Framework of LSB, Adaptive Steganalysis with IQM and Stegnography of Digital Media

M.Revathi[*], J B Bhattacharjee[**], S.Vijayalakshmi[**]

[*]PG student in the department of ECE Rajalakshmi Engineering College, Chennai-602105, India, mrevathi_ece2609@rediffmail.com
[**]Faculty in the department of ECE, Affiliated to Anna University Chennai-600025, India, jbbhattacharjee@yahoo.com

Abstract

This paper propose a general framework for the detection of the length of a secret message hidden in the LSBs of samples for a large class of digital media contents (such as image). An ideal steganographic technique namely Adaptive Steganography that exploits the natural variations in the pixel intensities of a cover image to hide the secret message is also implemented. The present techniques holds best for steganalysis of images that have been potentially subjected to steganographic algorithms, both within the passive warden and active warden frameworks which leave statistical evidence can be exploited for detection with the aid of "ANOVA" for image quality features and multivariate regression analysis as an optimal classifier. A case study on the LSB steganalysis of color images and experimental results for adaptive steganalysis and image quality metrics are reported.

Keywords: *Digital media, LSB steganography, steganalysis, adaptive steganography.*

I. Introduction

The profusion of digital media (image, video, and audio) in our modern life has led to a rapid technological development of steganography and steganalysis with digital media files being the carrier contents (camouflage). In hiding process the following concept may be observed:

Cover-object: refers to the object used as the carrier to embed messages into. Many different objects have been employed to embed messages into for example images, audio, and video as well as file structures, and html pages to name a few.

Stego-object: refers to the object, which is carrying a hidden message. So given a cover object, and a message the goal of the steganographer is to produce a stego object which would carry the message. hiding information in other information.[9],[10]

There are other applications that drive interest in the subject of information hiding.

• Military and intelligence agencies require unobtrusive communications. Even if the content is encrypted, the detection of a signal on a modern battlefield may lead rapidly to an attack on the signaler. For this reason, military communications use techniques such as spread spectrum modulation or meteor scatter transmission to make signals hard for the enemy to detect or jam.

• Criminals also place great value on unobtrusive communications. Their preferred technologies include prepaid mobile phones, mobile phones that have been modified to change their identity frequently, and hacked corporate switchboards through which calls can be rerouted.

• Law enforcement and counter intelligence agencies are interested in understanding these technologies and their weaknesses, so as to detect and trace hidden messages.

• Recent attempts by some governments to limit online free speech and the civilian use of cryptography have spurred people concerned about liberties to develop techniques for anonymous communications on the net, including anonymous re-mailers and Web proxies.

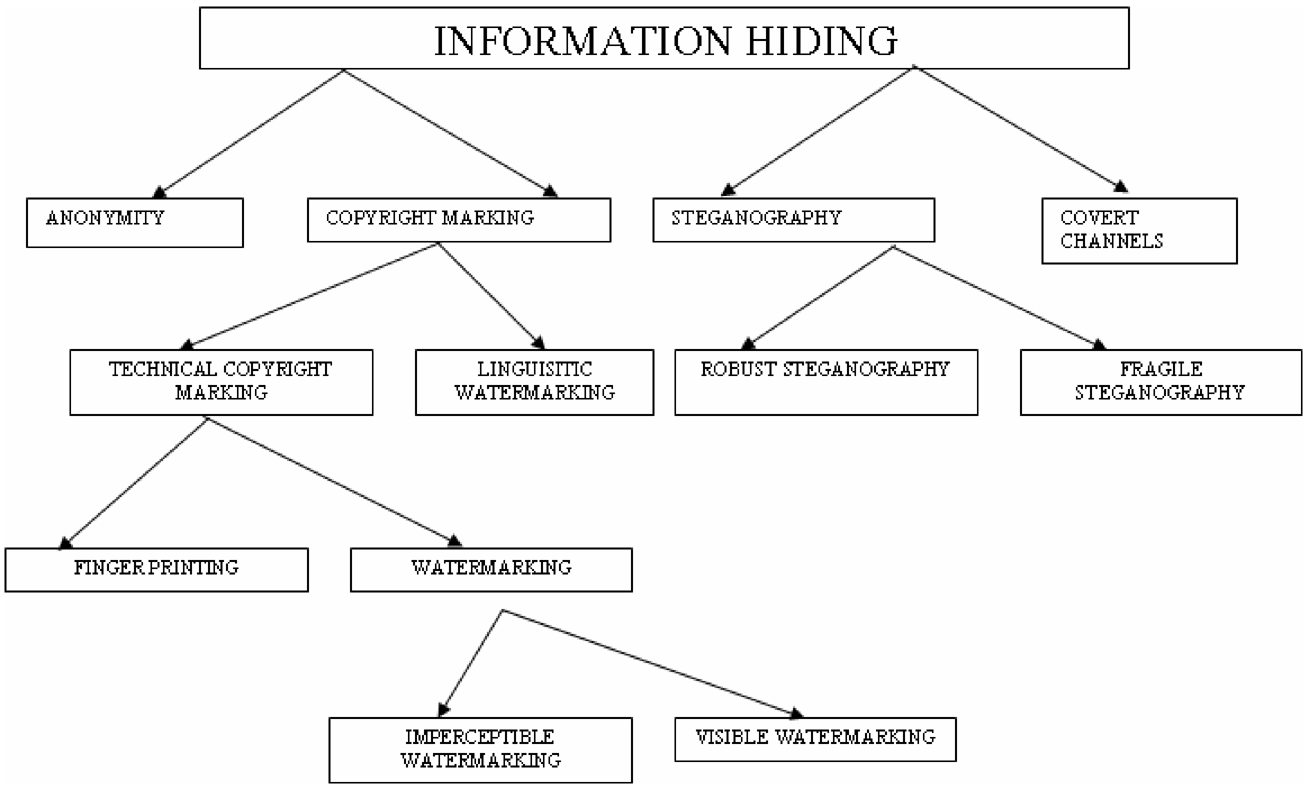


Figure.1 Classification of Information Hiding Techniques

• Schemes for digital elections and digital cash, make use of anonymous communication techniques.

• Marketers use email forgery techniques to send out huge numbers of unsolicited messages while avoiding responses from angry users.

The paper presentation is organized as follows. In Section II, a general framework for LSB steganalysis is exploited. Section III introduces adaptive steganography using filtering to take into account the sensitivity of the human visual system and also various statistical parameters generally being used by steg-analysis algorithms. Section IV details about steganlaysis using IQM by implementing ANOVA tests and performing regression analysis Section V investigates the experimental results.

II. Lsb steganography:

A widely used digital steganography technique is the least significant bit embedding (LSB embedding). In LSB steganography, the secrete messages, that is encrypted, are hidden in the LSBs of the samples of a digital signal. The perceptual transparency of the LSB steganography is easily achieved by the camouflage of noises inherent to digital signal acquisition process. In designing digital sensors, the quantizer sets the LSB of the binary sample representation at or even below the level of sensor noise energy in order not to lose precision.[1],[7]. This common engineering practice has seemingly made LSB steganography an attractive and popular technique.

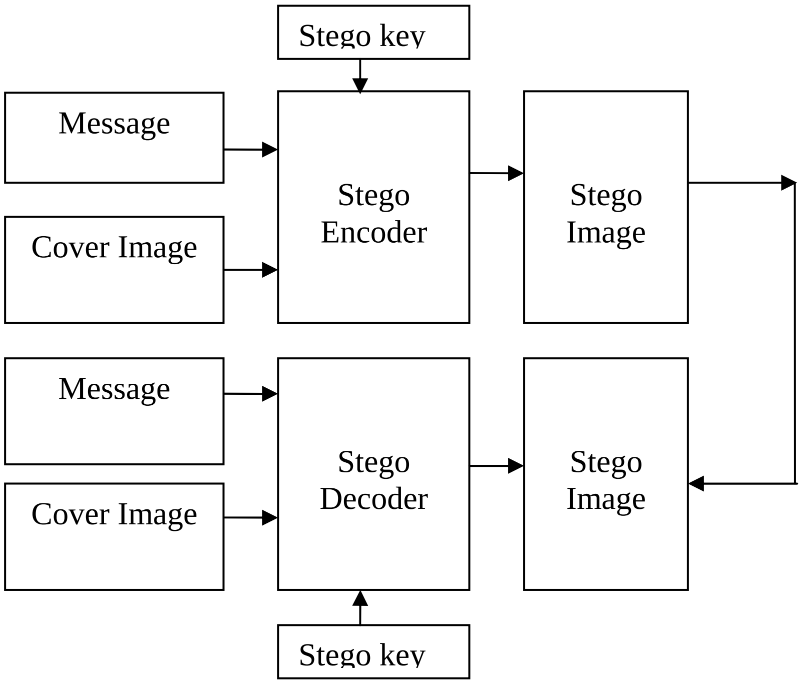


Figure 2. Basic Stegnographic model

III. Adaptive steganography using filtering

Adaptive Steganography reduces modifications to the image, and adapts the message embedding technique to the actual content and features of the image [2]. In general, to keep a good degree of stealthness, Adaptive methods embed message bits into certain random clusters of pixels (avoiding areas of uniform color) selecting pixels with large local standard deviation or image blocks containing a number of different colors.

The main advantage of adaptive steganography is that, the changes made to the cover image take into account the sensitivity of the human visual system and also various statistical parameters generally being used by steganalysis algorithms. The main challenge posed to existing adaptive steganography techniques is that the methods so far developed doesn't seem to have a way to control the amount of information that is to be hidden, for a given cover image. This problem is overcome in the method presented in this paper.

The proposed approach utilizes the sensitivity of the human visual system to adaptively modify the intensities of some pixels in a high frequency components spatial image (HFSI) of the cover image. The modification of pixel intensities depends on the magnitude of the pixels in HFSI and also on the local features of the cover image. If the contrast of the image is large (e.g., an edge), the intensities can be changed greatly without introducing any distortion to human eyes. On the other hand, if the contrast is small (e.g., a smooth surface), the intensities can only be tuned approximately.

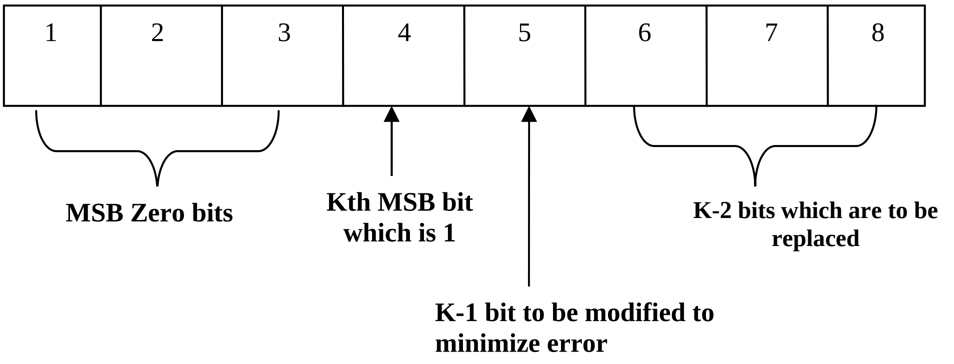

1
2
3
4
5
6
7
8
MSB Zero bits
Kth MSB bit which is 1
K-2 bits which are to be replaced
K-1 bit to be modified to minimize error

Figure 3 Embedding Algorithm

In this method, first the cover image is passed through a filter to separate the high and low frequency components of the image. The inverse transform of both the images is computed. Now the pixels values of HFSI are modified depending on the magnitude of the pixel i.e. more the magnitude more the Least Significant Bits (LSB's) of that pixel are changed and also the local features of cover image are considered. Now both the LFSI (Low Frequency components spatial image of cover image) and HFSI are added to form the stego -image. At the receiver the reverse process is to be done to recover the message.

IV. Steganalysis using iqm

The main goal of this paper is to develop a discriminator for cover images and stego images, using an appropriate set of IQMs [3]. Image quality measurement continues to be the subject of intensive research and experimentation. Objective image quality measures are based on image features, a functional of which, should correlate well with subjective judgment, that is, the degree of (dis)satisfaction of an observer. Objective quality measures have been utilized in coding artifact evaluation, performance prediction of vision algorithms, quality loss due to sensor inadequacy etc. This paper exploits image quality measures, not as predictors of subjective image quality or algorithmic performance, but specifically as a steganalysis tool, that is, as features in detecting watermarks or hidden messages [8].

In order to understand how these metrics measure analysis of variance (ANOVA) technique is used . Specifically, ANOVA was used to show whether a metric’s response was consistent with a change in the image or whether it was a random effect. The ranking of the goodness of the metrics was done according to the F-scores in the ANOVA tests to identify the ones that responded most consistently and strongly. The final analysis seek IQMs that are sensitive specifically to steganography effects, that is, those measures for which the variability in score data can be explained better because of some treatment rather then as random variations due to the image set. In the design phase of the steganalyzer, the normalized IQM scores are regressed [4] as, -1 and 1, depending upon whether an image did not or did contain a message. Similarly, IQM scores were calculated between the original images and their filtered versions.

In this context steganalysis refers to the body of techniques that are designed to discriminate between cover-objects and stego-objects. The method proposed in this work can be used to discriminate between images that have been subjected to steganography using any methods. The metrics that show significant result for each type, passive warden steganography and active warden steganography, are specified. The techniques presented here are novel and works well for any type of embedding technique [5],[6].

- A good Image Quality Metric should be accurate, consistent and monotonic.
- Prediction accuracy can be interpreted as the ability of the measure to detect the presence of hidden messages with minimum error on average
- Prediction monotonicity signifies that IQM scores should ideally be monotonic in their relationship to the embedded message size or watermark strength.
- Prediction consistency relates to the quality measure’s ability to provide accurate predictions for a large set of steganographic techniques and image types. This implies that the spread of quality scores due to factors of image variety, active warden or passive warden steganography methods should not eclipse the score differences arising from message embedding artifacts.

V. Experimnetal results

The experimental results demonstrates the effectiveness and robustness of the new steganalysis framework. Instead of Higher order statisitics, in this project estimation of the hidden message length is done using the Matlab software itself. It uses the LSB and Adaptive steganography which aims at embedding and retrieving the hidden message in the image file. And also it incorporates Image Quality Metrics for steganalysis. Perhaps more significantly, this project presents a general framework for a class of steganalysis techniques that estimate hidden message length by measuring some signature statistical quantity such as Mean square error and Peak Signal to Noise Ratio as shown in the Figures 7,8,10 and 11.

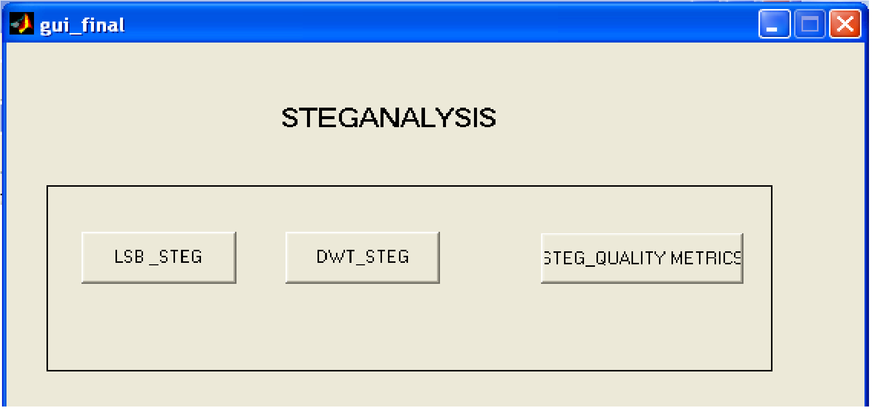
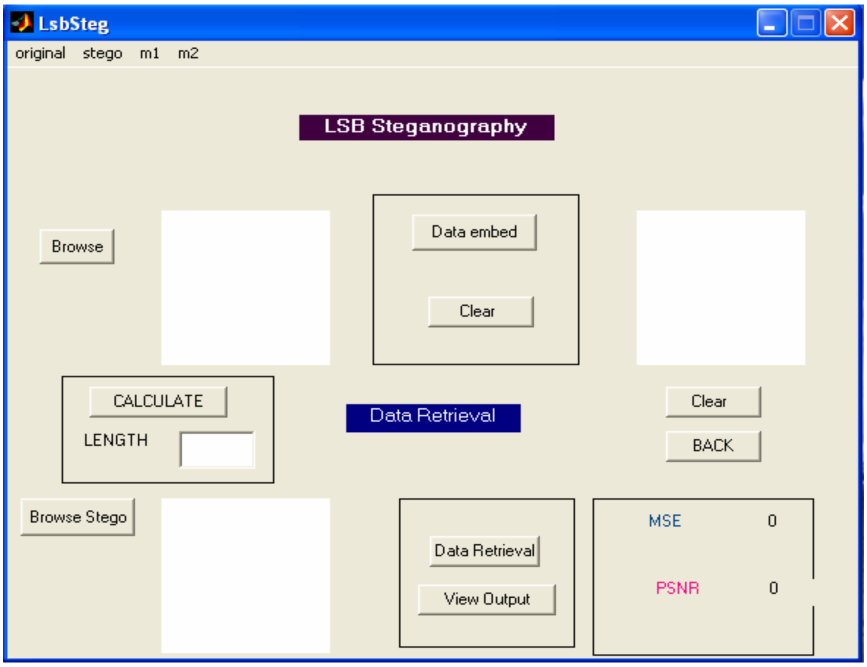


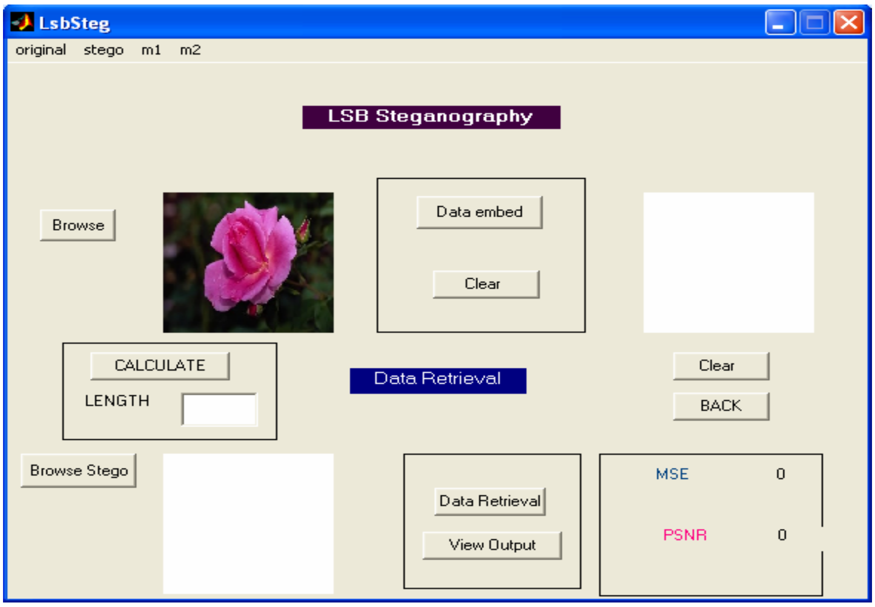
Figure 4 OUTPUT GUI



MSE 0

PSNR 0

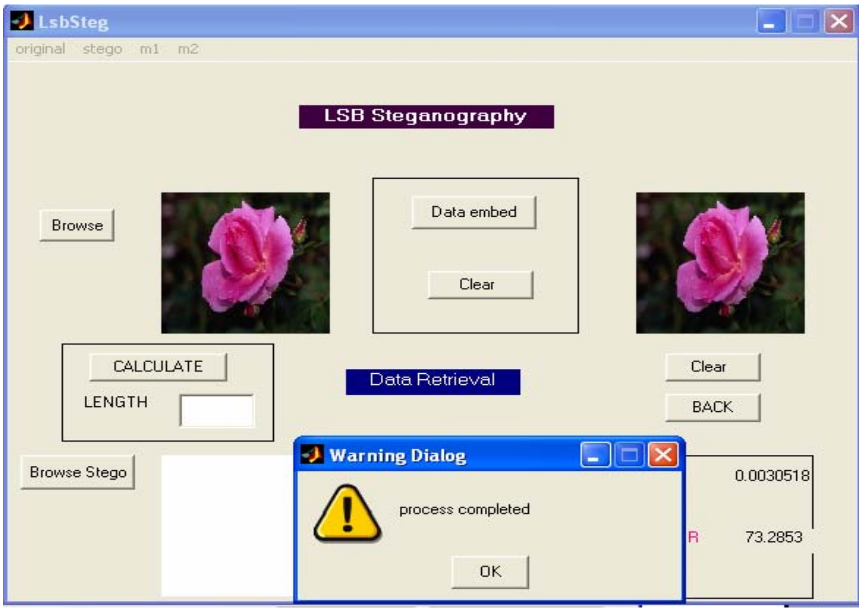
Figure 5 LSB STEGANOGRAPHY



MSE 0

PSNR 0

Figure 6 Cover Image for LSB Steganography



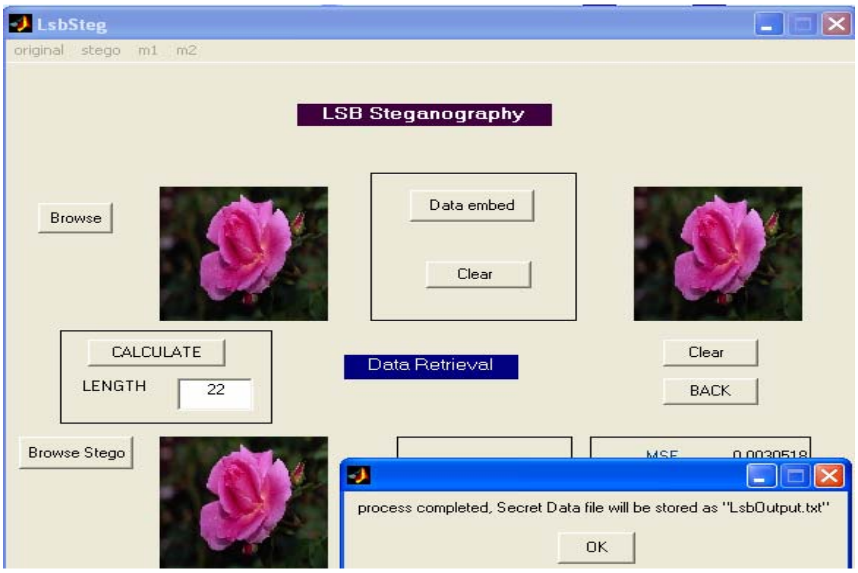
LENGTH

process completed

0.0030518

R 73.2853

Figure 7 Data Embedded Image for LSB Steganography

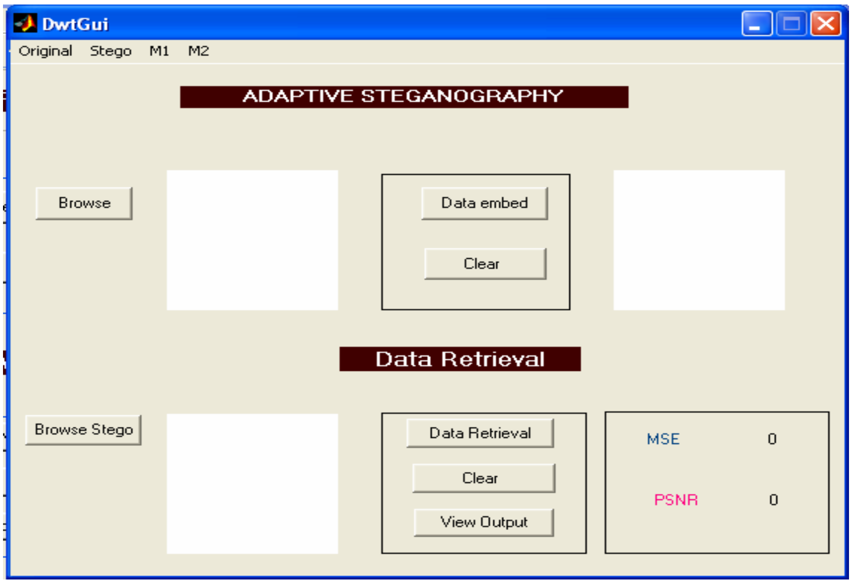


LENGTH 22

MSE 0.0030518

process completed, Secret Data file will be stored as "LsbOutput.txt"

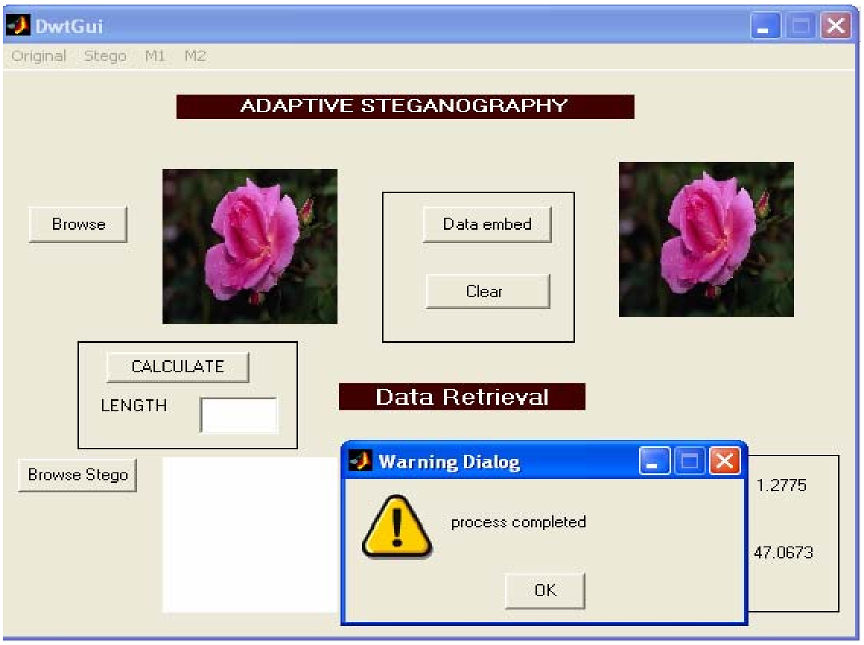
Figure 8 Data Retrieved Image for LSB Steganography



MSE 0

PSNR 0

Figure 9 Output GUI for Adaptive Steganography



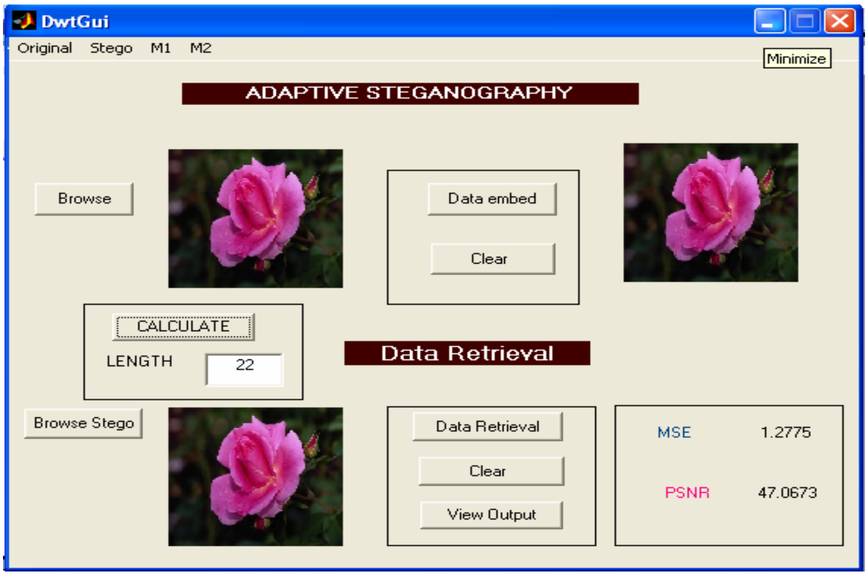
LENGTH

process completed

1.2775

47.0673

Figure 10 Embedded for Adaptive Steganography

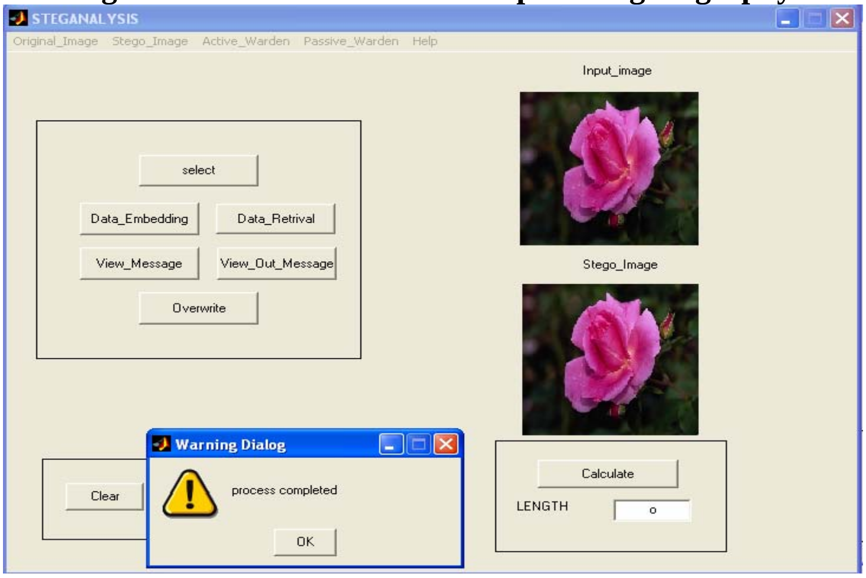


LENGTH 22

MSE 1.2775

PSNR 47.0673

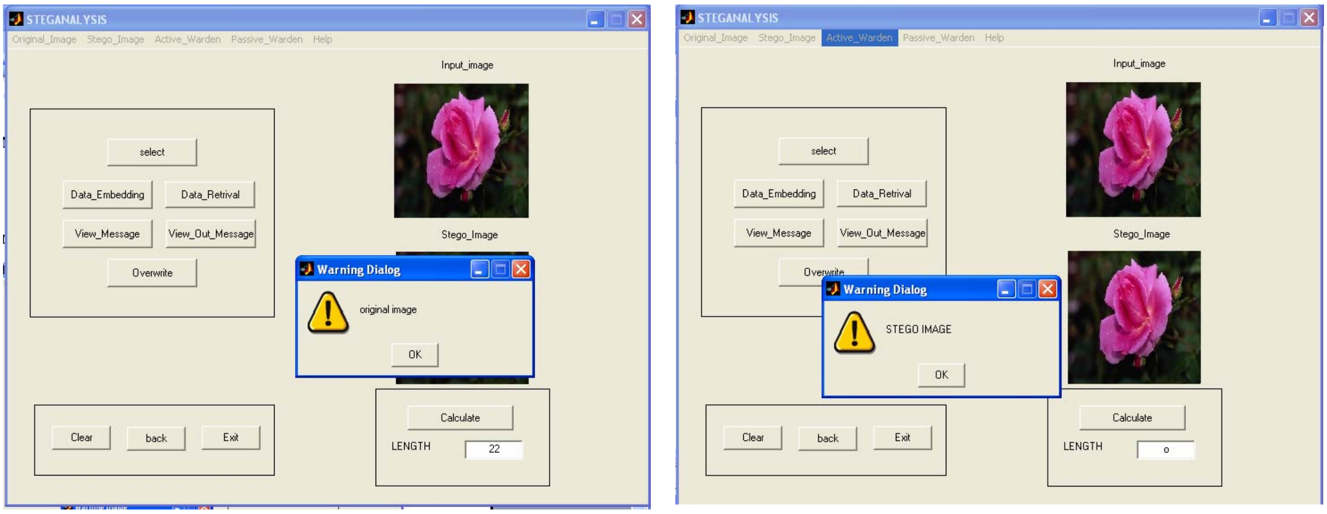
Figure 11 Data retrieval for Adaptive steganography



process completed

LENGTH 0

Figure 12 Embedded Image for Steganalysis



original image

STEGO IMAGE

Figure 13 Steganalysis for Active warden

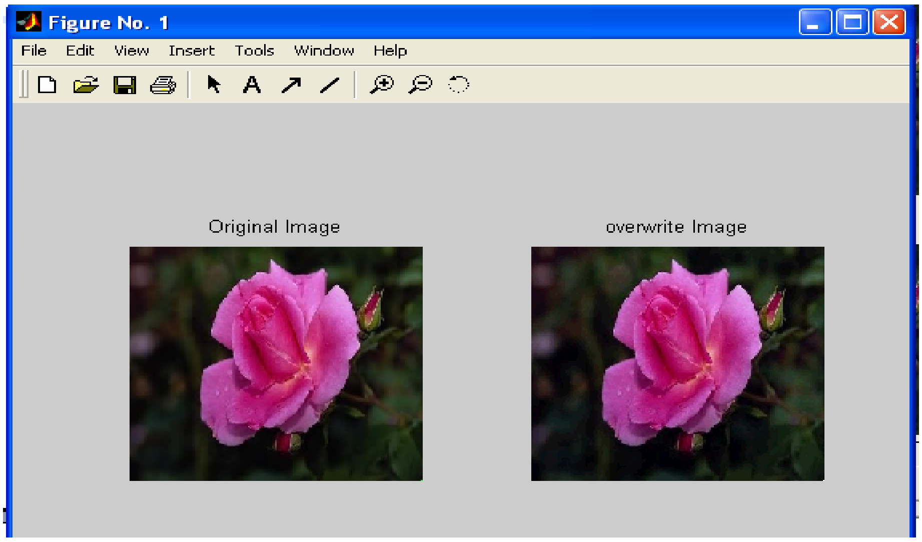
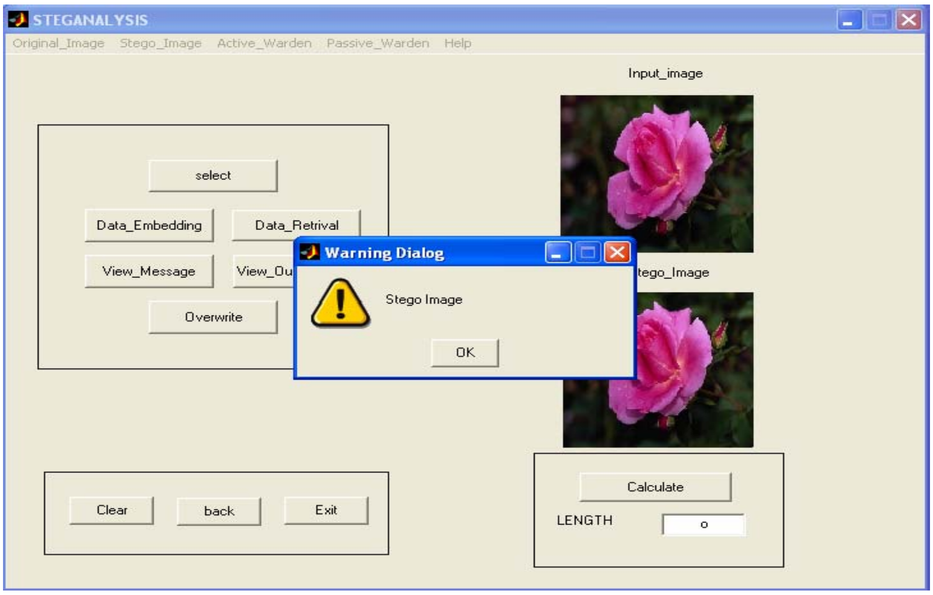


Figure 14 Data overwrite



Stego Image

Figure 15 Steganalysis for Passive warden

VI. conclusion and future work

A new general framework for LSB steganalysis of digital media contents was developed. For natural digital signals encountered in daily life such as image, the proposed framework can be used to estimate the hidden message length. This paper, addressed the problem of steganalysis of images, and developed a technique for discriminating between cover-images and stego-images based on the hypothesis that message-embedding schemes leave statistical evidence or structure in images that can be exploited for detection. For this purpose IQM image algorithm that offers better discriminative power to identify good features was implemented using ANOVA and Multivariate Regression analysis which is an optimal classifier.

Implementation of Adaptive Steganalysis for higher embedding capacity, enhanced security and selection cut off frequency for good visual perception was performed. This new method of adaptive steganography with higher embedding capacity is controlled through the filter cut-off frequency that was analyzed and shown to have a very high confidentiality due to the sharpness of information recovery with the cut-off frequency. In future the work can extended , by designing a frame work for digital media such as audio , video etc. and also advanced techniques and algorithms like spread spectrum , Fuzzy logic, Neural Networks can be implemented to improve its embedding and detection performance.

VII. References

1. M. M. Amin, M. Salleh, S. Ibrahim, M. R. K.Atmin and M. Z. I. Shamsuddin, "Information Hiding using Steganography", 4th national Conference on Telecommunication Technology, NCTT 2003, IEEE. Pp 21 - 25. January 14-15, 2003.
2. R. Chandramouli, N.D. Memon and G. Li, "Adaptive Steganography", Proc. Security and Watermarking of Multimedia Contents III, Special session on Steganalysis, SPIE Photonics West, Calif. 2002, pp. 69-78.
3. A. M. Eskicio˘glu and P. S. Fisher, “Image quality measures and their performance,”*IEEE Trans. Commun.*, vol. 43, pp. 2959–2965, Dec. 1995.
4. A. C. Rencher, *Methods of Multivariate Analysis*. New York: John Wiley, 1995, ch.6, 10.
5. M. Kutter, S. Voloshynovskiy, and A. Herrigel, “The watermark copy attack,” in *Proc. SPIE Conf. on Security and Watermarking of Multimedia Contents II*, San Jose, CA, 2000, pp. 371–380.
6. “Steganalysis of images created using current steganography software,” in *Proc. Workshop on Information Hiding*, ser. Lecture Notes in Computer Science. Portland, OR: Springer-Verlag, 1998, vol. 1525, pp. 273–289.
7. Chris Shoemaker, Prof Rudko “Hidden Bits: A Survey of Techniques for Digital Watermarking Independent Study EER-290 Spring 2002.
8. A.Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” in *Proc. 3rd Information Hiding Workshop*, Dresden, Germany, 1999, pp. 61–76
9. http://en.wikipedia.org/wiki/Steganography
10. http://data-hiding.com/

Article received: 2009-06-29