the embedding algorithm. Several factors influence the effectiveness of a steganographic system, the most important of which is the choice of the cover image.

In the extraction algorithm, I have done some steps:

- 1) Initially I have stego image and key and the message which is converted in the form of ASCII form. The hidden message is stored in Low level least significant bit.
- 2) I searched where our message is being stored, for that we set the threshold value which depends upon the cover image.
- 3) I check the stego image is even or odd then set the message bit either 0 or 1.
- 4) Inverse of embedding process

If pixel value = odd
Then the bit value is 1
Else if pixel value = even
Then the bit value is 0

V. EXPERIMENTAL RESULT

The experimental results presented in this section describe the performance of our proposed technique. For steganography we use LSB based well known embedding methods. To conduct our experiments, we have tested our scheme LSB embedding & Canny Edge Detector over more than 50 standard images of different resolutions including some of them with different images, „Test”, „Lena”, „Fruit” and etc. These test images are shown in table-2.

Generally, stego-image quality is considered from two aspects. First, we use the Peak Signal-to-Noise Ratio (PSNR) measurement to evaluate the difference between the stego and cover images. Second, we compare the quality of the stego image with the cover image as seen by the Human Visual System (HVS). Mean Square Error (MSE) is between the cover and stego images. For a cover image width and height are m and n, where I denote the cover-image and K denotes the stego-image MSE is defined as:

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

The general PSNR formula is defined as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

The maximum value of a pixel in grayscale image is 255. A higher PSNR indicates that the quality of the stego image is better and more similar to the cover image. Table-5.1 shows the results of LSB method. It shows the different images with MSE and PSNR parameters. For example „Test” stego-image has MSE 2.1348 and its PSNR is 44.837%, where in table-5.2 shows LSB with canny edge detector result in which images have greater PSNR and lower MSE. Table-5.3 shows the proposed method results with all above parameters. Through experimental results table-2 and 3 shows that proposed method has quite good embedding capacity.



Fig. 5.1 Image Cata Set For Experiments

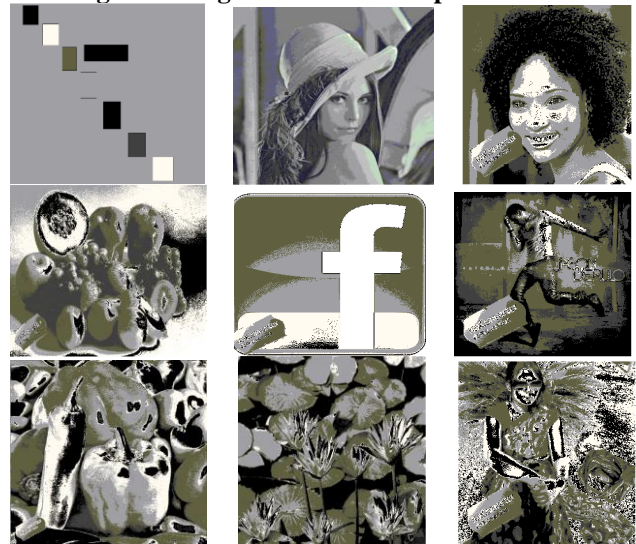


Fig 5.2 Stego Image Result Of Lsb Embedding Technique

Table 5.1: Lsb Embedding Based Results

IMAGE	MSE	PSNR
TEST	2.1348	44.837
Lena	3.1664	42.778
Hairstyle	13.338	36.88
Fruit	6.8863	39.751



Face book	10.181	38.083
Dance	15.796	36.145
Pepper	4.7394	41.374
Lotus	4.2102	41.888
Goggle	13.338	35.223

Table 5.2: Lsb Embedding With Canny Edge Detector Based Results

IMAGE	MSE	PSNR
TEST	496.14	48.757
Lena	67.75	68.667
Hairstyle	63.412	69.329
Fruit	84.615	66.444
Face book	61.813	69.584
Dance	80.385	66.957
Pepper	61.2	69.684
Lotus	59.462	69.972
Goggle	74.786	67.679



Fig 5.3 Stego Images Result Of Proposed Method

Table 5. 3: Proposed Method Results

IMAGE	MSE	PSNR
TEST	829.57	43.616
Lena	76.583	67.441
Hairstyle	54.059	70.925
Fruit	70.692	68.242
Face book	57.438	70.318
Dance	70.692	68.242
Pepper	61.267	69.673
Lotus	70.692	68.242
Goggle	65.643	68.983

After overall comparison of all the result it is clear that LSB Embedding is simple technique but It is not robust. If an image file embedded with a secret message using LSB Coding was resampled; the embedded information would be lost. It also doesn't give clarity to the stego image which can be easily detected by human eye as shown in Fig.5.2. Robustness can be improved somewhat by using an Edge detection technique while encoding the secret message. LSB embedding with Canny edge detector gives better result as compare to the LSB technique as it gives higher PSNR value, lower MSE value and better clarity to the stego Image but still the proposed method is best among these methods. It gives highest stego image clarity with highest PSNR and lowest MSE value except in case of "TEST"& "LENA" images as given in table 5.2 & 5.3. So the objects of this paper (clarity, authentication & Security) for different kind of images is fulfilled.

VI. CONCLUSION

A technique of information hiding using steganography, particularly edge detection filter has been presented, which is a way for labeling different color to identify dark area of image. This approach hides the text in selected dark places but the data is not put directly in those pixels and put in low bits of each eight bit pixel.

It uses the 3 advantageous approaches, which are:

1. Least significant bit insertion
2. Grey level approach with edge detection
3. Randomization

The LSB insertion was used to embed the message in to the cover image. The selection of pixel to embed was crucial, since the LSB insertion modifies the pixels. Modified pixels in areas of the image where there are pixels that are most like their neighbors were much more noticeable to the normal eye.

To solve this problem edge pixel were randomly selected to embed the message. The advantage of LSB is its simplicity to embed the bits of the message directly into the LSB plane of cover image. Also its perceptual transparency where the changes made to the cover-image cannot be traced by human eye. on the contrary, the LSB is very sensitive to any kind of filtering or manipulation of the stego-image.

Using the edge detection approach along with least significant bit method leads to high security. Even with a little object as an image, the embedded image is just like the original one.

REFERENCES

1. N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen", Computer Journal, IEEE, February 1998.
2. M. M. Amin, M. Salleh, S. Ibrahim, M.R.Katmin, M.Z.I. Shamsuddin, "Information Hiding using Steganography" Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam, Malaysia, 2003.
3. N. Provos and P. honeyman, "Hide and seek : an introduction to steganography" IEEE Computer Society, 2003.
4. K. Curran, X.Li, R. Clarke, "An investigation in to the use of the least significant bit substitution technique in digital watermarking", Journal of Applied Science 2 (3), pp. 648-654,2005.



Image Steganography Using LSB and Edge – Detection Technique

5. R. J. Anderson, F. A. P. Petitcolas, "On the limits of steganography", Journal of Selected areas in communications, 16(4), pp. 474-481, 1998.
6. G. J. Simmons, "The prisoners problem and the subliminal channel", Proc. of CRYPTO, 1983.
7. R. Chandramouli, M.Kharrazi, N. Memon, "Image Steganography: Concepts and Practice", proc. Of IWDW 2003, LNCS 2939, pp. 35-49, 2004.
8. R. Radhakrishnan, K. Shanmugasundaram, N. Memon, "Data Masking: A Secure-Covert Channel Paradigm", 2002.
9. D. Neeta, K. Sehla, "Implementation of LSB Steganography and its Evaluation or Various Bits", 2004.
10. C. Cachin, "An Information Theoretic model for steganography", 2004.
11. J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation", SPIE Symposium on Electronic Imaging, San Jose, CA, 2003.
12. A.D. Ker, "Steganalysis of LSB Matching in Grayscale Images", IEEE signal processing letters, vol. 12, No 6, 2005.
13. K. B. Raja, N. Shankar, K. R. Venugopal, L. M. Patnaik, "Steganalysis of LSB Embedded Images using Variable threshold color pair analysis", IEEE 2006.
14. C. Ming, Z. Ru, N. Xinxin, Y. Yixian, "Analysis of Current Steganography Tools: Classification & Features", Proc. of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006.
15. M. Niimi, H. Noda, E. Kawaguchi, "High Capacity and Secure Digital Steganography to Palette-Based Images", 2002.
16. N. Wu, M. Hwang, "Data Hiding Current Status and key issues", International Journal of Network Security, Jan 2007.
17. W. Luo, "Object-related illustration watermarks on cartoon images", Feb 2004.
18. R. Alwan, F. Kadhim, A. Al-Taani, "Data Embedding based on better use of bits in image pixels" International Journal of signal processing, 2005.
19. K. M. Singh, L. S. Singh, A. B. Singh, K. S. Devi "Hiding Secret Message in Edge of the Image" International conference of Information and Communication Technology, ICICT 2007.
20. J. Silman, "Steganography and steganalysis: An overview", SANS Institute 2001.
21. T. Jamil, "Steganography: The art of hiding information is plain sight", IEEE potentials, 1999.
22. H. Wang, S. Wang, "Cyber warfare: steganography vs. steganalysis", communication of the ACM, Oct 2004.
23. L.M. Marvel, Jr. C.G. Bonchelet, C. Retter, "Spread spectrum steganography" IEEE Transactions on Image Processing, 1999.
24. I.Avcibas, N.Memon, B. Sankur, "Steganalysis using image quality metrics" IEEE Transactions on Image Processing, Feb 2003.
25. J.R. Kreen, "Steganography And Steganalysis", Jan 2004.
26. E. Sodipo, "Steganography in principle".
27. <http://www.mirrors.wiretapped.net/security/steganography/blindside>
28. <http://www.wbailer.com/wbstego>
29. D. Artz, "Digital Steganography: Hiding Data within Data", 2001.
30. Y. Wang, P. Moalin, "Steganalysis of Block DCT image steganography".
31. J. Fridrich, M. Golan, D. Hoge, "Steganalysis of JPEG Images: Breaking the F5 Algorithm".
32. T. Morkel, J. H. P. Elloff, M.S. Olivier, "An Overview of Image Steganography".
33. S. C. Chapra, "Applied Numerical Methods with Matlab".
34. W. J. Palm, "Introduction to Matlab 7 for engineers", 2005.
35. H. Moore, "Matlab for Engineers", 2007.
36. Mehdi Hussain, M. Hussain, "Information hiding using edge boundaries of objects", International journal of security and application, 2011
37. Shiram K Vasudevan, Dharmendra T. Shivaram R, "Automotive Image Processing Technology using Canny's edge detector", international journal of engineering and technology 2010.
38. Manish kaushal, Arjan Singh, Baljit Singh, "Adaptive thresholding for edge detection in gray scale image", 2010.
39. P.D.Khandait, S.P.Khandait, "LSB technique for secure data communication".
40. Rishi R. Rakesh, Prabal Chaudhari, E.A. Murthy, "Thresholding in edge detection A Statistical Approach", IEEE Transaction on image processing, 2004
41. R. Chandramouli, Nasir Menon, "Analysis of LSB based image steganography techniques", 0-7803-6725, IEEE 2001.
42. E. Nadernejad, S. sharifzadeh, H. Hassaupour, "Edge detection techniques evaluation and comparison", 2008.
43. Mamta Juneja, Parvinder Singh Sadhu "Performance evaluation of edge detection technique for image and spatial domain", international journal of computer theory and Engineering, 2009.
44. Chang-Chou-Lin, Wen-Hsiang Tsai, "Secret image sharing with steganography and authentication", The journal of system and software 2004.
45. Ching-Nung Yang, Tse-Shih Chan, Kun Hsuan, 'Improvements of image sharing with steganography and authentication', The journal of system and software 2004.
46. Rupinder Kaur, Mandeep Kaur, Rahul Malhotra, "a new approach towards steganography", IJCSIT, 2011.
47. Sujay Narayana, Gaurav Prasad, "Two new approaches for second image steganography using cryptography techniques and type commissions", SIJIT, 2011.
48. Kathryn Hempstalk, "Hiding behind corner-using edge in images for better Steganography".
49. Amanpreet kaur, Renu Dhir, Geeta Sikka, "A new image steganography based on first component alteration technique", IJCSIS, 2009.
50. Raman Maini, Dr. Himanshu Agrawal "study and comparison of various image edge detection techniques", International journal of image processing.
51. N. Senthilkumar, R.Rajesh, "Edge detection techniques for image segmentation-A Survey of soft computing approaches", International journal of recent trends in engineering, 2009