IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Research Paper on Image Stegnography

Priyanka Sharma[1], Astha Gautam[2], Ruchi Singh[3]

M.Tech. Student, Computer Science & Engineering, LRIET, Solan, India[1]

Assistant Professor, Computer Science & Engineering, LRIET, Solan, India[2]

Assistant Professor, Computer Science & Engineering, LRIET, Solan, India[3]

Abstract: The steganography is a powerful security method with which we can hide a secret message inside an object. Steganography is a technique used to protect the data by just hiding the data into data or information behind information. Currently, many types of steganography techniques are being used such as text, image, audio/video and protocol but digital images are the most widely used. There are many steganography procedures in which everyone has its own strength and weakness in terms of security and complexity. Some of which provides hiddenness of information while some provides a huge secret message to be hidden. This dissertation provides an overview of steganography specially image steganography and its uses. It attempts to design and develop the good steganography algorithm and briefly describes about the Least Significant Bit image steganography algorithm. In this dissertation, two parameters are used in order to measure the quality of image. First is PSNR and second is MSE.

Keywords: Steganography, Visual Cryptography, Steganography Techniques, Stego Image, PSNR, MSE.

I. INTRODUCTION

The word "Steganography" comes from the Greek steganos (covered or secret) and graphy (writing or drawing) and thus means, literally, covered writing. It is a data hiding techniques, which aims at transmitting a message on a channel where some other kind of information is already being transmitted. The goal of steganography is to hide messages inside the images in such a way that does not allow any "enemy" to even detect that there is a secret message present in the image. Steganography attempts to hide the existence of communication. The basic structure of Steganography is made up of three components:

- The Carrier image
- The Message
- The Key

The carrier can be a painting, or a digital image. It is the object that will "carry" the hidden message. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light, or even lemon juice.

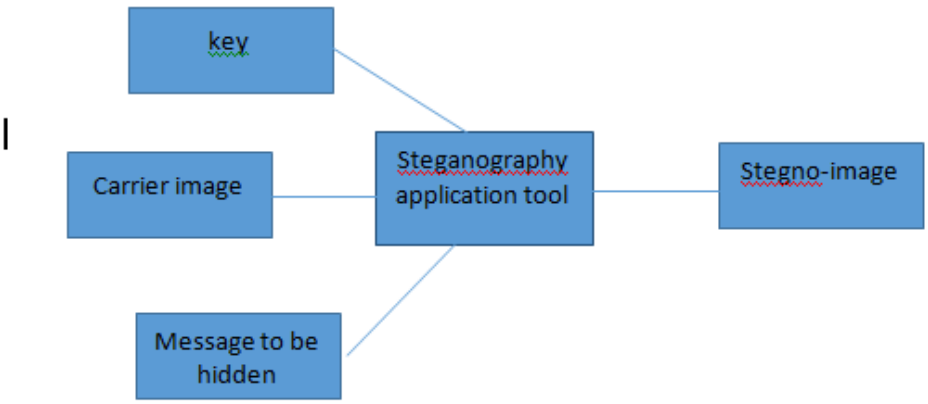

Fig 1. Block Diagram of steganography

II. NEED OF STEGANOGRAPHY

Currently, the use of internet increasing quickly. One of the most important area which attracted by people is security is related to internet and also related to communication. At present, security for hiding data is most popular technique

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

which receives more attention than cryptography. Various methods such as cryptography, coding Steganography, etc. are used for hidden communication. The major benefit of Steganography over other coding techniques is that it hiding the data inside other data in such a way that no other person recipient, even know the existence of it.

A. Terms used in Steganography are:
i. Cover Image
The medium in which information is to be hidden. It may be an audio, video, image or a text file.
ii. Key
It's a secret value which help in encoding or extraction of data, without which data cannot be encode and extract.
iii. Stego-image
A medium within which information is hidden.

B. Message
The data to be hidden or to be extracted.
For Steganography, the size of cover image can be of any size -8 bit, 24 bit, 32 bit, 36 bit. The image can be in any format either jpeg, gif, bmp, etc. we have a key which is used to select the random pixels in which data is to hide. Therefore Stego image is generated which is send to another person. Now on the receiver side the Stego image is processed and extraction of message can be done with the help of secret key. The key is the one by which receiver knows the position of the pixel on which message is rooted.

III. CLASSIFICATION OF STEGANOGRAPHY

- Text based Steganography
- Image based Steganography
- Audio based Steganography
- Video based Steganography

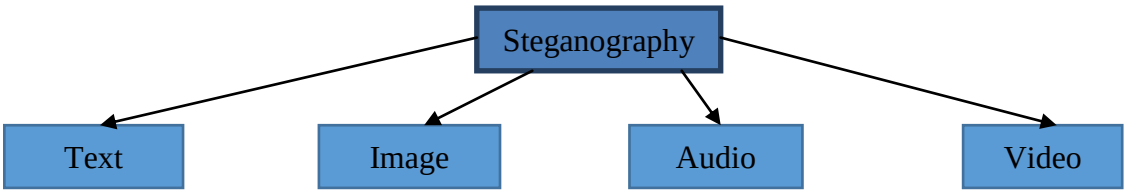

Fig 2. Steganography types

A. Text-based Steganography
In this, the message that is to be sent is rooted firstly in a text file by formatting. The format it based on line-shift coding, word-shift coding, feature coding etc. Reformatting of the text destroys the rooted content hence the technique is not robust.

B. Audio Steganography
This Alters audio files so that they contain hidden messages. The techniques are LSB manipulation, phase coding and echo hiding.

C. Image Steganography
This Steganography hides the message in the images. This is the most popular technique because of the fact that almost no perceivable changes occur. Some of the commonly used methods of embedding payload in cover image are least Significant Bits (LSB) substitution in which the LSBs of cover image pixel are altered to hide the payload and more data can be hidden in edges.

D. Video Steganography
Video Steganography is a technique to hide files or information into digital video format. Video is used as carrier for hidden information. Generally discrete cosine transforms (DCT which is used to hide the information in each of the images in the video, which is not visible by the human eye.

IV. STEGANOGRAPHY TECHNIQUES

There are some approaches in classifying the Steganography techniques are given below:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

A. Substitution Technique
These techniques try to encode secret data by substituting insignificant parts of the cover image by secret data bits. It consists of many techniques such as least significant bit substitution, pseudorandom permutation etc.

B. Transform Domain Technique
These techniques conceal message in a significant area of the cover image which makes them stronger to attack. It consists of DCT, DWT methods**.**

C. Spread Spectrum Technique
In this technique, it tries to extend a secret messtechnique, it is hard to remove the embedded message. It includes two types of methods: -one is direct sequence method and second is frequency hopping.

D. Distortion Technique
This technique requires the knowledge of original cover in the decoding process. Most text based hiding methods are of distortion type. age over a cover, in order to make it impossible to recognize.

V. PROPOSED WORK

In the proposed work we merge two techniques text steganography and image steganography. Proposed text based steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence construction.

A. Encoding
- Representation of each letter in secret message by its equivalent ASCII code.
- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts.
- Choosing of suitable letters from table 1 corresponding to the 4 bit parts.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
- Encoding is not case sensitive.

B. Decoding
- First letter in each word of cover message is taken and represented by corresponding 4 bit number.
- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

LETTER	CODE NO	LETTER	CODE NO. S
E	15	M	7
A	14	H	7
R	13	G	6
I	13	B	5
O	12	F	4
T	11	Y	4
N	11	W	3
S	10	K	3
L	10	V	3
C	9	X	2
U	8	Z	2
D	8	J	1
P	7	Q	0

Table 1. Number Assignment

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

VI. RESULT AND DISCUSSION

In this we have discussed about result of the proposed work. Firstly cover image is taken in which we have to hide the Stegokey. First we take a 1.png image and perform steganography and second we take cameraman.tif . calculate the values of PSNR and MSE.

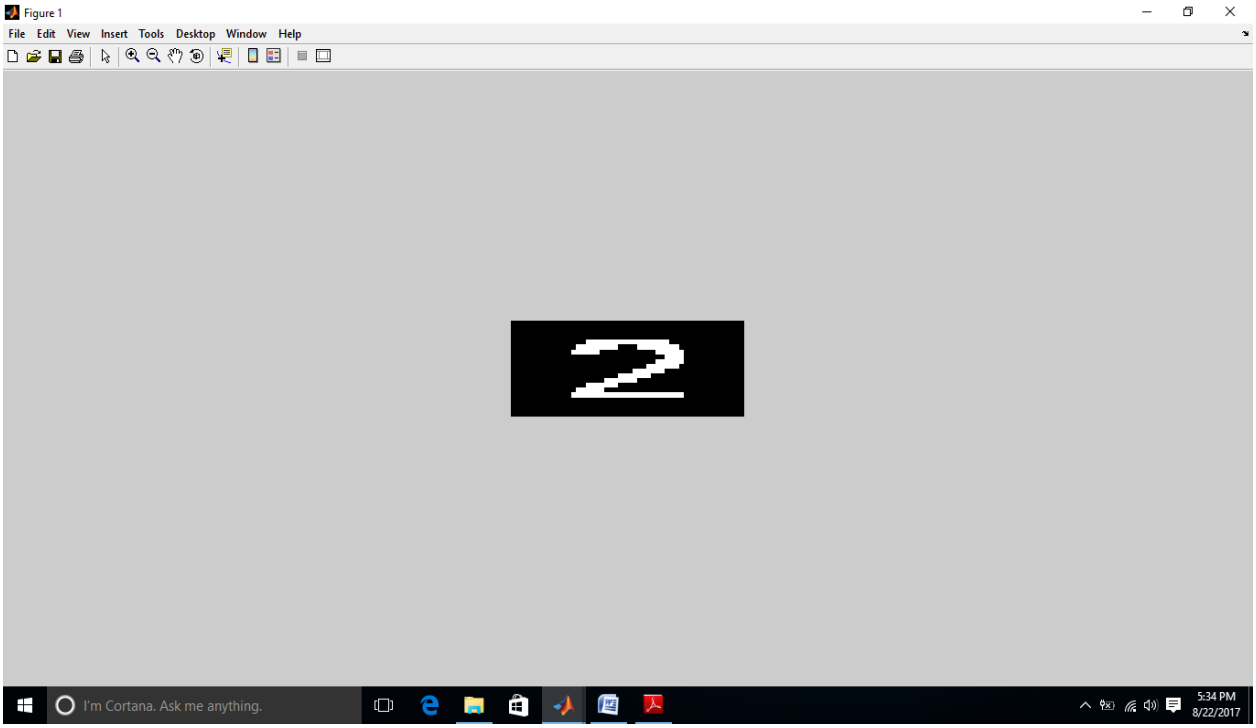

Fig 3. Stego key

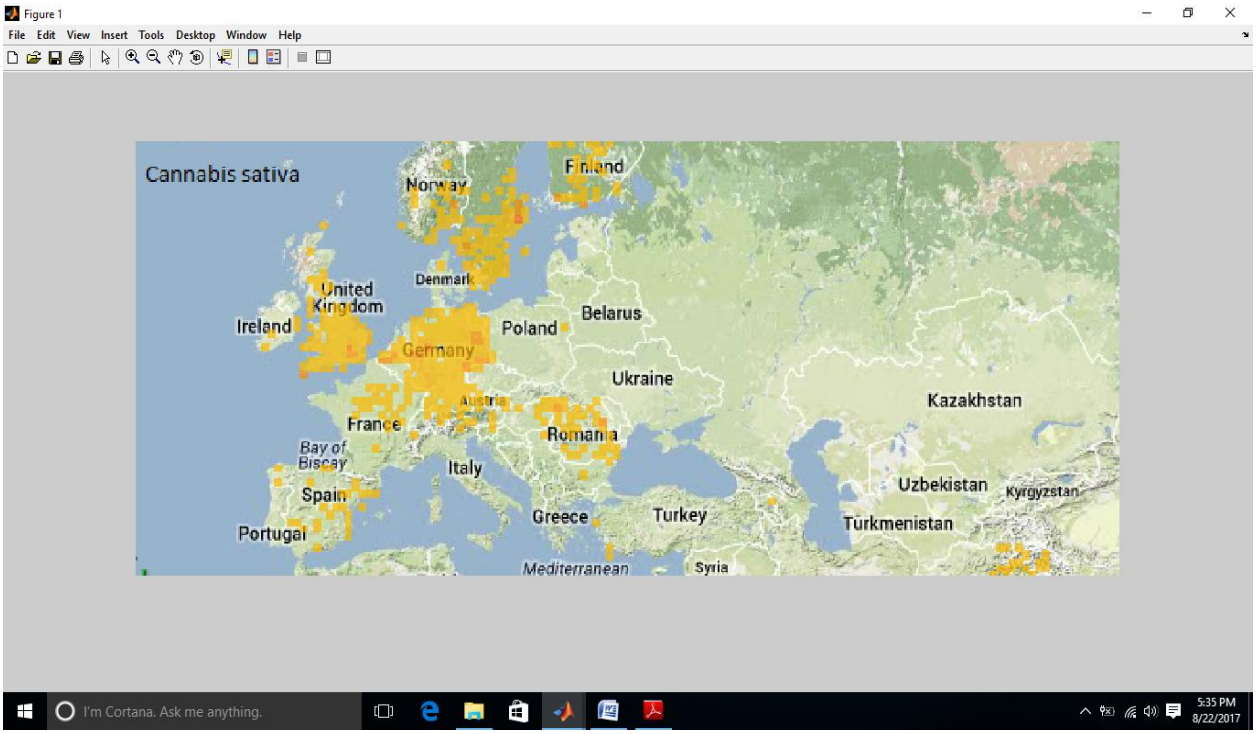

Fig 4. Cover image

DOI10.17148/IJARCCE.2017.6830

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

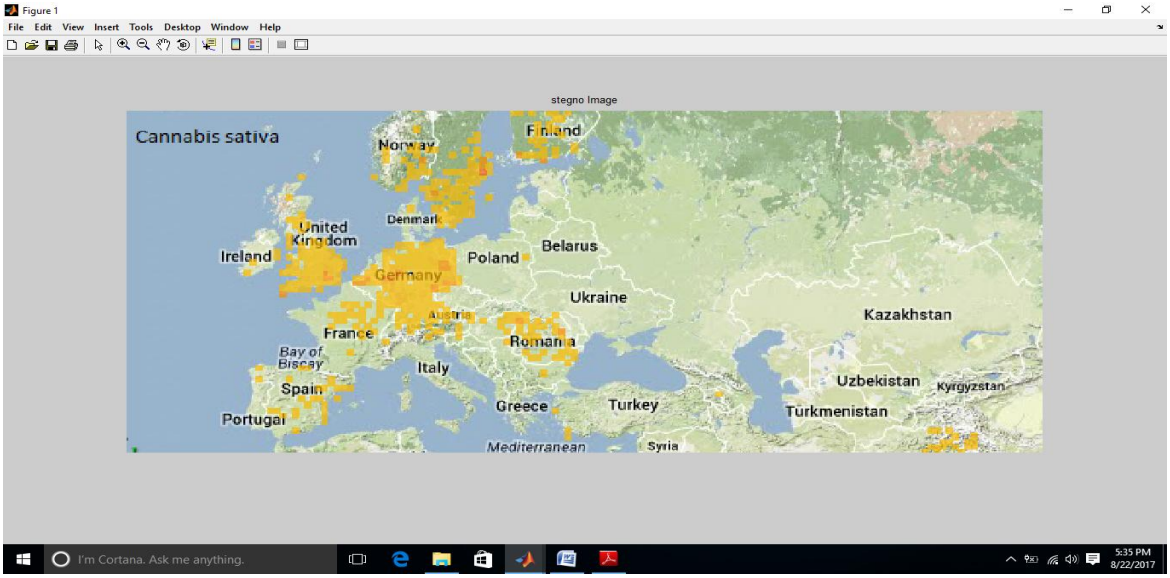

Fig 5. Stegno image

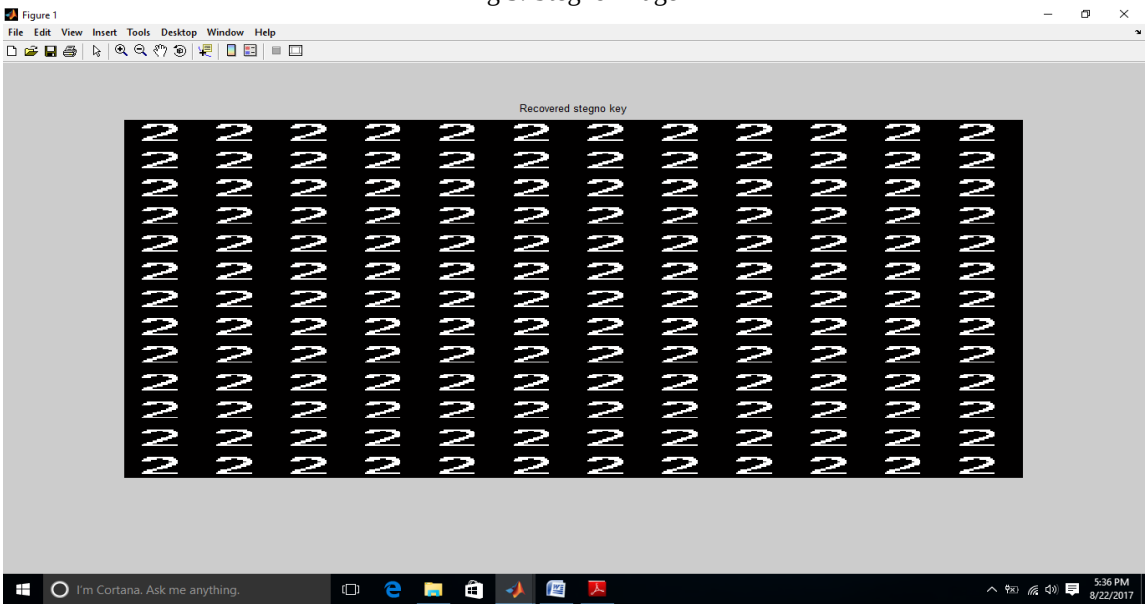

Fig 6. Recovered Stegno key

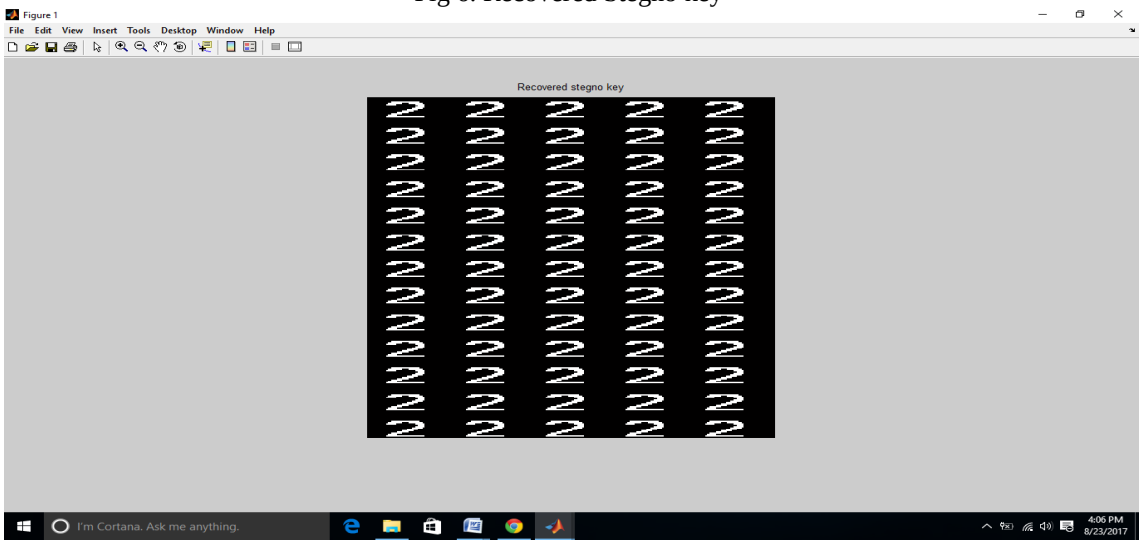

Fig 7. Stego key

DOI10.17148/IJARCCE.2017.6830

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Fig 8. Cover image

Fig 9. Stegno image

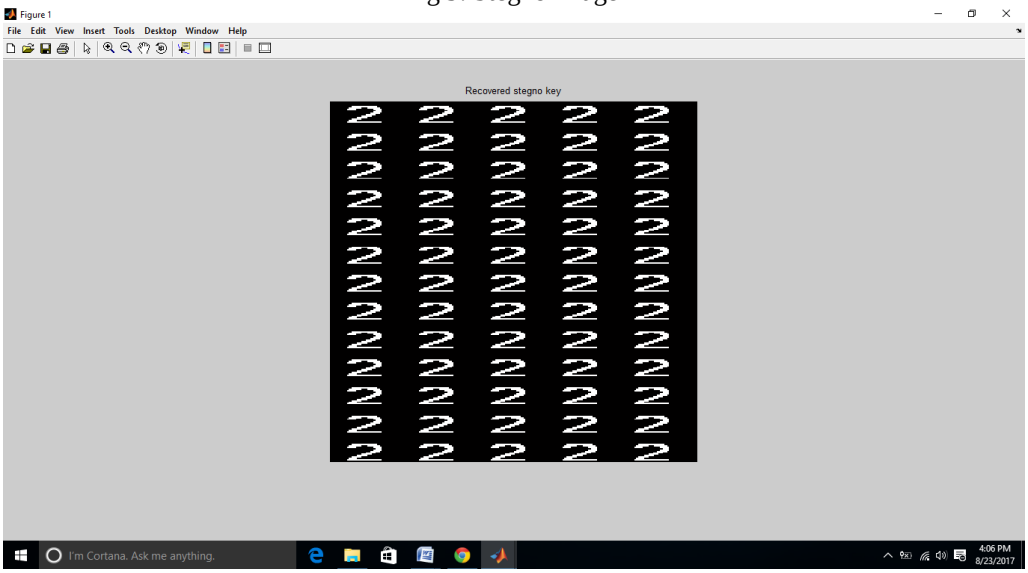

Fig 10. Recovered Stegno key

DOI10.17148/IJARCCE.2017.6830

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Table 2. PSNR and MSE Comparison

Images	PSNR	MSE
1.png	53.5426	0.1368
Cameraman.tif	70.2840	0.0199

A. PSNR (Peak Signal to Noise Ratio)

PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representmnbvcxz741a/852tion, because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codec"s. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image.

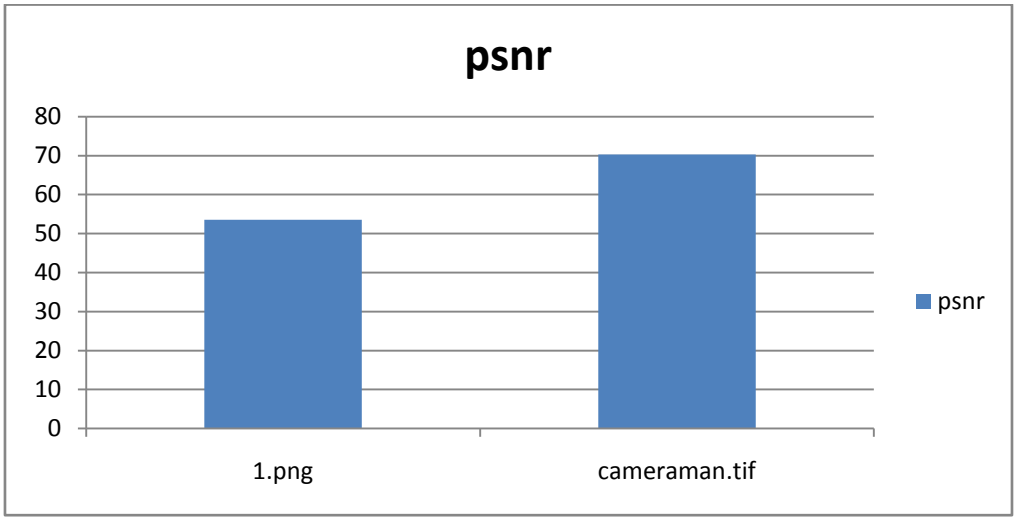

Fig 11. PSNR of images

B. MSE (Mean Squared Error)

MSE of an estimator measures the average of the squares of the error or deviations, that is, the difference between the estimator and what is estimated. The MSE assesses the quality of an estimator or predictor. MSE is a risk function, corresponding to the Expected value of the squared error loss or quadratic loss. When we compared these results with the results shown in previous work, we found that the mean square error value in previous work is more as compared to our work. The MSE assesses the quality of an estimator or predictor.

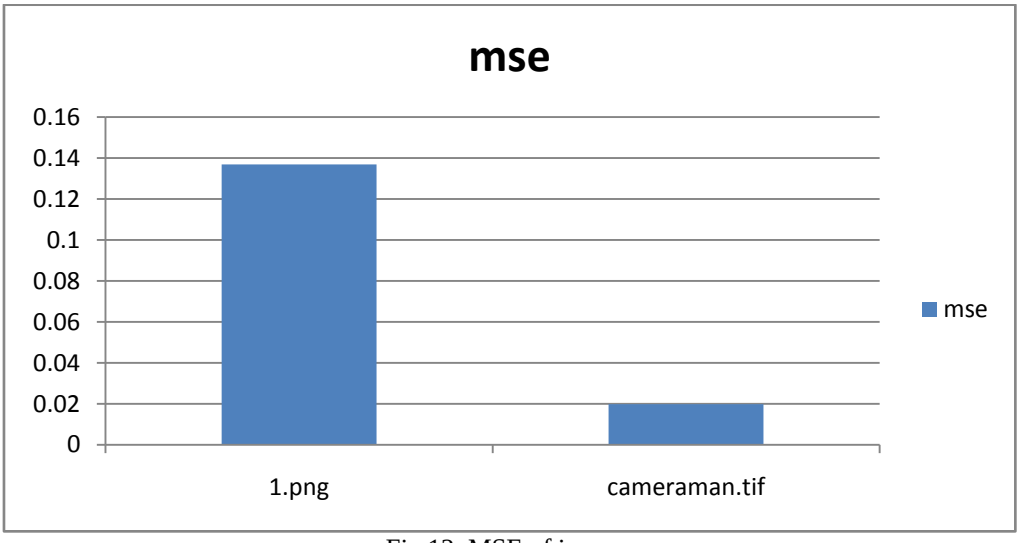

Fig 12. MSE of images

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

VII. CONCLUSION AND FUTURE WORK

Steganography is an effective way to hide sensitive information. In this paper we have used the LSB Technique on images to obtain secure stego-image. Our results indicate that the LSB insertion using simple LSB insertion is better than using random encoding technique. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key. The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image, so it is easy to be implementing in both gray scale and color image. This thesis focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate.

Our main goal in this research work is to give new insights and directions on how to improve existing methods of hiding secret messages, possibly by combining Steganography and Cryptography. We start by describing the main existing methods and techniques in Steganography that allow us to hide the existence of a message. We then illustrate the different approaches that help us achieve a higher level of secrecy and security, together with their limitations. The first method is about combining Steganography and Cryptography in such a way to make it harder for a Stegoanalyst to retrieve the plaintext of a secret message from a stego-object if cryptanalysis were not used. In the proposed work we merge two techniques text Steganography and image steganography for secure information hiding. In this work,we provide two level securities to message. First we apply encoding and decoding based text steganography, secondly, using image steganography with LSB for higher level security and we increase the PSNR value of stego image.

In future we apply various filtering techniques on it and improve PSNR and MSE.

REFERENCES

[1] Stuti Goel, Arun Rana and Manpreet kaur, "Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems, vol.3, May 2013, pp. 20-30.
[2] Himanshu Gupta, Ritesh Kumar and Soni Changlani, "Steganography Using LSB Bit Substitution for Data Hiding", International Journal Of Advanced Research in Computer Science and Electronics Engineering, vol.2, October 2013, pp. 676-680.
[3] Vikas Tyagi, Atul Kumar, Roshan patel, Sachin Tyagi and Saurabh Singh Gangwar," Image Steganography using Least Significant Bit With Cryptography", Journal of Global Research in Computer Science, vol.3, March 2012, pp. 53-55.
[4] Vijay Kumar Sharma and Vishal Shrivatav, "A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimizing Detection", Journal of Theoretical and Applied Information Technology, vol.36, February 2012, pp.1-8.
[5] Navdeep Kaur and Sukhjeet K.Ranade, "High Capacity Data Embedding System in DCT Domain for Colored Images", International Journal of Computing and Business Research, vol.3, September 2012.
[6] Zaidoon Kh.Al-Ani, A.A Zaidan, B.B Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography", Journal of Computing, vol.2, March 2010, pp.158-165.
[7] Khan Farhan Rafat and Muhammad Sher, "Survey Report: - State of the Art in Digital Steganography Focusing ASCII Text Documents", International Journal of Computer Science and Information Security, vol.7, 2010, pp.63-72.
[8] Nadeem Akhtar, Pragati Johri and Shahbaaz Khan, "Enhancing the Security and Quality of LSB Based Image Steganography", Proceedings of IEEE International Conference on Computational Intelligence and Communication Networks, September 2013, pp.385-390.
[9] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding Using Digital Images", Defence Science Journal, vol.62, January 2012, pp.11-18.
[10] Mamta Juneja and Parvinder S. Sandhu, "An improved LSB based Steganography with Enhanced Security and Embedding/ Extraction", Proceedings of IEEE International Conference on Intelligent Computational Systems, January 2013, pp. 29-34.
[11] Gopika Mane, Priti Deshmukh, Sukul Fadnis, Sheetal Jadhav and Manoj S.wakchoure, "Imperceptible Stego- Marked Image Manipulation for Encrypted Data Hiding", International Journal of Application or Innovation in Engineering & Management, vol.2, October 2013, pp.72-77.