ISSN No:-2456-2165

Data Hiding using JPEG Steganography

Nidhi Singh[1], Shaik Karishma[2], S.Shiva Kumar[3], R Odaiah[4]
Guide[4], Associate Professor[4], ECE Department,
Geethanjali College of Engineering and Technology, Hyderabad, India

Abstract:- Steganography and Steganalysis are two side of the same coin. This paper discuss about how a message or data can be hidden inside an image using JPEG Steganography. Along with this, RC5 encryption and Chaos cryptography are also used so that, an outsider is not able to access the data within the image. This paper also discuss about how a data is stored or hidden inside an image and how we can recover data from the same image. This type of systems are made to make our applications and data more secure from the threats. This paper focus on using lifting wavelet transform (LWT) instead of using old methods like DCT.

Keywords:- *Steganography, RC5Encryption, Chaos Cryptography, Lifting Wavelet Transform.*

I. INTRODUCTION

Security plays an important role in the world of information technology. It is necessary to secure our data from being access, stolen and manipulated. During communication there is a high risk that data can be accessed by the third party. We are able to hear many news about data hacking. The hackers are able to access the data and files because the security levels are low when they were implemented on the systems. To ensure high security we must use several techniques and methods to overcome these problems. It should be always keep in mind whenever we are implementing a system where we have to store a confidential data or files, we should implement high-quality level of encryption and decryption process which in turn make our system highly secure.

This paper mainly briefs about how a message or data can be conceal in an image with high amount of security level. The data or text are encoded and then they are stored into an image. The image in which data is embedded is known as Stego image. Whenever a person sees a stego image, it will look like a normal image, but the person cannot able to see the data hidden in that image. This is the quality of Steganography where a third party is not able to see the data and the image is also transferred securely from sender to receiver. To embed message into an image and to extract same message from that mage is not a huge process, but to prepare this system we should know how Chaos cryptography, RC5 encryption and Lifting Wavelet Transform are done. The security level of the system depends upon the algorithm we are preparing, so that third party is not able to extract our data.

II. DESCRIPTION

A. Steganography

Steganography means hiding or covering a text, image or file into another image, file or video. It's an art of hiding data where a sender and receiver knows a secret message is hidden into a file, where a third person cannot suspect that data is hidden into a image. Once a data is embedded into the image Its not an easy task to extract message from it.

Steganography has become more popular because, both data and communication between two parties are secured. This is the main advantage of steganography over cryptography.

B. Steganalysis

Steganalysis is a process of detecting data which is hidden into an image, video or another file. The main use of steganalysis is to identify any data which is hidden, if it is found that any data is covered or concealed by another file or image, the process will also help to recover the hidden data.

C. RC5 Encryption

Secret messages or data or not embedded directly into an image. With the help of RC5 encryption the original message is encoded. This encoded text is known as Cipher text. The obtained cipher text is then store into an image. RC5 is a symmetric key block cipher, which works fast when implemented. We use RC5 encryption because it has more number of iterations and strong key. Due to RC5 encryption data security level becomes more flexible.

D. Chaos Cryptography

Chaos cryptography is a study where a data is transferred from sender to receiver with high security in the presence of third party. Chaos cryptography algorithms are created in such a way that the result obtained from that algorithm produce confusion. This helps the quality of the security level of the system.

E. Lifting Wavelet Transform(LWT)

Lifting wavelet transform is commonly used because it design wavelets and perform discrete wavelet transform. By using this transform, it is very useful because two different works designing wavelet and DWT are done simultaneously. It is also easy to understand and can be used for irregular sampling.

III. LITERATURE REVIEW

The previous methods or techniques of Steganography of image were based on DCT{direct cosine transform).DCT have its drawbacks. In the present method we have used Lifting Wavelet Transform, RC5 encryption and Chaos cryptography.

IV. WORKING

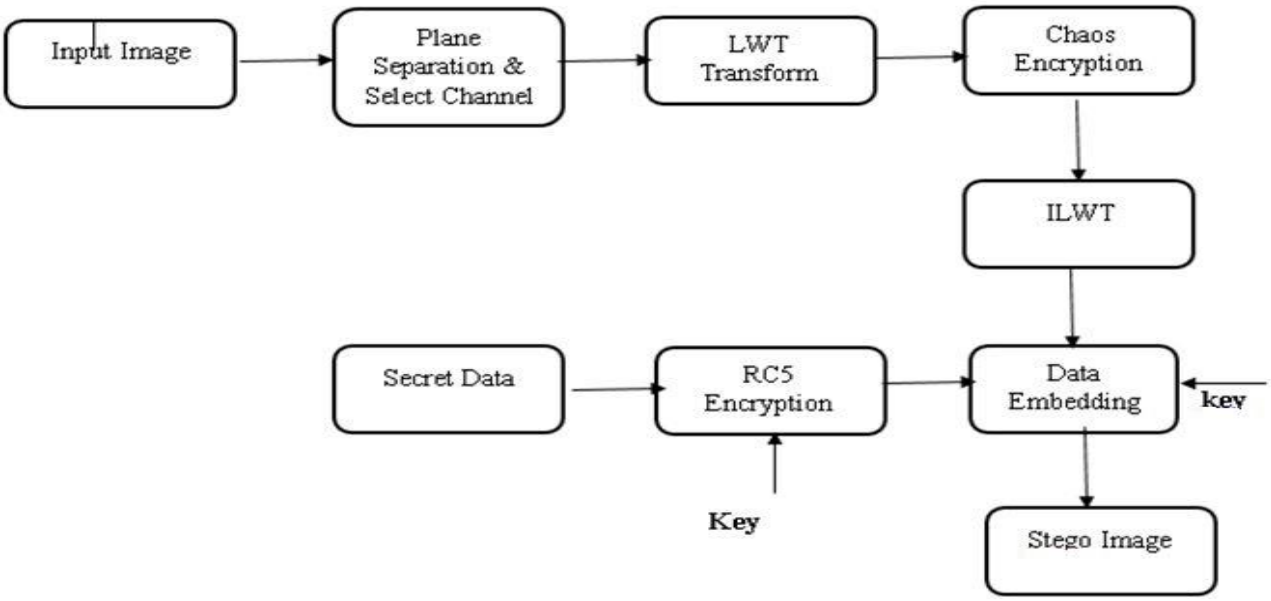

Fig 1:- Embedding Process of Steganography

The fig 1 shows how a secret data is embedded into an image. The first step is to take an image as an input which can be either in JPEG or PNG or bmp format. Then the input image is separated from its blue plane. This is done because data can be easily hidden at blue plane. With the help of LWT, samples of image are formed .In these samples we hide our secret data. Before hiding the data should be converted into cipher text with the help of RC5 encryption. Chaos Encryption is done just to secure data from outside threats. After hiding the data inverse lifting wavelet transform is applied, so that image gain its original color. The image in which data is hidden is known as Stego image.

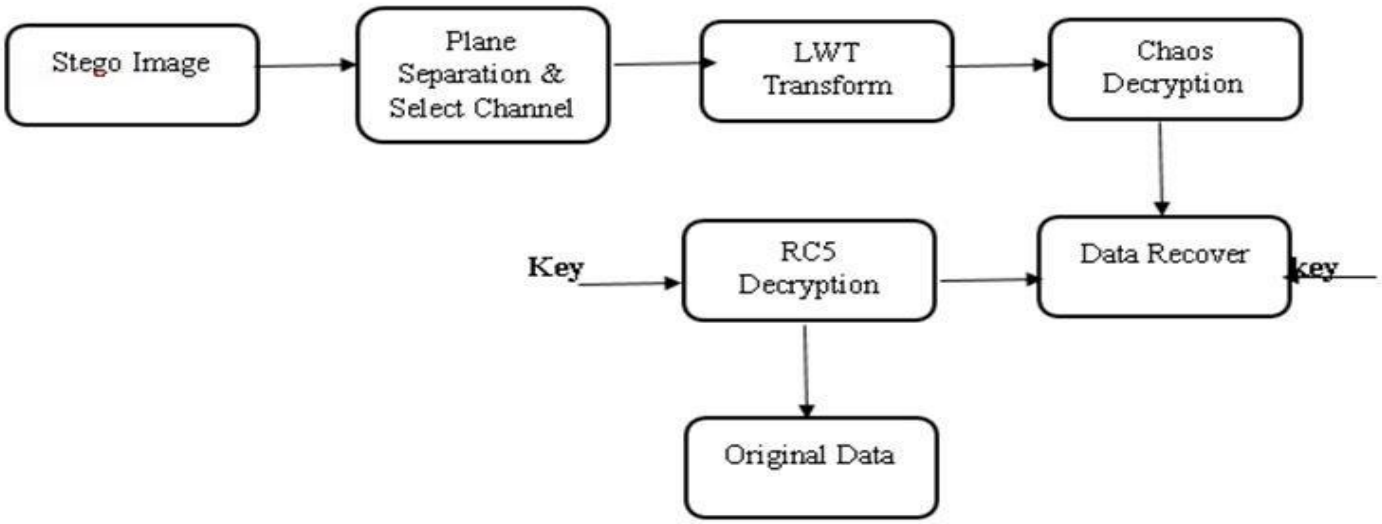

Fig 2:- Extraction Process of Steganography

The fig 2 shows how a hidden data is recovered from the stego image. First we should take the stego image as an input. Again the stego image is separated from its blue plane. Here also we will apply LWT to get the samples of the image. After getting the samples of image, extraction of data can be done easily. But the data which we extract is in encoded form. With the help of RC5 decryption, the data in encoded form is decoded and we are able to recover the original data.

V. RESULTS

The process of embedding data into an image and to extract the same data from it, works on matlab. A required code should be written and dumped into the matlab which will successfully run the project.

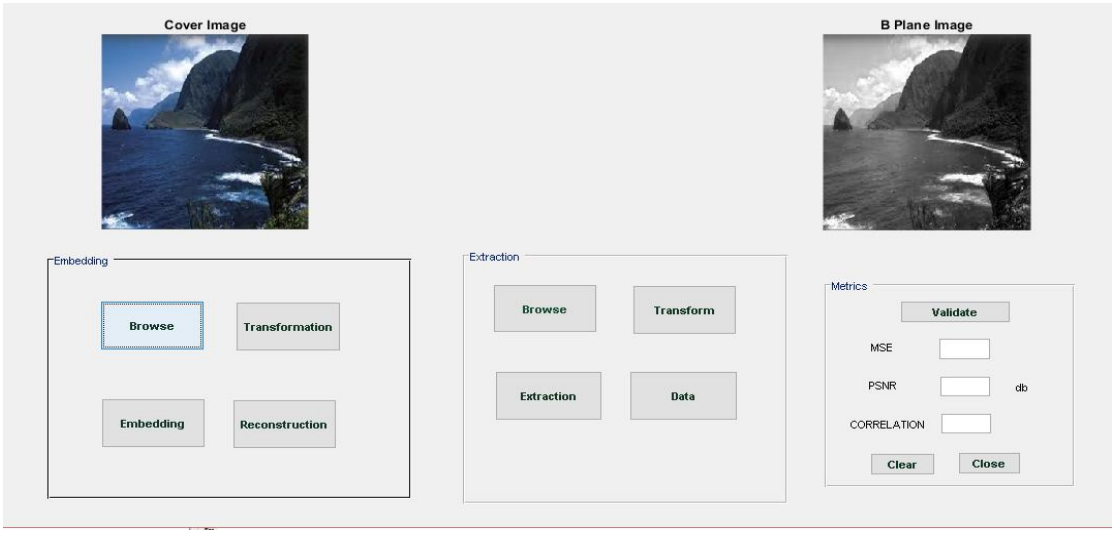

Fig 3:- Conversion of Input Image into Blue Plane

Fig 4:- wavelet Decomposition of Blue Plane Image

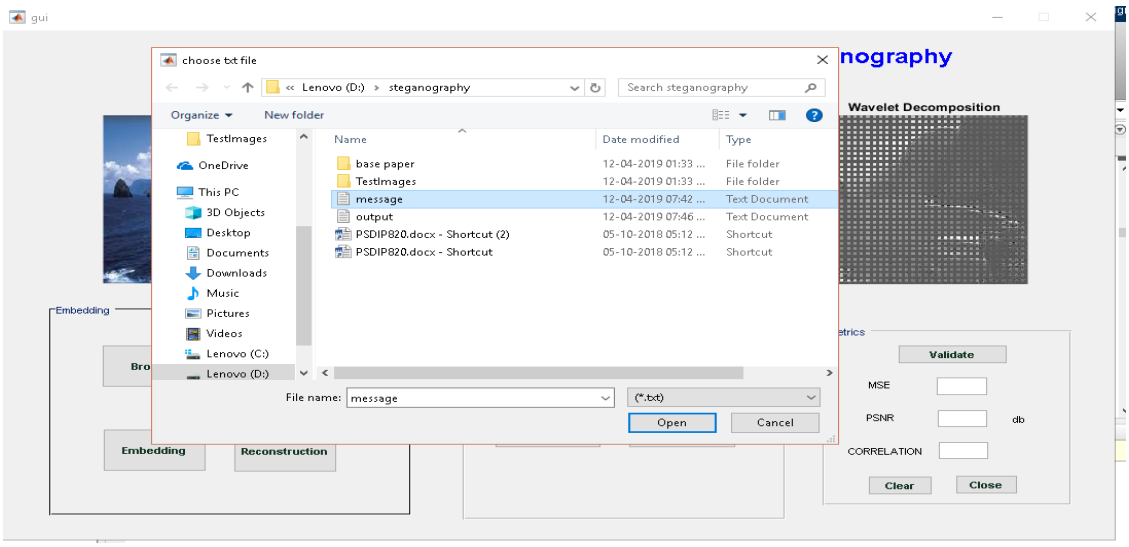

Fig 5:- Message is Browsed to keep inside the Image

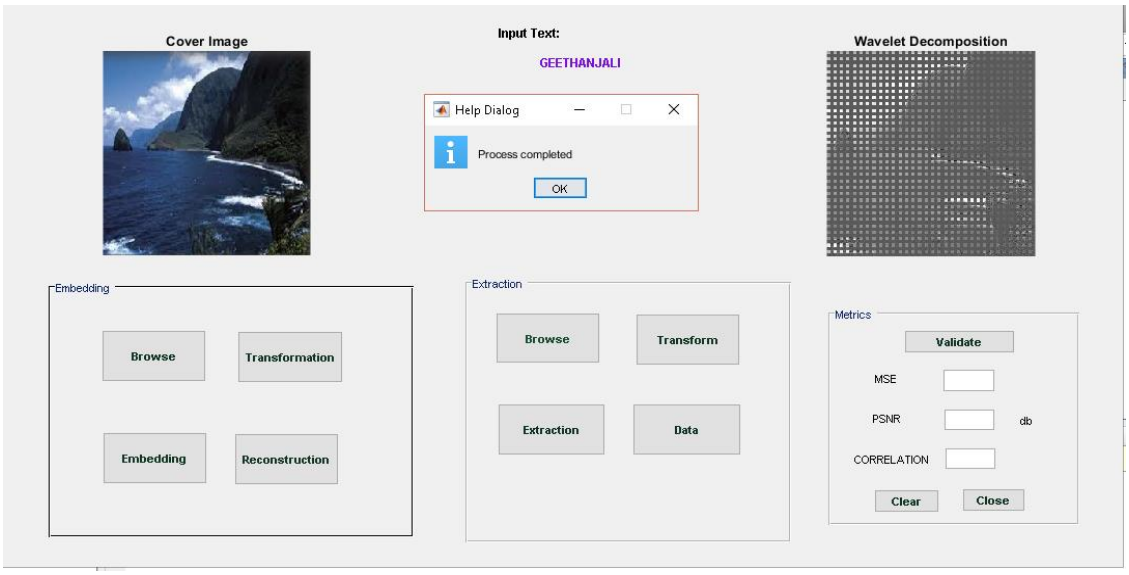

Fig 6:- After taking input Message it is Converted into Cipher Text

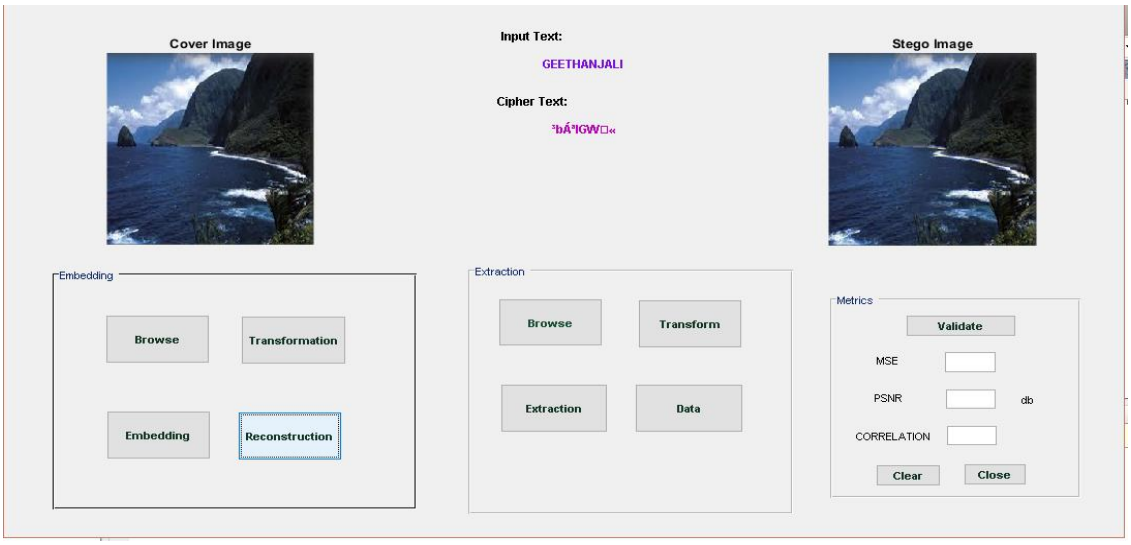

Fig 7:- Message in Cipher text is Stored into the Image

Fig 8:- Recovery of Original Data from the Cipher Text is done by taking the same Stego Image

VI. CONCLUSION

The main target behind this concept is the security of data, so that another people are not able to access, modify or delete our confidential data.This application is mainly useful in Military Service Medical information protection and Research Institutes where confidential data are protected with high security.

REFERENCES

[1]. Image Steganography Based on Mantissa Replacement using LWT N Sathisha1, K Suresh Babu2, K B Raja2, K R Venugopal3 1Department of ECE, Govt. S K S J Technological Institute, Bangalore, India. 2Department of ECE, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. 3Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India.

[2]. T. Denemark and J. Fridrich, "Improving selection-channel-aware steganalysis features," in *Proceedings IS&T International Symposium on Electronic Imaging 2016* (A. Alattar and N. D. Memon, eds.), (San Francisco, CA), February 14–18 2016.

[3]. Statistical Steganalysis for Content-Adaptive Steganography V.Gokula Krishanan1, M.Deepak2, S.Praveen Kumar3, B.Vinoth Kumar4 Assistant Professor1, UG Scholar2, 3, 4 Department of CSE Panimalar Institute of Technology, Chennai, India