International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

A NOVEL TECHNIQUE OF IMAGE STEGANOGRAPHY

Amuktha Godavarthy

Department of Electronics and Communication Engineering, SRM Institute of Science and Technology Kattankulathur, Chennai

---

ABSTRACT:- Data Hiding technique is an important technique in todays era. Because of the hackers in the whole world it is very difficult to send any confidential message to the other person. With the help of the image steganography we can hide our secret data in any image with the help of a particular key then only it will be opened. The objective of the project is to hide our secret data in any image, text or audio files so that hackers will not be able to guess it. In this paper we used different techniques to hide our secret data and extract over data when it has been sent to the other person with the help of particular key, we can open it.

Keywords—Steganography, Stego image, DCT, DWT, GUI data.

I. INTRODUCTION

In today's world security plays an important role in the technology. It is ruling the entire internet which plays an important role in the whole world. The main problems in security is Confidentiality, Data Integrity, Authentication and many more. The messages are encrypted secretly to different customers. The Decrypted messages is use to rebuilt the secret data. In this Image Steganography which is nothing but hiding the secret data in any text or any images. If we want to hide any secret data confidentially, we can hide behind any image so that third party will not be able to notice that secret data is hidden behind one image. This will be only useful if we add key to our secret data otherwise anyone can open our secret data. Secret key will be generated with the help of reversible polynomial function using numerical key. In this paper different algorithms techniques have been used to hide the secret data.

We are going to use key to hide our data with different algorithms technique so that third party will not be able to open it. The secret image and the cover image will be embedded together to build a Stego image. This reversible image sharing process is used to recreate the secret image and cover image.

The objective of the project is to hide the secret data into any image, text, audio or video so that third party will not be able to see it.

Organization of the project

The first chapter deals with the general introduction of Image Steganography and also and also the literature survey where various works for the project was already done and published. The second chapter speaks about the block diagram of the transmitter and the receiver of the image steganography to hide our data. The third chapter deals with the stimulated results of the image steganography. The fourth chapter deals with the conclusion and the future work of the project.

II. BLOCK DIAGRAM

Block diagram of Transmitter:

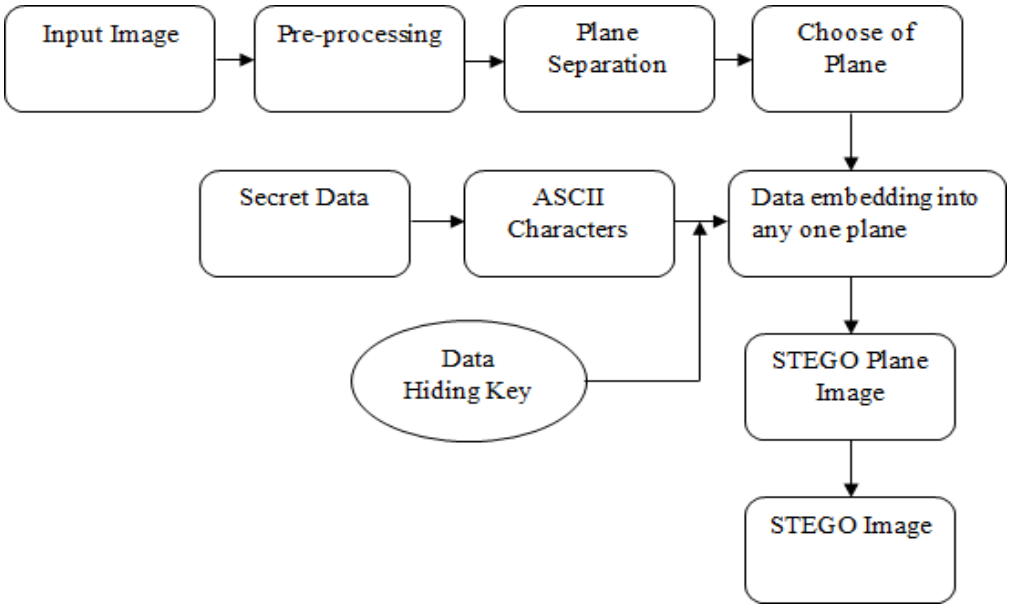

Fig.1: Block diagram of Transmitter

This is the Block diagram in transmitter in fig 1 side in this first of all we will take the image where we have to hide our secret data. That image we will do reshape and resize of the image then in plane separation three different planes are there R,G,B planes in that we will hide our data in one plane. Now we are going to select one plane in which we are going to hide our data. After selecting we will apply DWT and DCT techniques. This DCT and DWT are the different transform techniques. In DWT we will separate the image to original image by {LL,LH,HL,HH}. Then we will hide our secret data in that image. The secret data will be converted into Binary value. In the embedding process we will encrypt our secret data will the help of different transformation techniques. For embedding we will use the data hiding key so that third party will not be able to see it. This key should be of four passcode value. After embedding we can stego image which the original image and the data separately.

Extraction Process: -

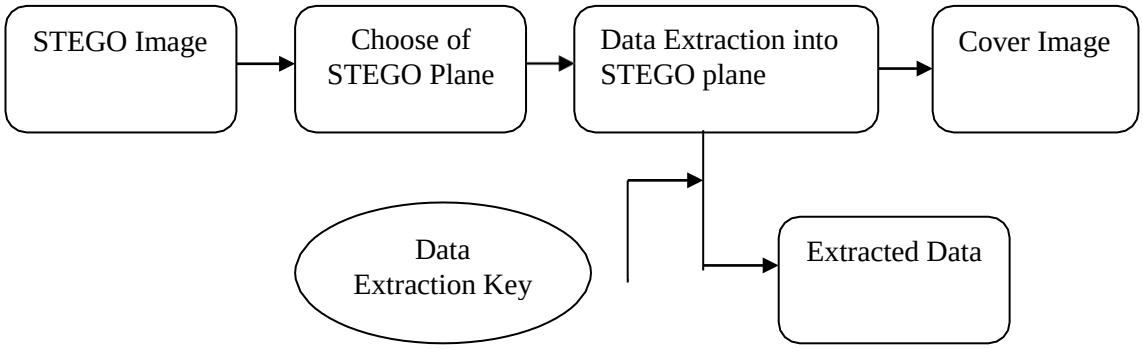

Fig no.2: Block Diagram of Extraction Process

In fig.2 this Extraction Process the stego image will be taken in which the image will be encrypted in that stego image the secret data is stored and we have to extract the secret data and stego image separately for this we are using Extraction Process. In this Extraction Process the image will be encrypted with the help of key using that key we can encrypt the

image. To extract the secret data, we have to apply again one key which is having four passcodes in it. Using that key, we can extract the secret data in it.

For Encoding the Hidden Data:

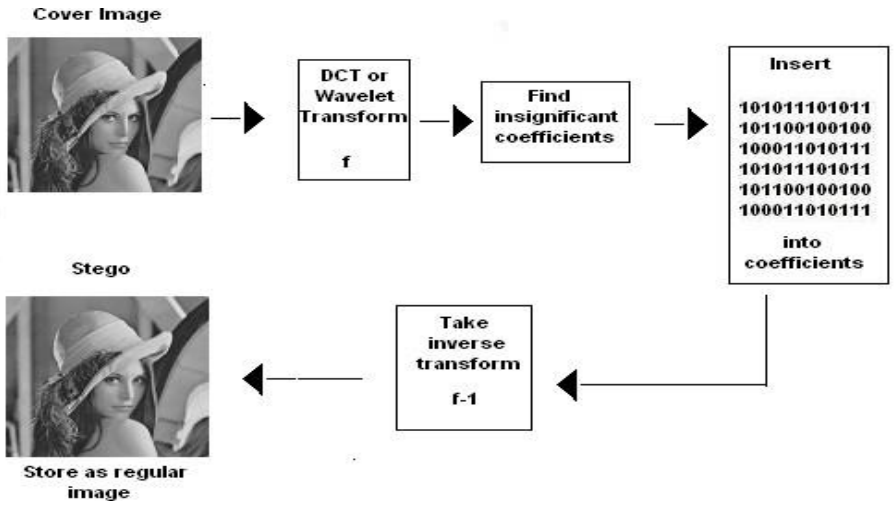

Fig no.3: To Encode Hidden Data

Take the DCT or wavelet transform of the cover image then we will find the coefficients below a certain threshold after that we have to replace these bits with bits to be hidden (can use LSB insertion) with this we will take the inverse transform because of that the it will store as regular image.

For Decoding the Hidden Data:

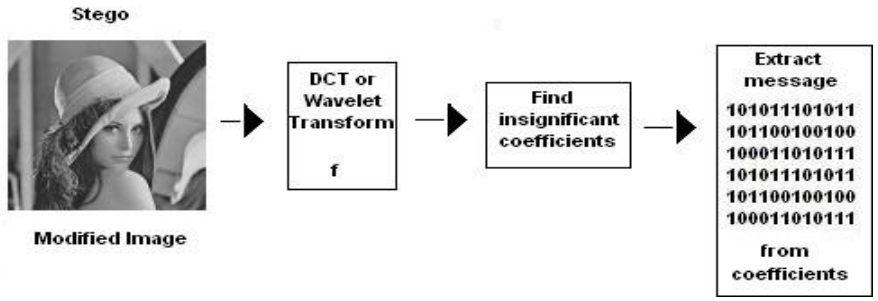

Fig no.4: To Decode Hidden Data

Take the transform of the modified image then we have to find the coefficients below a certain threshold then we will extract bits of data from these coefficients after that we will combine the bits into an actual message.

III. STIMULATED RESULTS

DWT IMAGE

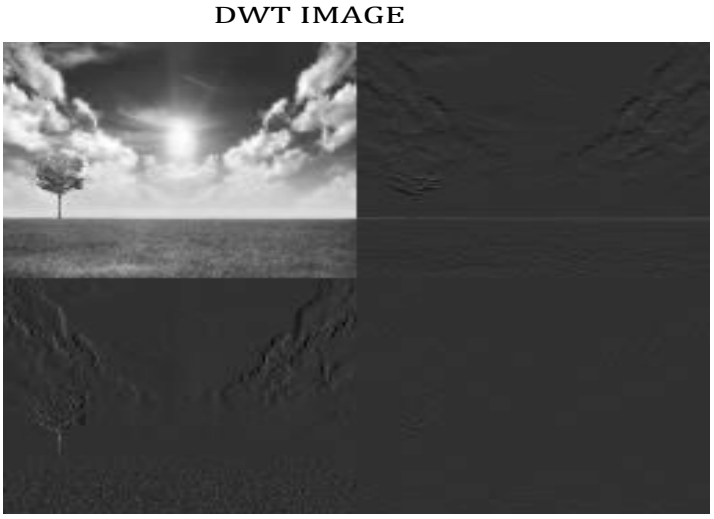

Fig no.5: Dwt Image

DWT is Discrete Wavelet Transform which means Splitting the exact information. Wavelet means nothing but the set of data.

DCT IMAGE

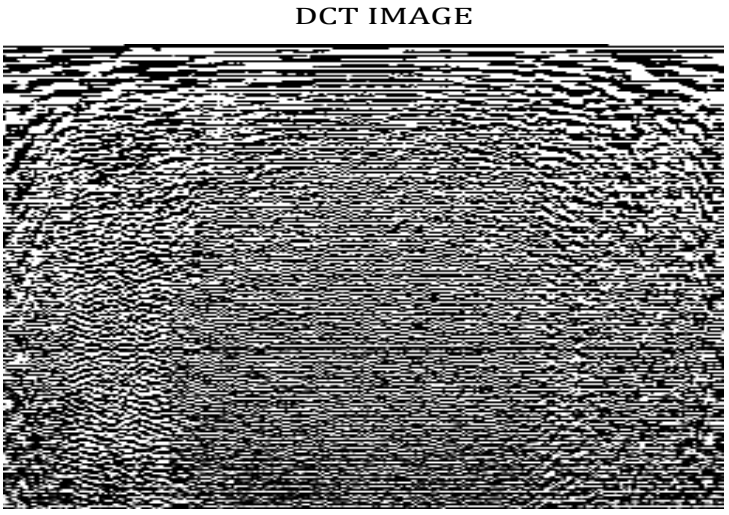

Fig no.6: Dct Image

DCT means Discrete Cosine Transform in which it depends upon the cosine it will split the data into low information and high information.

STEGO ENCRYPT IMAGE

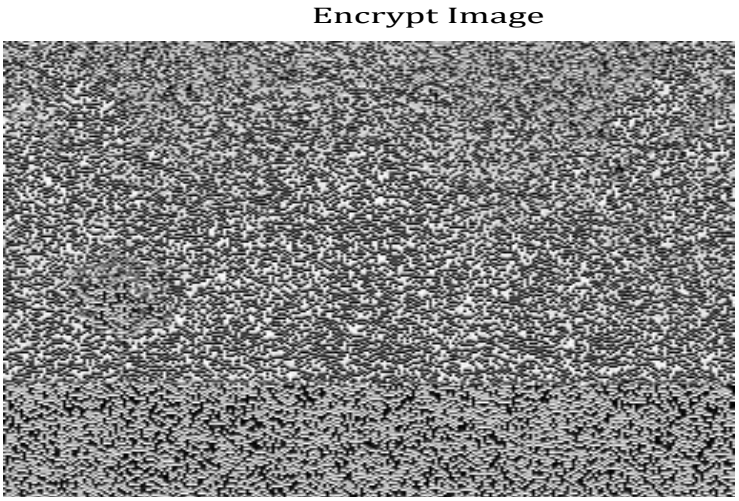

Fig no.7: Stego Encrypt Image

DECRYPT IMAGE

Fig no.8 : Decrypt Image

This is the original image after decrypting the image and the secret data.

GUI_4BIT

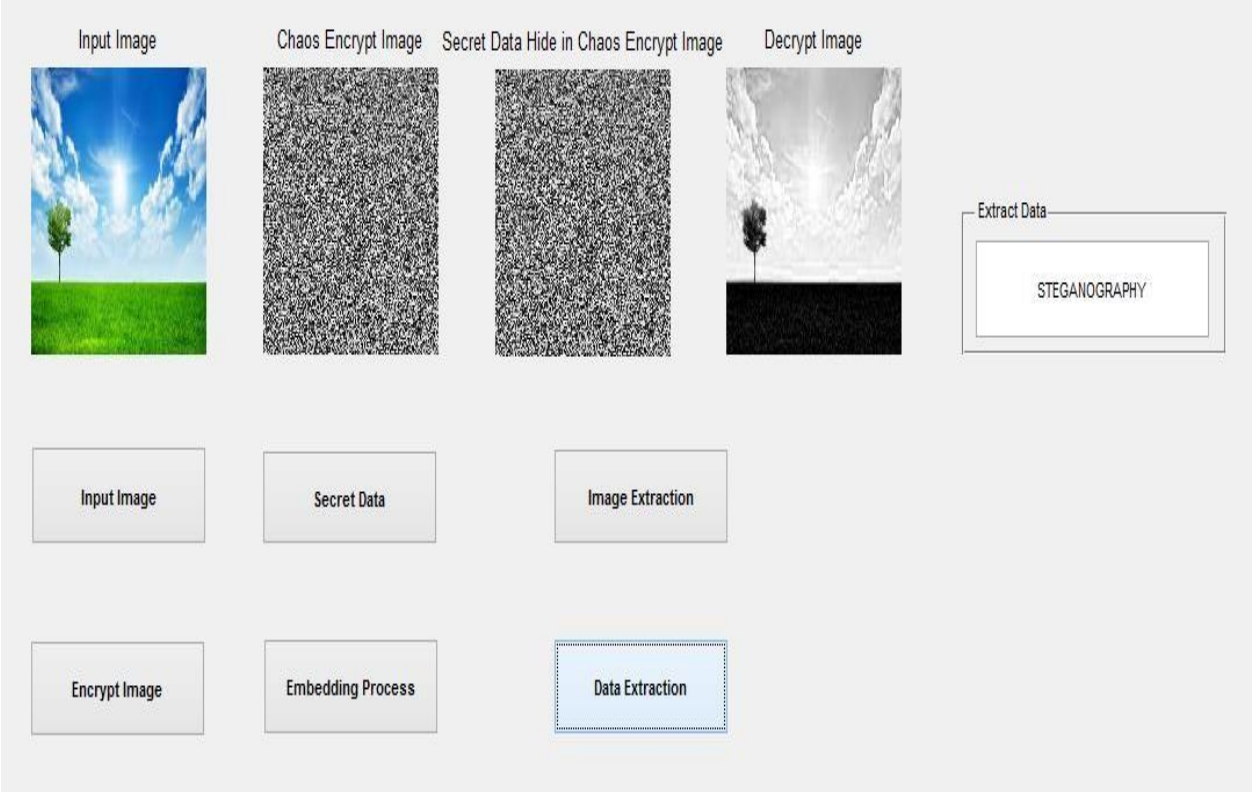

Fig no.9:GUI data

This is the Graphic User Interface bit in which the MATLAB will create a separate window to transmit and to receive the data and the images.

IV. CONCLUSION

The project stated that with the help of encryption of the compressed images and the data hiding information to protect the videos from data hacking. In this we used LSB, DWT, DCT technique in which we encrypted and decrypted the hidden data before and after embedding and extraction. Bit XOR operation method is used for data conversion to binary numbers**.** In order to accommodate to different scope, data extraction will be done either in the encrypted area or at the decrypted area to recover original data without any loss. With this we conclude that we can hide our secret data in any text, image or in video with the help of key so that third party will not be able to see our they can't be able to hack. We can use different algorithms also like Chaos Encryption technique.

REFERENCES

[1]. Mukta Goel and Rohit Goel ," Comparative Analysis of Wavelet Filters on Hybrid Transform Domain Image Steganography Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013.

[2]. Dr. Sudeep Thepade and Smita S. Chavan , "Appraise Of Multifarious Image Steganography Techniques ", /International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 2, March -April 2013, pp.1067-1174.

[3]. Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar," A Novel Technique for Image Steganography Based on DWT and Huffman Encoding" International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6).

[4]. Usha B.A1, Dr.N.K Srinath, Dr. Ravikumar C N, Puttaraju, Manu and Vijaykumar , "Hybrid Fusion Methods in Image Steganography for Secured Data Transmission", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015.

[5]. Veerdeep Kaur Maan and Harmanjot Singh Dhaliwal," 32×32 Vector Quantization Based Colour Image Steganography", International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319- 7463 Vol. 2 Issue 9, September-2013, pp: (28-33)