A NOVEL APPROACH TO THE INFORMATION SECURITY USING RC4 AND LSB TECHNIQUES

Sri Ram Polisetty[1] Niharika Tangella[2], Lavanya B [3], Geetha Sri DS [4], Ishwarya L [5]

[1,2,3,4,5] CSE, Faculty of Engineering, Godavari Institute of Engineering and Technology (A), Rajahmundry, A.P, INDIA.

Abstract: *Steganography is the art of hiding data within data where it is an encryption technique that can be used along with cryptography as an extra-secure technique to secure data. The security of information can be prospered by using encryption and steganography. In cryptography, at first the original form of data is encrypted into another form and then it is transferred. The proposed system improves the security system by combining these two techniques. In this system, the encrypted data is embedded in a BMP/JPEG image file and intends for data confidentiality, data authentication and data integrity. Data is encrypted with RC4 encryption algorithm and then embedded the encrypted data in the BMP/JPEG image file using LSB steganographic method where the primary goal of this system could be attained.*

Index Terms - Steganography, Encryption, Cryptography, RC4, LSB, Decryption, Information Security.

I. INTRODUCTION

1.1 Need for Security

A severe issue for computer network is to avert data from getting confined to unauthorized users. So there is need for information security. For this reason encryption techniques were introduced which provides security for the information. Most encryption techniques have an easy implementation and are commonly used in the field of information security. Steganography is one of the best and tranquil techniques to hide data/information.

Steganography is art of hiding data that avoid the detection of hidden messages/data. Steganographic method consists of cover media into which the secret information is embedded. The embedding process produces a stego medium by substituting the information with data from hidden message. To hide information, steganography gives a huge chance such that no one knows the existence of hidden message/data.[1][2]

1.2 Steganography

In steganographic model, message is the data that the sender wants to keep it confidential. The message can be plaintext, cipher text, other image, or anything that can be embedded. The cover medium with the embedded message is called as stego-object. The below figure shows the Steganography Process Model[1][2][3]

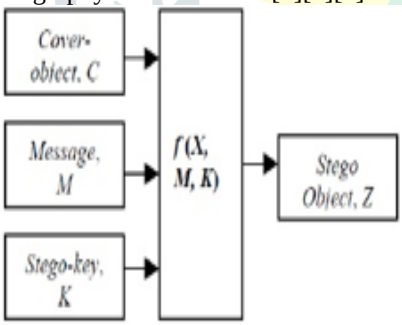

Figure1: Steganographic Process Model

1.3 Cryptography

Cryptography uses mathematics to encrypt and decrypt data. Cryptography aids to store important information, so that it cannot be read by any intruder except the intended receiver. The Encryption and Decryption process in Cryptography are shown in Figures respectively. [1][3]

1.4 Steganography and cryptography

Steganography and cryptography are well known and majorly used techniques that secure information in order to hide their presence. The figure 4 shows the Combination of Steganography and Cryptography. [1][4][5]

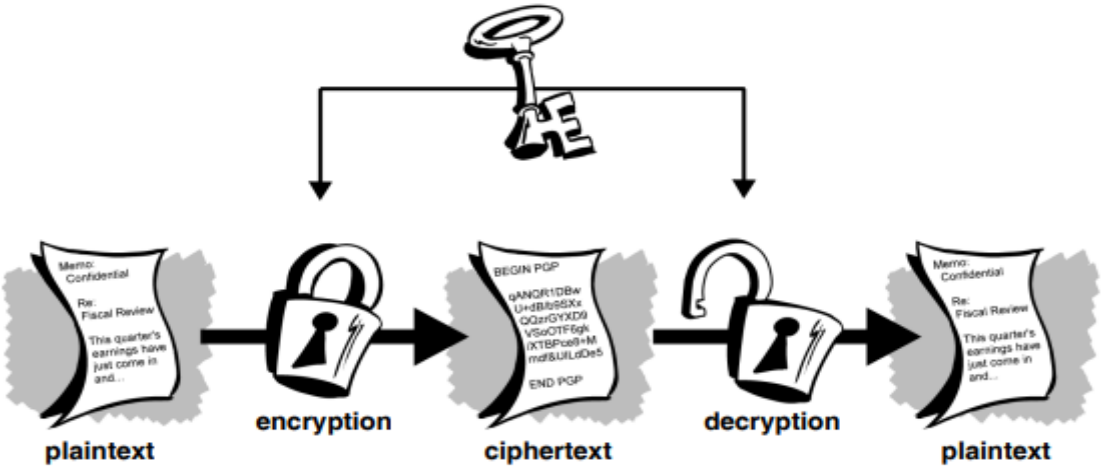

Figure2: Encryption process in cryptography

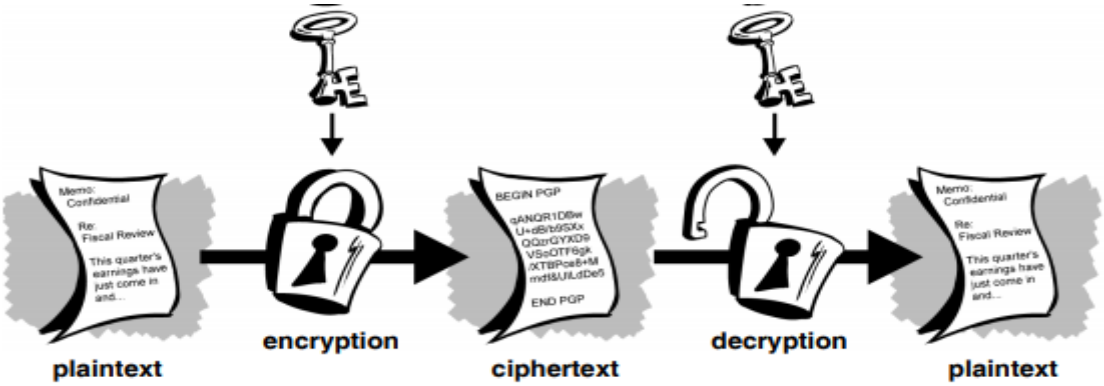

Figure3: Decryption process in cryptography

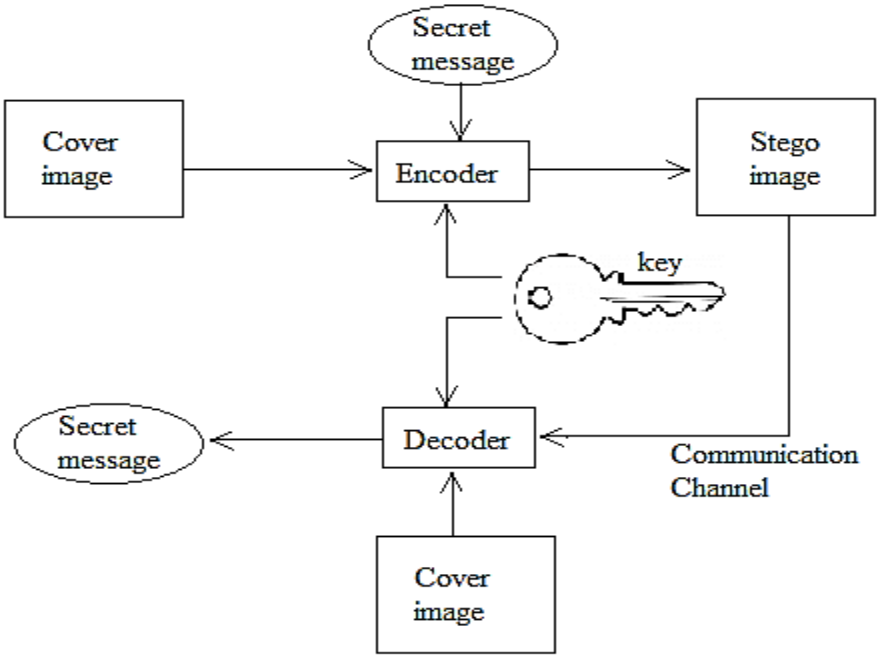

Figure4: Combination of Steganography and Cryptography

II. LITERATURE SURVEY

2.1 LSB ALGORITHM

The modest Steganography methodology is the least significant bits insertion i.e LSB. The secret messages are embedded directly. In LSB technique, the least significant bits of the pixels are substituted by the message bits which are permuted formerly embedding.[1][2][3]

The following examples show how the letter A can be out of sight in the first eight bytes of three pixels in a 24-bit image. Pixels:
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

A: 10000001
Result: (00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)
LSB insertion necessitates on average that half the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to hide the following character of the hidden message.
The advantages of Least-Significant-Bit steganographic data embedding is that it is easy to understand, easy to implement, and it produces stego-image that is almost close to cover image and its visual infidelity cannot *be judged* by human eyes.

2.2 RC4 ALGORITHM

RC4 is a stream cipher and symmetric key algorithm. The similar algorithm is used for both the encryption and decryption as well, as the data is XORed with the generated key. The key stream is totally sovereign of plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to produce a pseudo-random stream which is XORed with the plaintext to give the cipher text.
The input is XORed with these values. The encryption and decryption process is the same as the data stream is merely XORed with the generated key sequence. If it is fed in an encrypted message, it will produce the decrypted message output, and if it is fed in plaintext message, it will produce the encrypted version. [6][7]

Performance Measure

PSNR is most easily defined through the Mean Squared Error. *MSE* is defined as:

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

The PSNR (in dB) is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Here, MAX_I is the maximum pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. [8][9]

Tawfiq S. Barhoom, Sheren Mohammed Abo Mousa proposed a research article "*A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm"* where blowfish encryption Algorithm is proposed in the Steganographic system This work is concerned with implementing Steganography for images, with an improvement security and image quality.

Ms. Hemlata Sharma, Ms.MithleshArya, Mr. Dinesh Goyal proposed a research article "*Secure Image Hiding Algorithm using Cryptography and Steganography*" where the secret image is first encrypted by using BLOWFISH algorithm which has very good performance and is a most powerful technique compared to other Algorithms. The encrypted image is embedded with video using LSB Approach of steganography.

Tawiq S. Barhoom , Sheren Mohammed Abu Mousa proposed a research article entitled "*Secure Image Hiding Algorithm using Cryptography and Steganography*" where the experimental results shows that the stego-image is visually indistinguishable from the original cover image .It comes under the assumption that I the feature is visible, the point of attack is evident ,thus the goal here is always to cover up the very existence of the embedded data and that the algorithm has a high capacity and a good invisibility.

Pooja Rani, Mrs Preeti Sharma proposed a research article "*Cryptography Using Image Steganography"* where addition of an extra layer of security is added to provide safety to document in today's words. If any how intruder is able to detect the text in the image. Then also that text is no more than cipher text. Lots of techniques can be applied to get cipher text from plain text. Thus still intruder is far away from getting our precious data.

Hayfaa Abdulzahra, Robain Ahmed, Norzila Mohd Noor proposed a research article "*Combining Cryptography and Steganography for Data Hiding in Images*" where it is designed to combine the features of both cryptography and steganography, which will provide a higher level of security. It is better than the technique used separately. Simple LSB method was used to embed the secret message into the image. The last bit in each pixel used to conceal the message binary code.

Varsha, Dr.Rajender Singh Chhillar proposed a research article"*Data Hiding Using Steganography and Cryptography"* where a secured ADVANCED based LSB technique for image steganography has been proposed. An efficient stenographic method for embedding secret messages into cover images without producing any major changes has been accomplished through ADVANCEDLSB method. In this work, a new way of hiding information in an image with less variation in image bits have been proposed, which makes our technique secure and more efficient than LSB. 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.

Allam Mousa, Ahmad Hamad proposed a research article "*Evaluation of the RC4 Algorithm for Data Encryption"* where Analysis of the effect of different parameters of the RC4 encryption algorithm where examined and experimental work was performed to illustrate the performance of this algorithm based on changing some of these parameters. The execution time as a function of the encryption key length and the file size was examined; this has been stated as complexity and security.

Naitik P Kamdar, Dipesh G. Kamdar, Dharmesh N.khandhar proposed a research article"*Performance Evaluation of LSB based Steganography for optimization of PSNR and MSE"* where analysis of LSB based steganography In colour image. LSB based Steganography embed the text message in least significant bits of digital picture. Least significant bit (LSB) insertion is a simple, common approach to embedding information in a carrier/cover file.comaparative analysis is made to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods has been estimated by computing the mean square error (MSE) and PSNR (peak signal to noise ratio).the analysis shows PSNR and MSE improved in the LSB methods.

Mohammed Abdul Majeed , Rossilawati Sulaiman proposed a research article entitled *"An improved LSB Image Steganography technique using Bit-inverse in 24 Bit colour image"* where the technique have good quality of invisibility and undetectability. In terms of security property, two additional levels of security were added to the standard LSB steganography. The first level is that this technique only uses the green and blue colour instead of three colours red, green, and blue, in the standard LSB. The second level exploits the new bit inversion technique, which reverses the bits of the stego image pixels after the standard LSB is applied.

Tiyasa Gupta, Assouma Alassane Mouhamadou Hafifou, Ramachandra Tawker, Vaidhehi V proposed a research article "*An enhanced approach to steganography: obscurity***"** where Enhancement of the image steganography system using F5 Algorithm to provide a means of secure communication. A stegokey has been applied to the system during embedment of the message into the cover image as well as during extracting the message from the cover image. This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside them. The master work of this application is in supporting any type of images and any type of document file and lower limitation on file size to hide, because of the use of maximum memory space in pictures to hide the file.

Nadeem Akhtar, Pragati Johri, Shahbaaz Khan proposed a research article entitled "*Enhancing the Security and Quality of LSB based Image Steganography*" where bit inversion method enhances the stego-image quality. The enhancement in PSNR is not bounded. The improvement in PSNR may be very large for some image as in the case of TestPat image and for some other image, it may be small as for 3things image. For given a message image, a set of cover image can be considered and that cover image is selected for which the improvement is largest.

Govinda Borse, Vijay Anand, Kailash Patel proposed a research article "*Steganography: Exploring an ancient art of Hiding Information from Past to the Future"* where steganography is an art of hiding message and has been in use from thousands of years. But according to time the techniques used behind it is changing.

Dr.M.Umamaheswari, Prof.S.Sivasubramanian, S.Pandiarajan proposed a research article *"Analysis of Different Steganographic Algorithms for Secured Data Hiding*" where Success in steganographic secrecy results from selecting the proper mechanisms. However, a stego medium which seems innocent enough may, upon further investigation, actually broadcast the existence of embedded information. Development in the area of covert communications and steganography will continue. Research in building more robust methods that can survive image manipulation and attacks continues to grow. The more information is placed in the public's reach on the Internet, the more owners of such information need to protect themselves from theft and false representation. Systems to recover seemingly destroyed information and steganalysis techniques will be useful to law enforcement authorities in computer forensics and digital traffic analysis.

R.Nivedhitha, Dr.T.Meyyappan proposed a research article "*Image Security Using Steganography and Cryptographic Techniques"* where the combination of cryptography and steganography has been achieved by using the DES algorithm and LSB technique. Data encryption standard (DES) is used to encrypt secret image and LSB technique is used to hide encrypted secret image into cover image. To yield better imperceptibility the proposed method provided a higher similarity between the cover and stego pictures as a result. When steganography is combined with encryption a good security was achieved between two parties in case of secret communication, it is hardly attracted from eavesdropper by naked eye. Finally we can conclude that the proposed technique is effective for secret data communication.

III. PROPOSED WORK

In the existing system, Image Steganography using LSB algorithm has been used. And there is lack of data security due to the simplicity of the LSB algorithm. Due to this the intruder may tamper or steal the data. This is the problem addressed here and the feasible solution is proposed by us.

3.1 SYSTEM ARCHITECTURE

System architecture is the conceptual model that defines the structure, behavior, and more views of a system. Key operations in the proposed project are described below in the form of a tree.

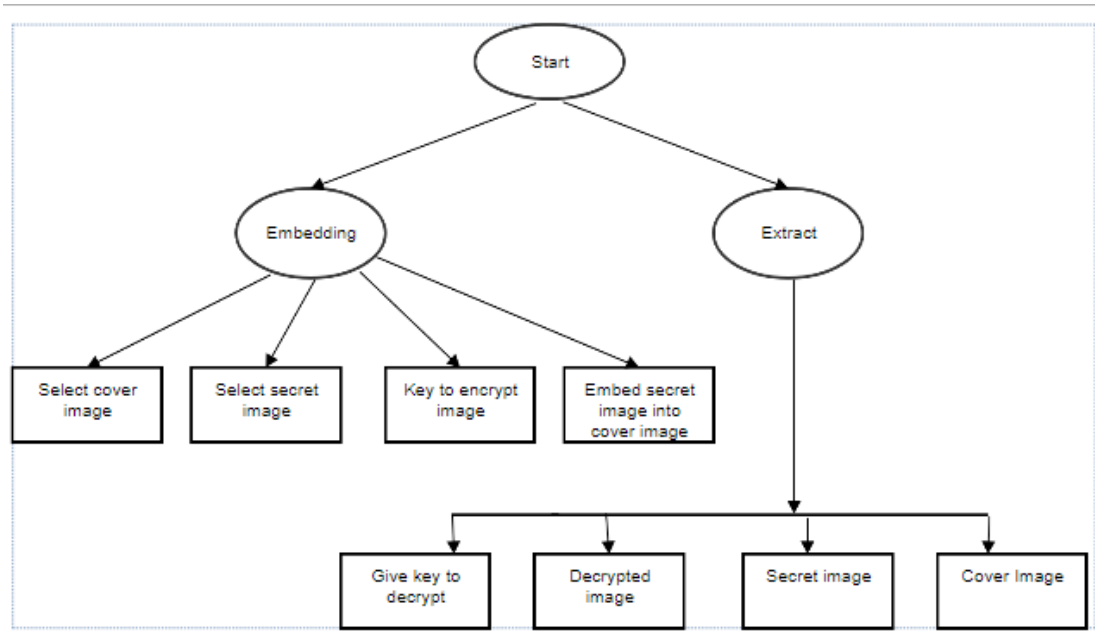

Figure 5: System Architecture

3.2 IMPLEMENTATION

As far as the implementation section is concerned, it mainly deals with the Pre-Processing, Resize, Filtering of Images given as input, Image Encryption, Embedding, Decryption.

Input Images: Input Images takes two images as input, one is cover image and the other is secret image. The Input images are read into the workspace using "imread" command. The images are displayed using "imshow" command.

Image Preprocessing: It consists of image resizing and image filtering.

Image Resize: The input images are resized to a fixed size i.e. 256*256 to make all the images to fixed size which are different in sizes.

Image Filtering: Image Filtering is done to remove the unwanted disturbances and noises in the input images.

Encryption: Encryption is a process in which the secret data is transformed into an unreadable format. The encryption of data is done with the help of the cryptography algorithm named RC4 which is also called as public key cryptography. Here a key is given to encrypt the data which provides security to the data that is intended to send.

Image Embedding: After the encryption of the secret data is done, the encrypted data is embedded into a cover image, which is done using the most traditional way of image steganography i.e. LSB algorithm.

Decryption: Decryption is the process in which the encrypted data is changed in to its original form. By giving the key, the image is decrypted and the secret data is reconstructed and come to its original form.

Performance Measure: At last the performance is measured by taking the two factors into consideration. They are as follows:

- Mean squared Error

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

- Peak Signal to Noise Ratio

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$
$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

IV. RESULTS AND DISCUSSION

4.1 Input

The input consists of two images where image1 is cover image and image2 is secret image. Input images are read into the workspace using "imread" command. The images are displayed using "imshow" command. The below figure 7.1 shows the input which consists of two images where image1 is cover image and image2 is secret image.

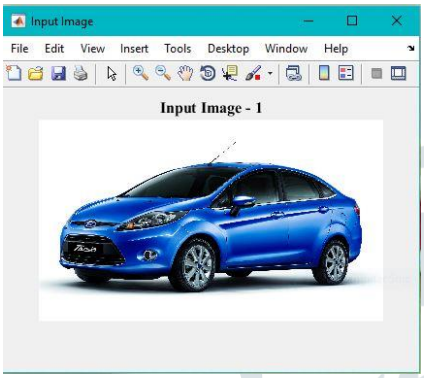

Figure 6a: Cover Image

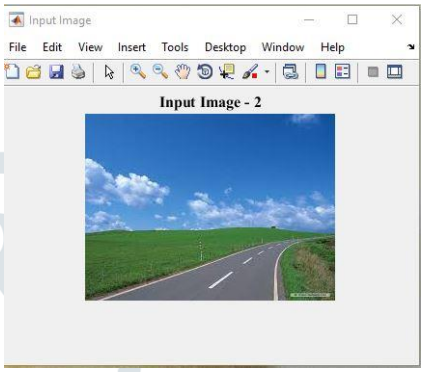

Figure 6b: Secret Image

4.2 Image Pre processing

The Image Pre Processing which consists of Image Resizing which is done to make the cover and secret images to a fixed size, 256*256 and applying Filter that is Guassian Filter which is done to remove the unwanted disturbances in the Images.

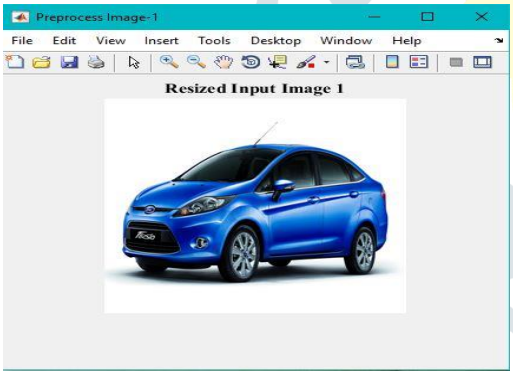

Figure 7a: Resized Image1

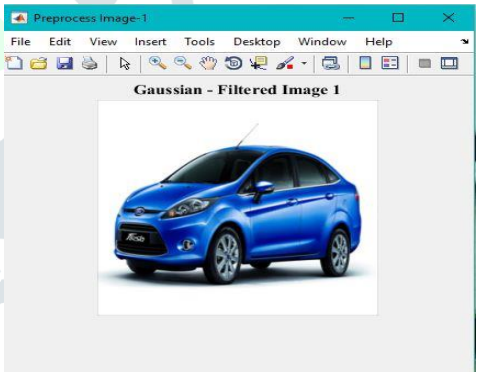

Figure7b: Filtered Image 1

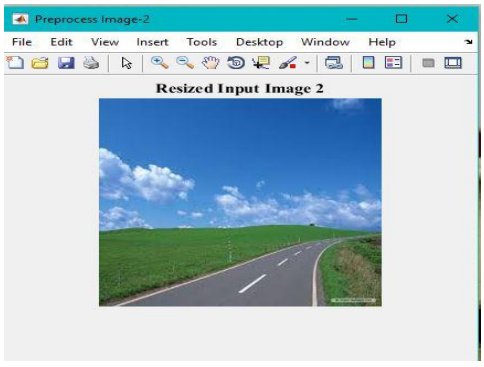

Figure7c: Resized Image 2

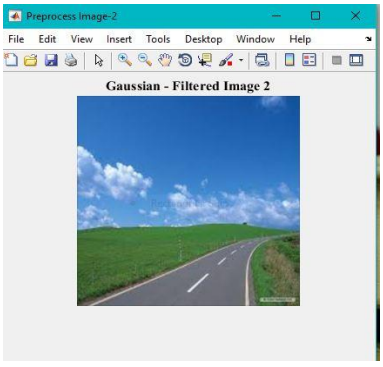

Figure7d: Filtered Image 2

4.3 Encryption

For encrypting the secret image RC4 Algorithm which is also called as Symmetric Key Algorithm in which the same Key is used to encrypt and decrypt. The key is used to encrypt the secret image.

Figure 8a: Giving Key

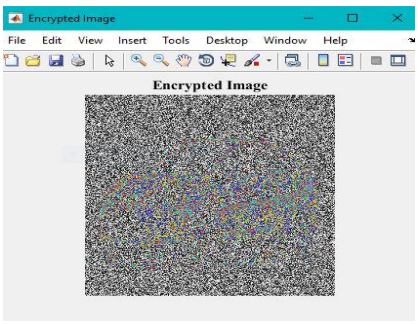

Figure 8b: Encrypted Image

4.4 Image Embedding

In Image Embedding the encrypted image is embedded into the cover image. For Image Embedding LSB Algorithm in which the replacing of LSB of cover image with each bit of secret image is done. The figure9 shows the Embedded Image.

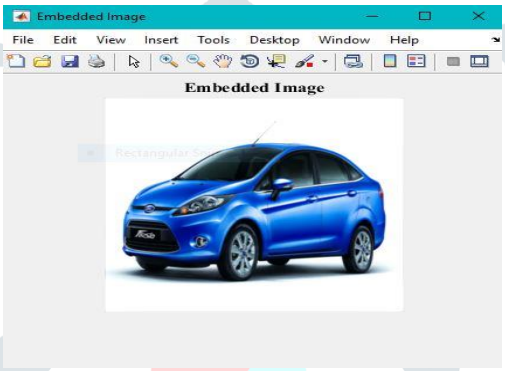

Figure 9: Embedded Image

4.5 Decryption

Decryption phase includes giving key back to reconstruct the encrypted Image.

Figure 10a: Giving Key to decrypt

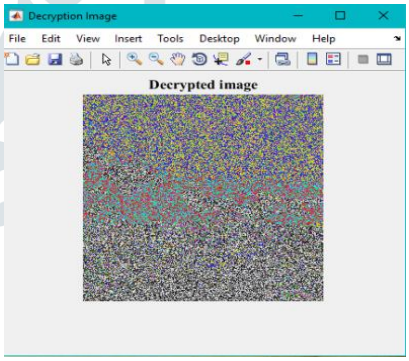

Figure 10b: Decrypted Image

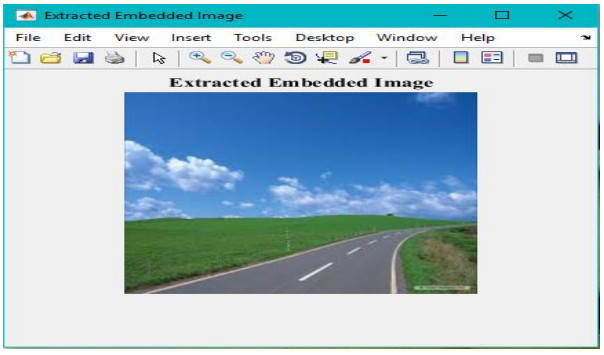

Figure 10c: Extracted Embedded Image

4.6 Performance Measure

In performance Measure, Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error.

Mean Squared Error

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

Peak Signal to Noise Ratio

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

The below table shows the Results of MSE, PSNR and Time

Sample Input	MSE(dB)	PSNR(dB)	TIME(SEC)
1	119220000	32.6327	17.6849
2	159000000	33.8705	18.911
3	140340000	33.341	20.8268
4	158540000	33.8705	18.911
5	138270000	33.2765	17.6331

Table1: Results of MSE, PSNR and Time

For the sample inputs considered in table1, the Figures 11 and 12 represents the graphical views.

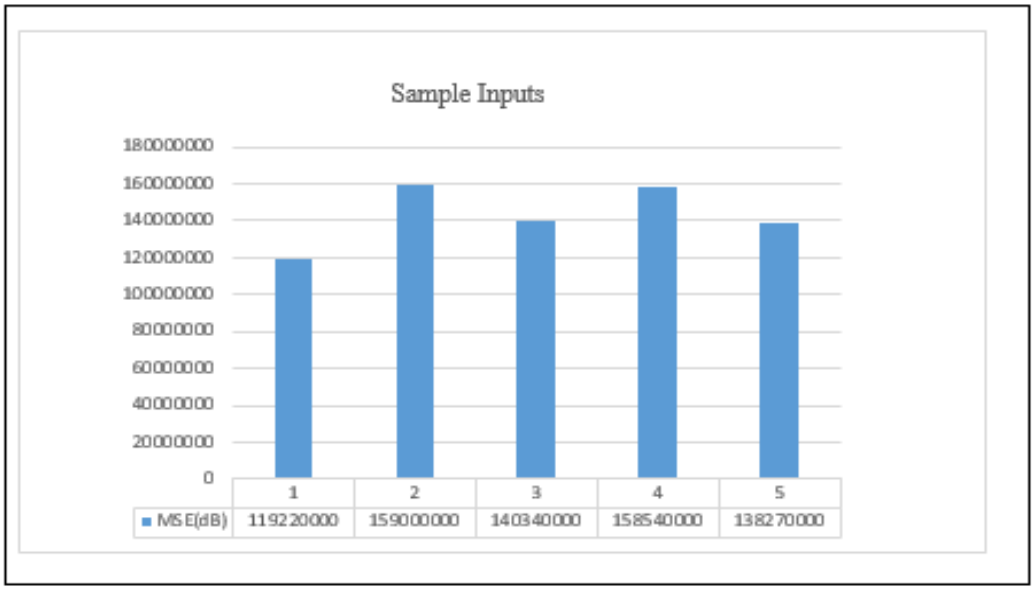

Figure 11: Graphical View of MSE

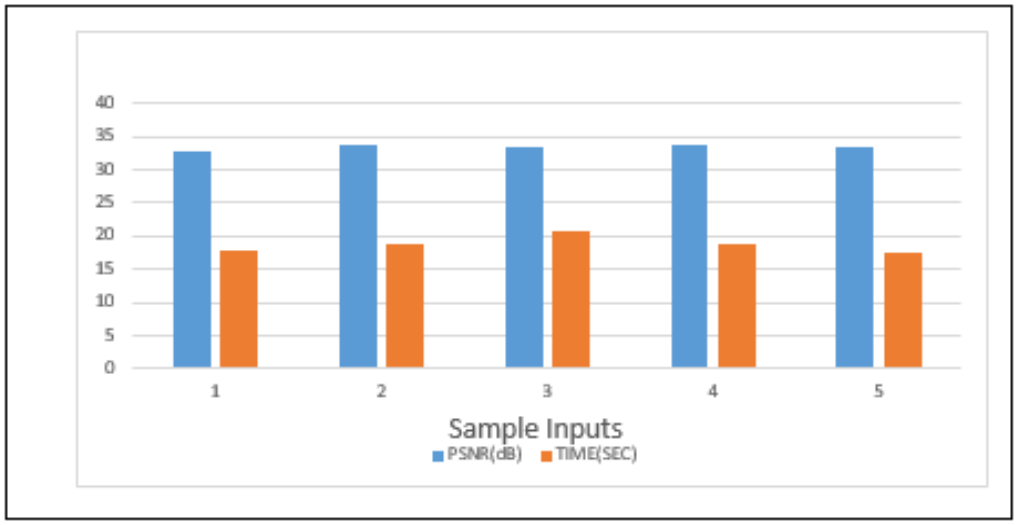

Figure 12: Graphical View of PSNR, TIME

V. CONCLUSIONS AND FUTURE SCOPE

5.1 Conclusions

To implement the proposed system, Literature survey is well done. The System Implementation is done successfully and the first objective of the proposed system is achieved by encrypting the secret image using RC4 Algorithm, in which a key is generated that is used to encrypt and decrypt the image and then the encrypted image is embedded in to the cover image using LSB Algorithm. By comparing the existing and proposed systems the second objective is achieved. More over the proposed system is more secured than the existing one by making use of embedded RC4 and LSB techniques.

5.2 Future Scope

Image encryption is an important and effective technique to protect image security. Future work, a novel approach to steganography through embedded cryptographic algorithm, in which a text file will be encrypted as image file is done.

REFERENCES

[1] *Tawfiq S. Barhoom, Sheren Mohammed Abo Mousa* proposed a research article "A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm" International Journal of Research in Engineering and Science (IJRES).

[2] *Ms. Hemlata Sharma, Ms.MithleshArya, Mr. Dinesh Goyal* proposed a research article "Secure Image Hiding Algorithm using Cryptography and Steganography"IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 01-06 www.iosrjournals.org.

[3]*Tawiq S. Barhoom, Sheren Mohammed Abu Mousa* "Secure Image Hiding Algorithm using Cryptography and Steganography" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 006

[4]*Pooja Rani, Mrs Preeti Sharma* "Cryptography Using Image Steganography" International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 5, Issue. 7, July 2016

[5] *Hayfaa Abdulzahra, Robissah Ahmad, Norliza Mohd Noor* "Combining Cryptography and Steganography for Data Hiding in Images" International Conference in Computer Science and Network Technology (ICCSNT). IEEE, 2(11): 1017-1020.

[6]*Varsha, Dr .Rajender Singh Chhillar* "Data Hiding Using Steganography and Cryptography" IJCSMC, Vol. 4, Issue. 4, April 2015, pg.802 – 805

[7] *Allam Mousa, Ahmad Hamad* "Evaluation of the RC4 Algorithm for Data Encryption" International Journal of Computer Science and Application-vol 3 JUNE 2006.

[8] *Naitik P Kamdar, Dipesh G. Kamdar, Dharmesh N.khandhar* proposed a research article "*Performance Evaluation of LSB based Steganography for optimization of PSNR and MSE*" Journal of Information, Knowledge and Research in Electronics and Communication Engineering ISSN: 0975 – 6779| NOV 12 TO OCT 13 | VOLUME – 02, ISSUE – 02

[9]*Mohammed Abdul Majeed, Rossilawati Sulaiman* "An Improved LSB image Steganography technique using Bit-inverse in 24 Bit colour image" Journal of Theoretical and Applied Information Technology 20th October 2015. Vol.80. No.2

[10]*Tiyasa Gupta, Assouma Alassane Mouhamadou Hafifou, Ramachandra Tawker, Vaidhehi V* "An Enhanced approach to Steganography: Obscurity" International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 9, Volume 2 (September 2015).

[11] *Nadeem Akhtar, Pragati Johri, Shahbaaz Khan* "Enhancing the Security and Quality of LSB based Image Steganography" 5th International Conference on Computational Intelligence and Communication Network-2013.

[12] *Govinda Borse, Vijay Anand, Kailash Patel* "Steganography: Exploring an ancient art of Hiding Information from Past to the Future" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 4, October 2013

Acknowledgements:

The author(s) feels it as a great privilege to thank Dr B.Sujatha, Professor and Head, Computer Science and Engineering, Dr.T.V.Prasad, Principal, Godavari Institute of Engineering and Technology (A) for their constant encouragement and members of the management, GIET Group of Institutions.