OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Assessment of Steganography using Image Edges for Enhancement in Security

Durgesh Nandani and Dr. Raghav Yadav
M.Tech Research Scholar, Department of computer science & information Technology, SHIATS-DU, Allahabad-211007
Assistant Professor , Department of computer science & information Technology, SHIATS-DU, Allahabad-211007

ABSTRACT:- *Steganography is the art of passing information in a manner that the very existence of the message is unknown. Steganography is a method of hiding secret messages in a cover object while communication takes place between sender and receiver. Security of confidential information has always been a major issue from the past times to the present time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone other than the receiver. Therefore from time to time researchers have developed many techniques to fulfill secure transfer of data and Steganography is one of them. In this paper we have proposed a new technique of image Steganography i.e. Steganography is applied on image edges with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses an ELSB (Edge based least significant bit) technique to generate a pattern for hiding data bits into ELSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form. Objective is not only to prevent the message being read but also to hide its existence. In this paper, canny arithmetic operator has been proved to have good detective effect in the common usage of edge detection. In the algorithm, self-adaptive filter is used to replace the Gaussian filter, morphological thinning is adopted to thin the edge and morphological operator is used to achieved the refining treatment of edge points detection and the single pixel level edge.*

Keywords: *Cryptography, Steganography, ELSB, RSA Encryption –Decryption, Embedding, Canny Edge detector*

I. INTRODUCTION

Steganography is a technique which is used to transmit a secret message under the cover of digital media such as images. It first pays much more attention on embedding payload rather than robustness against intentional attacks compared with watermark which is used to protect the copyright. Moreover, imperceptibility, which is the second requirement, is carefully considered in the Steganography algorithms. Thus, an effective Steganography scheme should not cause any perceptible distortion and have to achieve high capacity as well. In most Steganographic techniques, although only the most significant components are altered, many analytical techniques can reveal existence of the hidden message by detecting statistical difference between the cover and stego objects. The following two measures may be taken in developing Steganographic schemes to combat steganalysis:

Avoid conspicuous parts when embedding messages into the cover.

Improve embedding efficiency, i.e., embed more information per modification to the cover data.

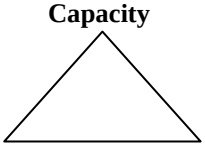


Figure 1: Magic Triangle-Three Requirements Model

To achieve this goal, in this paper, we proposed a very simple and effective method that based on the ELSB technique in combining with the edge detection mechanism. The ELSB Steganography, that replaces the ELSBs of the cover image by the secret message, is a widely used technique with low computational complexity and high insertion capacity. Although it has good perceptual transparency, it is vulnerable to steganalysis which is based on the statistical analysis. Many other Steganography algorithms have been developed such as spread spectrum embedding. But the embedding capacity is not satisfied. To develop a new ELSB Steganography algorithm that can against statistical analysis, we apply the edge detection mechanism in this proposed scheme. In each cover pixel, this mechanism allows selecting various numbers of ELSBs which are used to replace with the secret message.

Moreover, this mechanism helps improving not only the quality of the stego image but also the embedding payload. Noticeably, the advantage and strength of our scheme is obtained by the edge detection. Thus, to exploit as many edge pixels as possible in the cover image, we use canny edge detector. The first edge detector helps detecting a large number of edge pixels in an image to provide clear and thick edge images. Second is designed to be an optimal edge detector which is considered as the most rigorously defined operator and is widely used. Moreover, the canny edge detector can be attributed to its optimality according to the three criteria of good detection, good localization, and single response to an edge.

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn't be accessed. But in cryptography it's always clear to intermediate person that the message is in encrypted form, whereas in Steganography the secret message is made to hide in cover image so that it couldn't be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender. A model of the Steganographic process with cryptography is illustrated in Fig. 2.

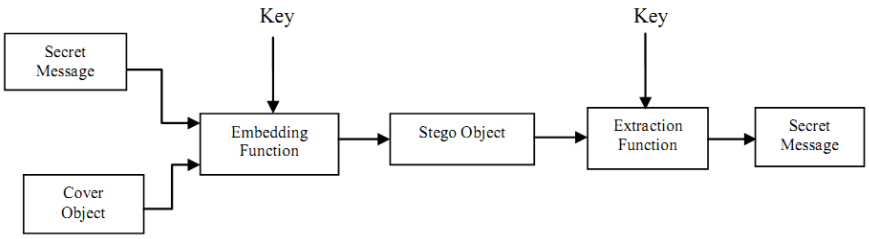


Figure 2: A model of the Steganographic process with cryptography

A. Edge detector

An edge is characterized by significant dissimilarity in gray levels being used to indicate the boundary between two regions in an image fragment. Edge detection is a significant area of the image processing and machine vision due to the fact that edges are considered to be the important features for analyzing the most essential information contained in images. Many classical edge operators such as Sobel, Prewitt, Laplacian and Canny operators are already available in the literature (Sonka, Hlavac, & Boyle,1999). Among these edge detection methods proposed so far, the Canny edge detector is considered the most rigorously defined operator and is widely used. The popularity of the Canny edge detector can be attributed to its optimality according to the three criteria of good detection, good localization, and single response to an edge. It also has a rather simple approximate implementation, which is the subject of this paper.

Figure 3: The cover image and the stego image.

B. Canny edge detector

The Canny edge operator has three characteristics (Nanning, 1998): (1) No important edges should be missed, and there should be no false edges, while the error detection rate should be kept low. (2) The distance between the actual and located position of the edge should be minimal. (3) There is only one response to a single edge. The Canny edge detector is widely used in computer vision to locate sharp intensity changes and to find the object boundaries in an image. The Canny edge detector classifies a pixel as an edge if the gradient magnitude of the pixel is greater than those of the pixels on both sides of it in the direction of maximum intensity change. A typical implementation of the canny edge detector (Trucco, & Verri, 1998; Jain, Kasturi, & Schunck, 1995) follows the following steps:

Step 1: The image is first smoothed by the Gaussian filter mask. At the beginning, we divide the image into a set of blocks. The size of each block is equal to the size of the Gaussian filter mask. The mask is applied in the image by convolution operation.

Step 2: Determine gradient magnitude and gradient direction of each pixel. This step is done by using the Sobel operators. Basically, we use 2-D spatial gradient in which Gx and Gy is defined as follows:

$$\mathbf{Gx} = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \qquad \mathbf{Gy} = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

Step 3: If the gradient magnitude at a pixel is greater than those of its neighbors in the gradient direction, mark the pixel as an edge. Otherwise, mark the pixel as the background.

Step 4: Remove the weak edges by hysteresis threshold.

In order to highlight the performance of the Canny edge detector, the experimental results of the test images ‘‘Tiffany”, ‘‘Lena”, ‘‘Pepper” and ‘‘Building” are considered. Fig. 5 shows the visual quality of the edge images and the number of edge pixels which are generated by the Canny edge detector. The edge images are generated by the Canny edge detector.

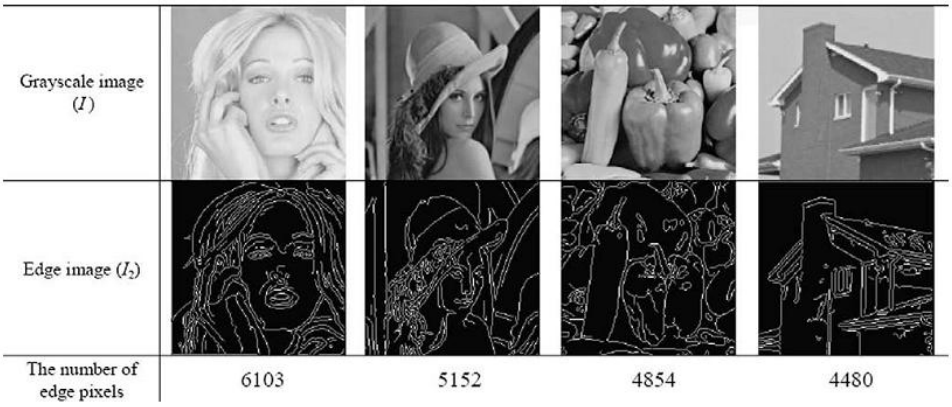


Figure 4: The Edge Images are generated by the Canny Edge Detector.

II. LITRATURE REVIEW

Abbas Cheddad et al. (2010) proposed Digital image Steganography: Survey and analysis of current methods [1]. Authors explained that Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files.

Anastasia Ioannidou et al. (2012) proposed a novel technique for image Steganography based on a high payload method and edge detection [2]. Authors explained that Image Steganography has received a lot of attention during the last decade due to the lowering of the cost of storage media, which has allowed for wide use of a large number of images.

Battikh. D et al. (2013) presented enhancement of two spatial Steganography algorithms by using a chaotic system: comparative analysis [3]. A chaos-based enhancement of two spatial Steganographic algorithms the AE-LSB and the EA-LSBMR and we study their performances.

C.L. Philip Chen et al. (2012) proposed A pattern recognition system for JPEG Steganography detection [4]. Authors explained that a pattern recognition system to detect anomalies in JPEG images, especially Steganography content.

Chang-Chou Lin et al. (2004) presented Secret image sharing with Steganography and authentication [5]. Authors explained that A novel approach to secret image sharing based on a ð k; np-threshold scheme with the additional capabilities of Steganography and authentication is proposed.

Yu-chi chen et al. (2014) presented "Encrypted signal-based reversible data hiding with public key cryptosystem [19]. Authors explained that Encrypted image-based reversible data hiding (EIRDH) is a well-known method allowing that the image provider gives the data hider an encrypted image, the data hider embeds the secret message into it to generate the encrypted image with the embedded secret message to the receiver, and finally the receiver can extract the message and recover the original image without encryption.

Ziguan cui et al. (2014) proposed Simple and effective image quality 0assessment based on edge enhanced mean square error [20]. Authors explain that Simple and effective image quality assessment (IQA) method is very desirable in many image and video processing applications, such as coding, transmission, restoration and enhancement. Classic pixel absolute error based objective IQA metrics such as mean square error (MSE) and corresponding peak signal to noise ratio (PSNR) are widely used for various applications due to low computation and clear physical meanings, but have also been criticized for poorly correlated with subjective evaluation.

III. MATERIALS AND METHODS

There are a large number of cryptographic and Steganographic methods that most of us are familiar with. The most widely used two techniques are:

1. RSA Algorithm
2. The canny edge detection algorithm

1. The RSA Algorithm

- **Key generation:**
  1. Select random prime numbers p and q, and check p! =q.
  2. Compute modulus n=p*q.
  3. Compute phi, Ø= (p-1) x (q-1).
  4. Select public exponent e, 1 <e <Ø such that gcd (e, Ø) =1.
  5. Compute private exponent, (d*e) mod Ø=1.
  6. Public key is {n, e}, private key, d.
- **Encryption:** c = (m ^ e) mod n.
- **Decryption:** m = (c ^ d) mod n.
- **Digital signature:** s = (H (m) ^ d)) mod n
- **Verification:** m'=(s ^ e) mod n.
  If m'=H (m) signature is correct.
  H is publicly known hash function

2. The canny edge detection algorithm

The canny algorithm consists of three criterion of the edge detection algorithm.

2.1 The criterion of SNR

The larger of the SNR, the higher quality of the detection edge . The SNR is defined as follow:

$$SNR = \frac{\left|\int_{-W}^{+W} G(-x)h(x)dx\right|}{\sigma\sqrt{\int_{-W}^{+W} h^2(x)dx}} \qquad (1)$$

Where, the G (x) represents the edge function, h(x) represents the impulse response of the filter of width is W. σ represents the mean square deviation of the Gaussian noise .

2.2 The criterion of positioning accuracy

The positioning accuracy of the edge is defined as follow:

$$L = \frac{\left|\int_{-W}^{+W} G'(-x)h'(-x)dx\right|}{\sigma\sqrt{\int_{-W}^{+W} h'^2(x)dx}} \qquad (2)$$

Where, the G(x) and h(x) respectively is the derivative of the G(x) and h(x) , the larger of the positioning accuracy, the result is better.

2.3 The criterion of the singleness edge response

To ensure the edge only have one response, the average distance D(f') of the zero-crossing point of the derivative of the impulse response of the edge detection algorithm. The D (f') should meet the follow formula:

$$D(f') = \pi \left\{ \frac{\int_{-\infty}^{+\infty} h'^2(x)dx}{\int_{-W}^{+W} h'^2(x)dx} \right\}^{\frac{1}{2}} \quad (3)$$

IV. PROPOSED METHODOLOGY

The problem statement consists of embedding the secret message in the LSB of each RGB pixels value of the cover image. Before embedding the secret message have to be converted to cipher text using RSA algorithm to enhance the secrecy of the message. In this approach we implemented a technique called Hash-LSB derived from LSB insertion on images**Edge Based Image Steganography Using Public- Key Cryptosystem (RSA)**

In a 24- bit bitmap each pixel is represented by 3 bytes, representing the red, green and blue color value for that pixel. The higher number, the more intense is the color for that to be a multiple of 4. However, using this extra bytes to hide the data would be unwise as these bytes are supposed to contain 0's and any alteration would be easily detectable.

A. Cover Image and Secret Message

In our proposed system, first of all we select a true color image of size 512 x 512 for to it as a cover image and a secret message which will be embedded in the cover image.

B. RSA Encryption and EDGE based Encoding

This approach of image Steganography is using RSA encryption technique to encrypt the secret data. Encryption includes a message or a file encryption for converting it into the cipher text. Encryption process will use recipient public key to encrypt secret data. It provides security by converting secret data into a cipher text, which will be difficult for any intruder to decrypt it without the recipient private key. At the start of this process we take cipher text encrypted from the secret message to be embedded in the cover image. In this process first we converted cipher text into binary form to convert it into bits. Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue channel respectively. The process is continued till entire message of bits will got embedded into the cover image.

Embedding Algorithm:

Step 1: Choose the cover image & secret message.
Step 2: Encrypt the message using RSA algorithm.
Step 3: Find Edges of each RGB pixels from cover image.
Step 4: Apply a hash function on LSB of cover image to get the position.
Step 5: Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function given in equation 1.
Step 6: Send stego image to receiver.

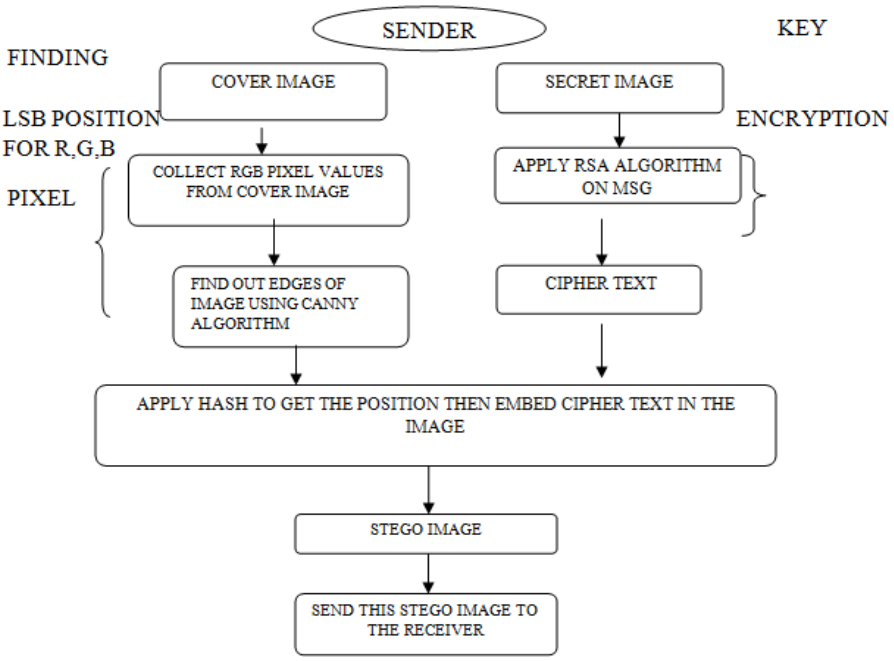


Figure 5: The process of embedding secret data into the cover image

C. EDGE based Decoding and RSA Decryption

In the decoding process we have again used the hash function to detect the positions of the edges , where the data bits had been embedded. When the position of the bits had been specified, the bits are then extracted from the position in the same order as they were embedded. At the end of this process we will get the message in binary form which again converted into decimal form, and with same process we got the cipher text message. After retrieving the positions of edges that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable form.

Retrieval Algorithm:

Step 1: Receive a stego image.
Step 2: Find edges of each RGB pixels from stego image.
Step 3: Apply hash function to get the position of edges with hidden data.
Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.
Step 5: Apply RSA algorithm to decrypt the retrieved data.
Step 6: Finally read the secret message.

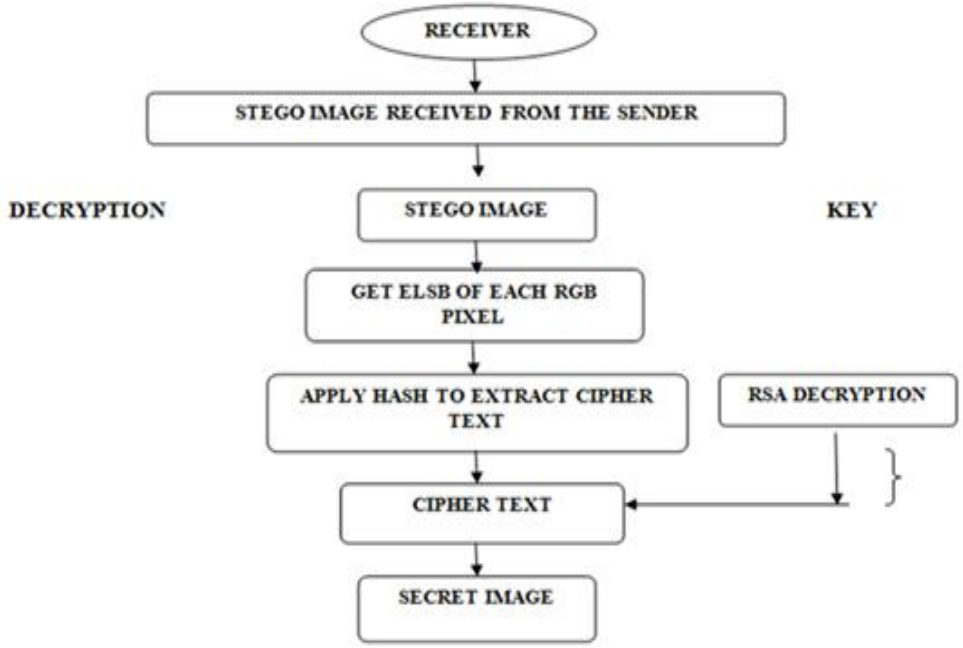


Figure 6: The process of retrieving secret data from the stego image

V. PERFORMANCE ANALYSIS AND RESULTS

Evaluation Criteria for Different Techniques:

1. **Invisibility:** The invisibility of Steganography algorithm is the first requirement, since the strength of Steganography lies in its ability to un notice by the human eye [8].The algorithm is compromised if the image is tampered.
2. **Payload capacity:** Steganography aims to hide the communication as watermarking that embeds the copyright information. So payload capacity also needed for embedding the information.
3. **Robustness:** After embedding data should be remain as it even if cropping, filtering is applied to the stego-image. Steganography algorithms should be robust against any changed made to the imag**e.**
4. **Independent of file format:** Only one type of file format is used between two parties that seem to be suspicious. The strong Steganography algorithms has the ability to embed data in any type of file means it is independent of any file format. So there is no problem of finding the image in right format to use as cover image.

5. **Unsuspicious files:** This requirement includes all characteristics of a Steganography algorithm that may result in images that are not used normally and may cause problem [8].Abnormal size is example of unsuspicious file which will further result in examining the image.
6. **Security:** It should be impossible for attacker to detect the information even if it knows the existence of information. It is measured in terms of Peak signal noise ratio by using eq. 1. PSNR is used to analyze the quality of image. High PSNR high is the security as little difference in cover image and stego image.

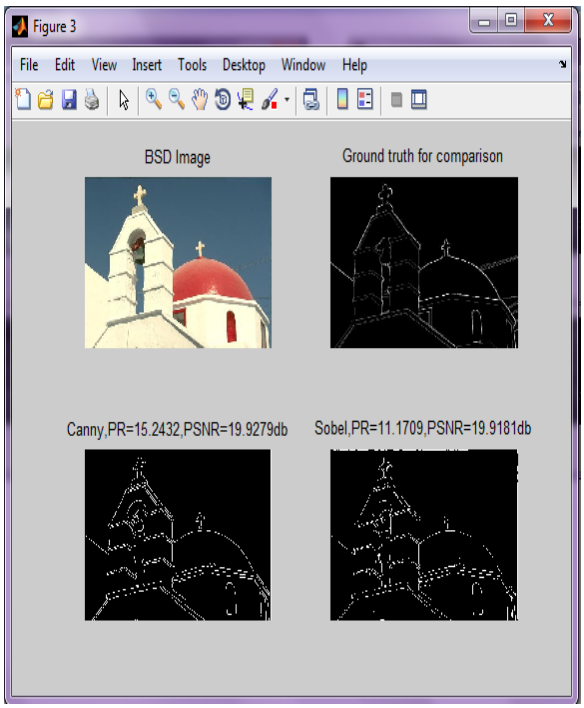
   Where R=maximum value and MSE =Mean square error.

$$\text{PSNR} = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \qquad \text{..... (1)}$$

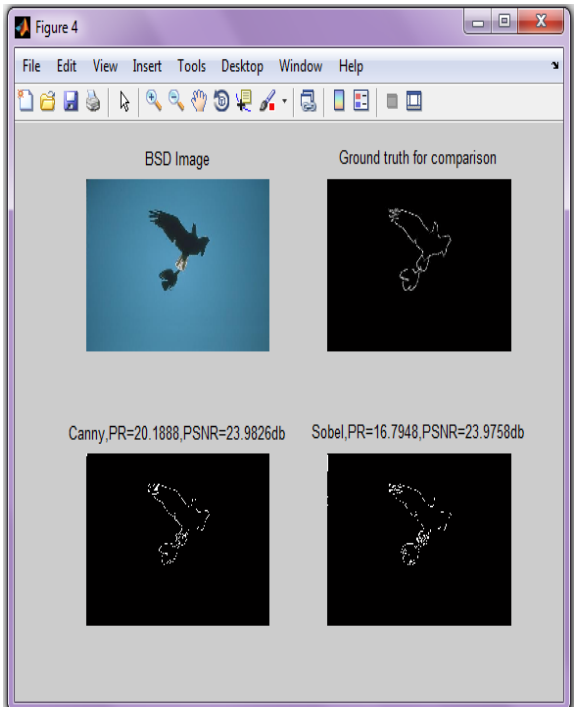
$$PSNR = 10 \times \log_{10}\frac{255^2}{MSE}(dB)$$

7. **Mean square Error** is first calculated to calculate peak signal noise ratio.MSE represents the error between original image and compressed image. The error is lower if value of MSE is lower.

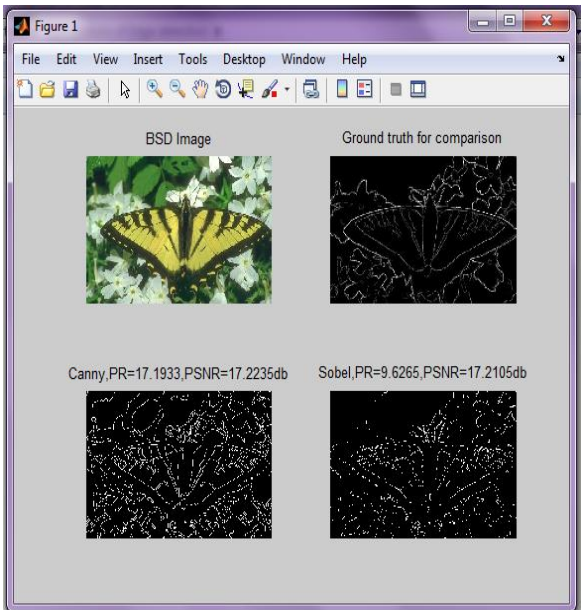
$$MSE = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}(I_{ij} - I'_{ij})^2$$



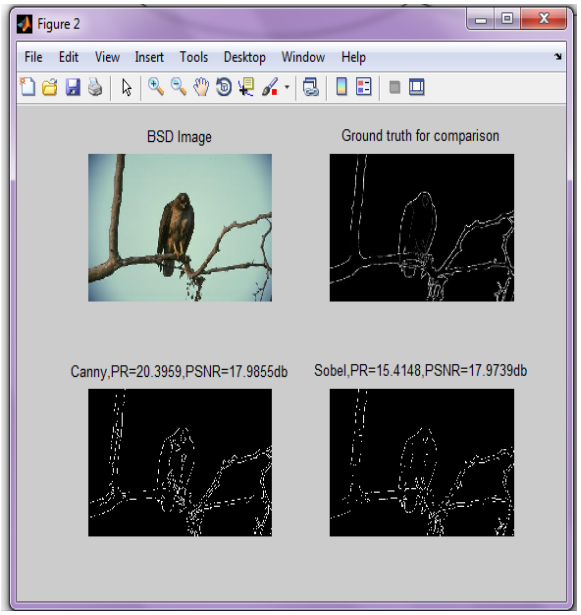
(a)



(b)

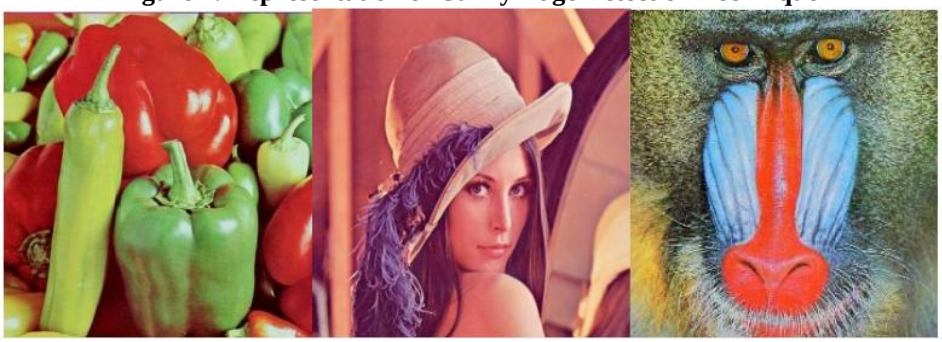


(c)



(d)

Figure 7: Representation of Canny Edge Detection Technique



Peppers.tif **Lena.tif** **Baboon.tif**

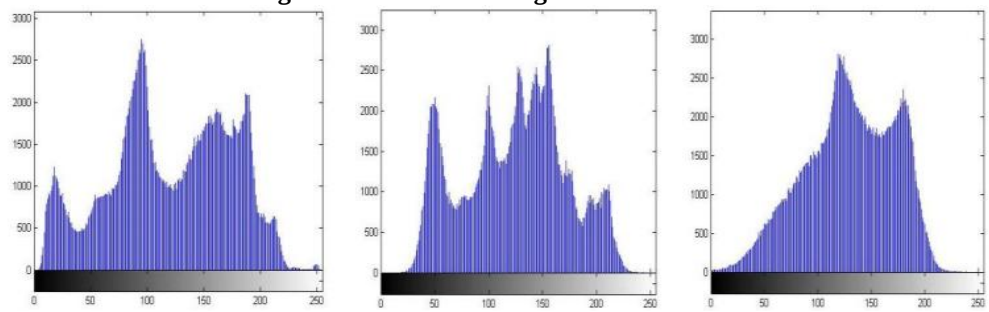
Figure 8: Original Images of Size 512x512

Peppers.tif **Lena.tif** **Baboon.tif**

Figure 9: After Applying Edge Detection Algorithm

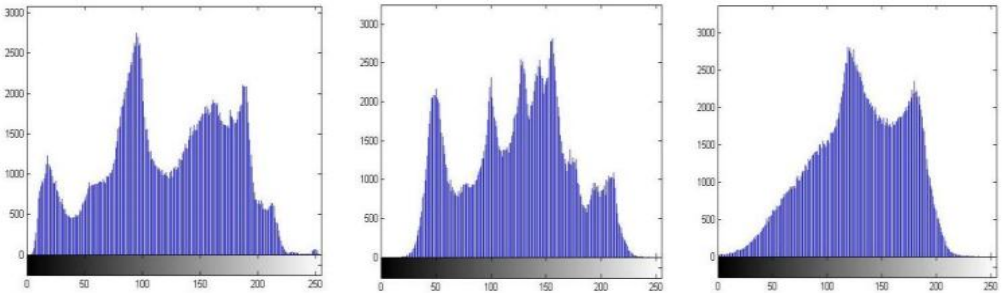
Peppers.tif **Lena.tif** **Baboon.tif**

Figure 10: Encoded images with text data



Peppers Histogram **Lena Histogram** **Baboon Histogram**

Figure 11: Histograms of Original Images



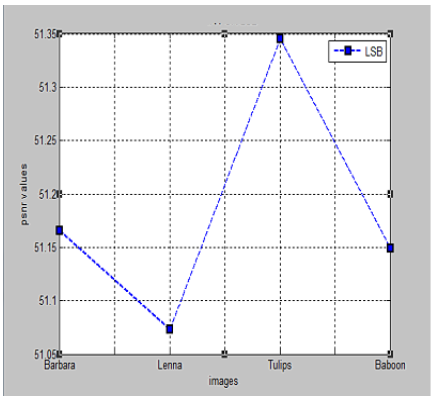
Peppers Histogram **Lena Histogram** **Baboon Histogram**

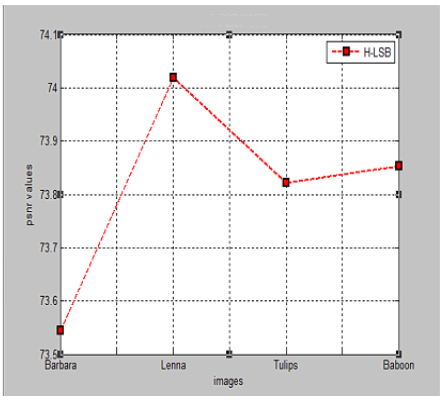
Figure 12: Histograms of Original Images

Table 1. MSE Outputs

Text Data to be Hide (Bytes)	Lena	Peppers	Baboon
792	1.9044	3.7463	3.3397
1702	4.4395	8.0184	6.7508
2547	6.4501	12.4848	9.4621
4110	10.4937	20.1557	13.9992
6075	18.3308	31.9407	20.2122
11346	35.9050	53.8168	36.1801

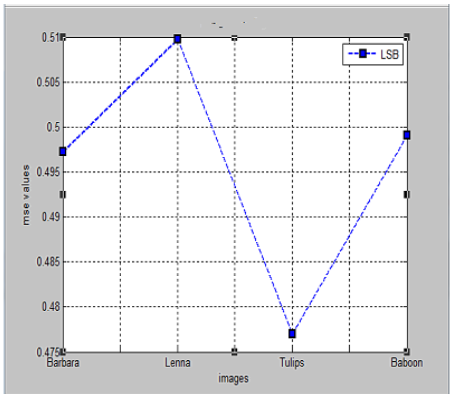
Table 2. PSNR Outputs			
Text Data to be Hide (Bytes)	**Lena**	**Peppers**	**Baboon**
792	45.3672	42.4288	42.9277
1702	41.6915	39.1239	39.8712
2547	40.0692	37.2010	38.4049
4110	37.9555	35.1208	36.7038
6075	35.5330	33.1214	35.1087
11346	32.6133	30.8556	32.5801

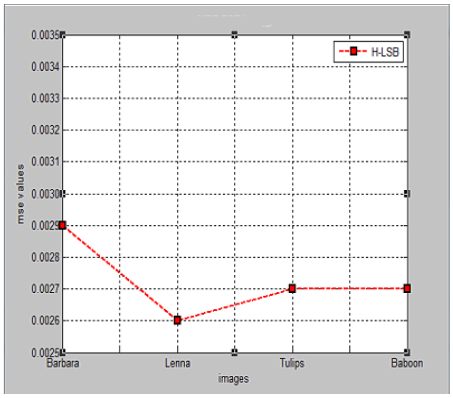




(a) LSB technique with RSA **(b) EDGE based ELSB technique with RSA**

Figure 11: The graphical representation of PSNR value





(a) LSB technique with RSA **(b) EDGE based ELSB technique with RSA**

Figure 12: The graphical representation of MSE value

VI. CONCLUSION

A secured EDGE based technique for image Steganography has been implemented. An efficient Steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through ELSB method. In this work, a new way of hiding information in an image with less variation in image bits have been created, which makes our technique secure and more efficient. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that's why we used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet. The ELSB technique have been applied to .tiff images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been

evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images. The future scope for the proposed method might be the development of an enhanced Steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the Steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

VII. REFERENCES

[1]. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt. "Digital image Steganography: Survey and analysis of current methods" ELSEVIR Signal Processing 90 (2010) 727 –752.

[2]. Anastasia Ioannidis, Spyros T. Halkidis, George Stephan ides. "A novel technique for image Steganography based on a high payload method and edge detection" ELSEVIER Expert Systems with Applications 39 (2012).

[3]. Battikh. D , El Assad, Bakhache , B. Deforges O. "Enhancement of two spatial Steganography algorithms by using a chaotic system: comparative analysis". Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference Publisher: IEEE 9-12 Dec. 2013

[4]. C.L. Philip Chen, Mei-Ching Chen, Sos Agaian , Yicong Zhou, Anuradha Roy, Benjamin M. Rodriguez. "A pattern recognition system for JPEG Steganography detection" ELSEVIER Optics Communications 285 (2012) 4252 –4261.

[5]. Chang-Chou Lin, Wen-Hsiang Tsai. "Secret image sharing with Steganography and authentication" ELSEVIER the Journal of Systems and Software 73 (2004) 405–414. E. Argyle. "Techniques for edge detection," Proc. IEEE, vol. 59, pp.285-286, 1971

[6]. Esra Satir a, Hakan Isik. "A compression-based text Steganography method" ELSEVIER, The Journal of Systems and Software 85 (2012).

[7]. Falesh M. Shelke1, Ashwini A. Dongre, Pravin D. Soni. "Comparison of different techniques for Steganography in images" International Journal of Application or Innovation in Engineering & Management Volume 3, Issue 2, February 2014.

[8]. Iranpour M. " Adaptive edge tracing Steganography" ELMAR, 2013 IEEE 55th International Symposium Conference 25-27 Sept. 2013

[9]. J. F. Canny. "A computational approach to edge detection". IEEE Trans.Pattern Anal. Machine Intell., vol. PAMI-8, no. 6, pp. 679-697, 1986.

[10]. K. Naveen Brahma Teja, Dr. G. L. Madhumati K. Rama Koteswara Rao. "Data Hiding Using EDGE Based Steganography" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 11, November 2012.

[11]. Mare, S.F. ; Vladutiu, M. ; Prodan, L. "Secret data communication system using Steganography, AES and RSA" Design and Technology in Electronic Packaging (SIITME), 2011 IEEE 17th International Symposium for 20-23 Oct. 2011.

[12]. Nitin Jain, Sachin Meshram, Shikha Dubey. "Image Steganography using LSB and Edge Detection Technique", IJCSE,July 2012

[13]. Pund-Dange, S. Desai, C.G. "Secured data communication system using RSA with mersenne primes and Steganography". Computing for Sustainable Global Development (INDIA Com), 2015 IEEE 2nd International Conference on 11-13 March 2015

[14]. R. C. Gonzalez and R. E. Woods. "Digital Image Processing". 2nd edition. Prentice Hall, 2002.

[15]. Ratnakirti Roya, Anirban Sarkara, Suvamoy Changder. "Chaos based Edge Adaptive Image Steganography" ELSEVIER (2013) 138-146.

[16]. Rishi R. Rakesh, Prabal Chaudhary, E.A. Murthy. "Thresholding in Edge Detection A Statistical approach" IEEE Transaction on Image Processing , 2004

[17]. S. Arora, S. Anand. "A Proposed method for Image Steganography using Edge Detection", International Journal for emerging technology and Advanced Engineering, vol3, pp 296-297, 2013.

[18]. T. Peli and D. Malah. "A Study of Edge Detection Algorithms". Computer Graphics and Image Processing, vol. 20, pp. 1-21, 1982.

[19]. Bing Wang, ShaoSheng Fan. "An improved CANNY edge detection algorithm ", 2009 Second IEEE International Workshop on Computer Science and Engineering.

[20]. Van Schyndel RG, Tirkel AZ, Osborne CF. A Digital Watermark. In International Conference on Image Processing. IEEE. 1994; page : 86–90.

[21]. Wen-Yuan Chena, Chin-Hsing Chenb.(2005) "A robust watermarking scheme using phase shift keying with the combination of amplitude boost and low amplitude block selection" ELSEVIER Pattern Recognition 38 (2005) 587–598.

[22]. Weiqi luo, jiwu huang. "edge adaptive image steganography based on lsb matching revisited" ieee transactions on information forensics and security, vol. 5, no. 2, june 2010.

[23]. Yu-chi chen, chih-wei shiu, gwoboa horng. "Encrypted signal-based reversible data hiding with public key cryptosystem" IEEE article Journal of visual communication and image representation, volume 25, issue 5, July 2014, pages 1164-1170

[24]. Ziguan Cui; Zongliang Gan; Guijin Tang; Feng Liu; Xiuchang Zhu. " simple and effective image quality assessment based on edge enhanced mean square error "Wireless Communications and Signal Processing (WCSP), 2014 Sixth International IEEE conference on September 11 , 2014