

Steganography Based on AES Algorithm and BPCS Technique for a Securing Image Data

Arjun Kumthe, Kajal Jadhav, Nikita Dhande, Prof. Arati Dandawate
Dhole Patil College of Engineering, SPPU, Pune,
Maharashtra India

Abstract—

A method of hiding secret messages in a cover object while communication takes place between sender and receiver is called Steganography. Security of confidential information has always been a major issue from the past times to the present time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone other than the receiver. Therefore from time to time researchers have developed many techniques to secure transfer of data and steganography is one of them. In this project we have proposed a new technique of image steganography i.e. BPCS tech. and Advanced Encryption standard algorithm for providing more security to data as well as our data hiding method. The proposed technique uses BPCS. This technique divides image in the bit planes we can also call it as 8bit plane. After that we use the AES algorithm work of the that algorithm is data encryption by using advanced technique. AES totally work on matrix transformation. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form. The providing the security to the data which is placed inside the image or hide the any kind of the data (audio, video, text, etc) in the image using by steganography technique. Protecting the image from the different attack which is done by third party.

Keywords— Steganography, AES, BPCS, Encryption, Decryption, Alpha Channeling

I. INTRODUCTION

Today world is fastest and world. For fastest growing world is totally depend upon the information. In that we can share information collect information and send and receive information from source to destination. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography method used to share information in a concealed manner. Steganography is one of the technique hiding secret message in image. But today all knows about Steganography, so any third party can attack on that and do mis use of the that information. For increasing the security of that data we are use some algorithm for encryption and decryption purpose. AES technique and Bit plane Complexity Segmentation technique use for increasing the security of the information. The secret message is convert to encrypt and decrypt form by using the technique advanced encryption standard. Hiding the secret message in the image using the bit plane complexity segmentation technique.

II. LITERATURE SURVEY

Today world is totally depends upon the information. So many organizations work on the how give the better security of the data. So we use the some paper and get a knowledge about that and understand the advantages and disadvantages of that paper and on that basis we work on that. Firstly we study about some project which is implemented in past. A New Approach for LSB Based Image Steganography using Secret key. (S.M. Masud Karim, Md. Saifur Rahman) this is paper which implemented in the past and it have some advantages which is Lower distortion and good image quality, High data hiding capacity, More efficient and reliable capacity and disadvantages is To achieve high degree of info network graphics format is used to save the images in little space when size of the image is increased. The another is Hash Based Least Significant Bit Technique for video Steganography (HLSB) (Kousik Dasgupta, J.K. Mandal, Paramartha Dutta) and advantage of this paper is Using video files in hiding info is the added security against the attack of hacker due to the relative complexity of the structure of video as compared to image files and disadvantages is Hased LSB tech a less amount of data are placed i.e. not feasible. Jing-Ming Guo, Thanh-Nam Le, Secret Communication Using JPEG Double Compression, Signal Processing Letters, IEEE, Vol. 17, Issue No. 10, Pages No. 879-882, Oct., 2010.

Weiqi Luo, Yuangen Wang, Jiwu Huang, Security Analysis on Spatial 1Steganography for JPEG Decompressed Images, Signal Processing Letters, IEEE, Vol. 18, Issue No. 1, Pages No. 39-42, Jan., 2011

Dr. Ekta Walia, Payal Jain, Navdeep, An Analysis of LSB DCT based Steganography, Global Journal of Computer Science and Technology, Vol. 10, Issue No. 1, April, 2010.

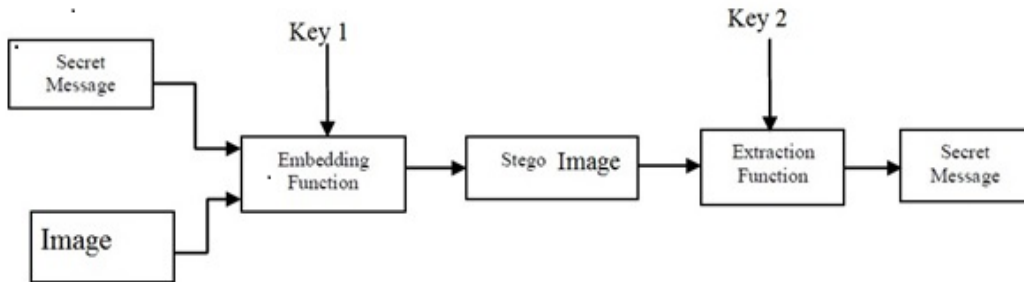
A New Approach for LSB Based Image Steganography using Secret Key. (S.M. Masud Karim, Md. Saifur Rahman) we also refer this paper and find out the same advantages and some drawbacks, and we working on the the drawbacks of this paper.

III. PROBLEM STATEMENT

The problem statement consists of embedding the secret message in the RGB pixels value of the cover image. Before embedding the secret message have to be converted to cipher text using AES technique to enhance the secrecy of the

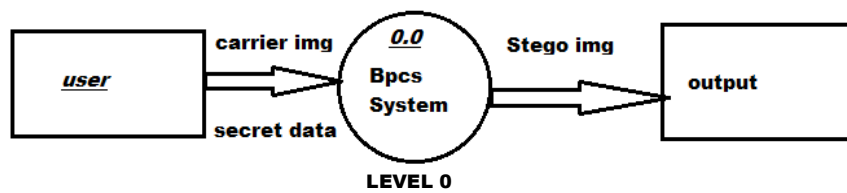
message. In this approach we implemented a technique called AES for the to encrypt and decrypt data and hiding the data in the image using the BPCS technique .The providing the security to the data which is placed inside the image or hide the any kind of the data (audio,video,text,etc) in the image using by steganography technique. Protecting the image from the different attack which is done by third party.

IV. BLOCK DIAGRAM

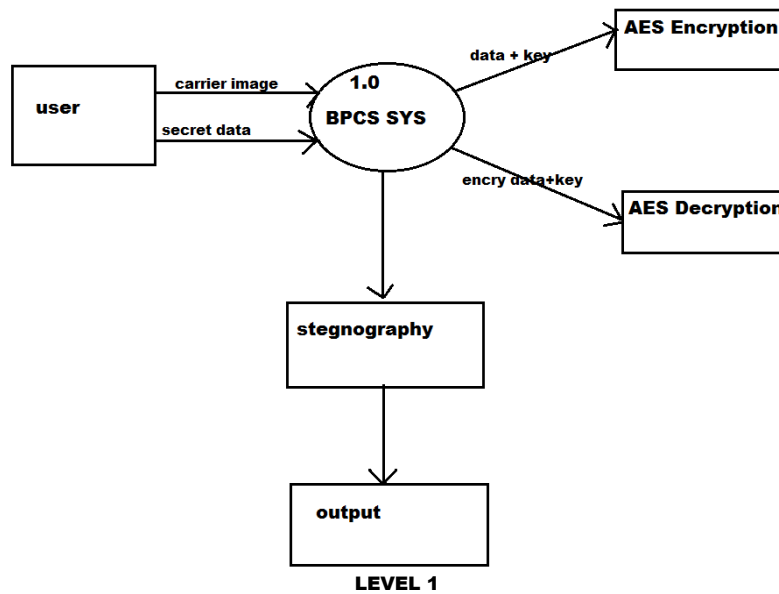


V. LEVELS BLOCK DIAGRAM

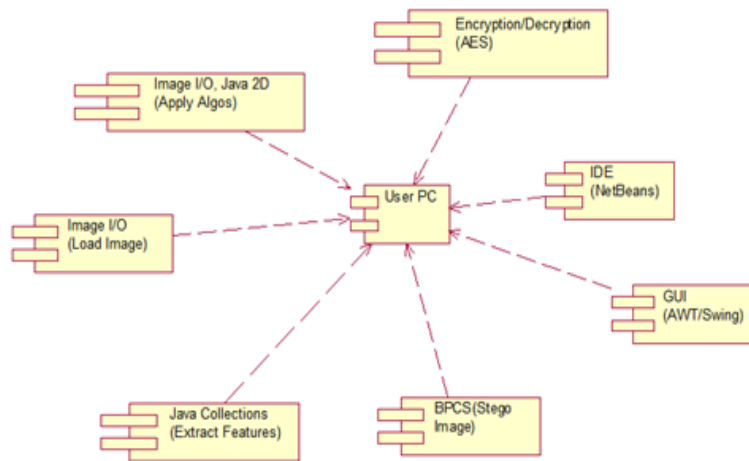
LEVEL 0:



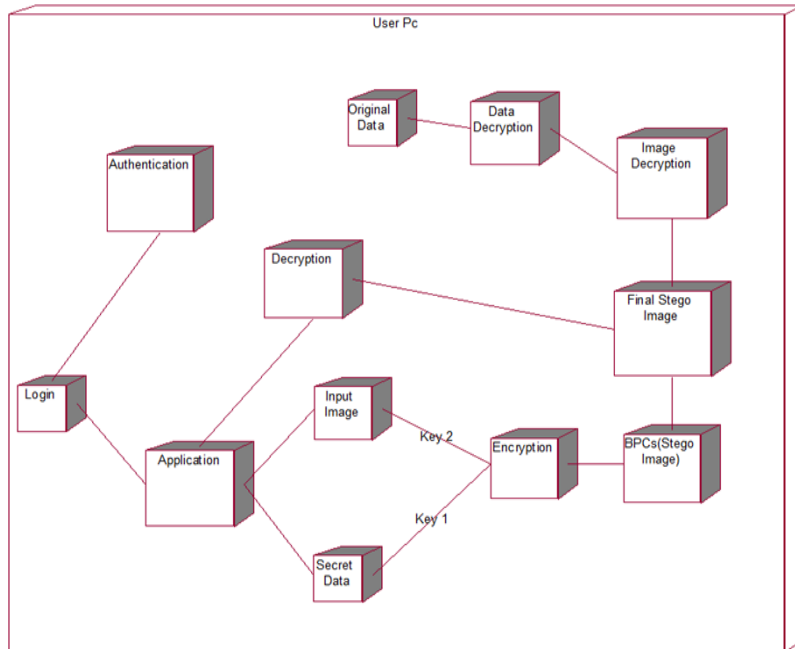
LEVEL 1:



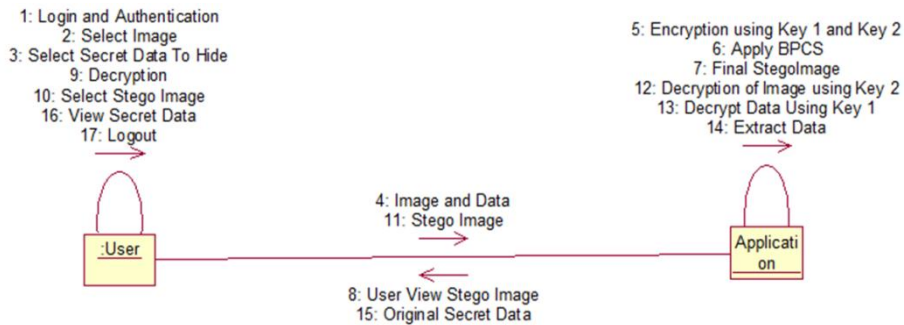
VI. UML DIAGRAMS



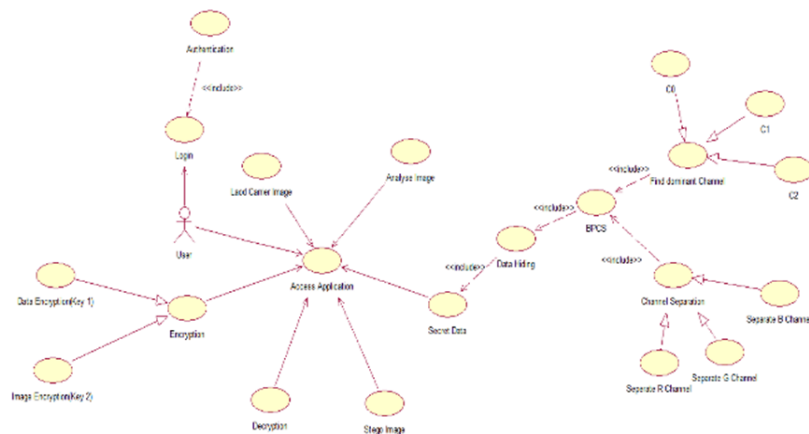
Component Diagram



Deployment Diagram



Collaboration Diagram



Use case diagram

VII. ALGORITHMS

Here We using the two main algorithm.

1. AES
2. BPCS

1. AES(Advanced Encryption Standard):

Step 1: Taking the only 128 bit data at a time as input.

Step 2: Key

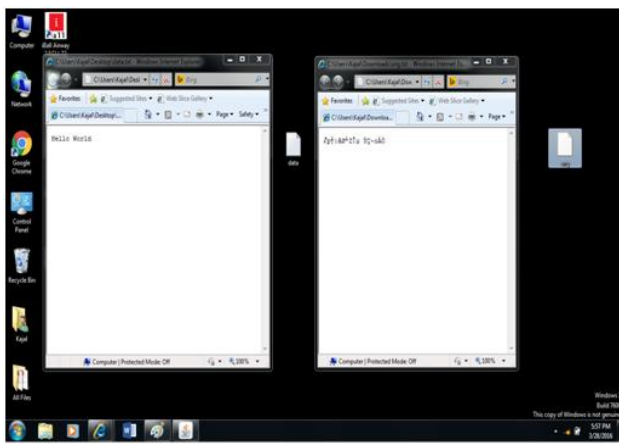
Round key are derived from the cipher key using. Advanced Encryption Standard wants a one 128-bit round key block for each round plus one more.

Step 3: Add Round Key : each byte of the state is combined with a block of the round key
 Step 4: Sub Bytes: the non-linear substitution step where each byte is replaced
 Shift Rows: The step where the last three rows of the state are shifted cyclically a certain number of steps.
 Mix-Columns: mixing operation which operates on the columns, combining the four bytescolumn.
 Add Round Key: this the last round.
 Step 5: Subbytes , ShiftRows, AddRoundKey.

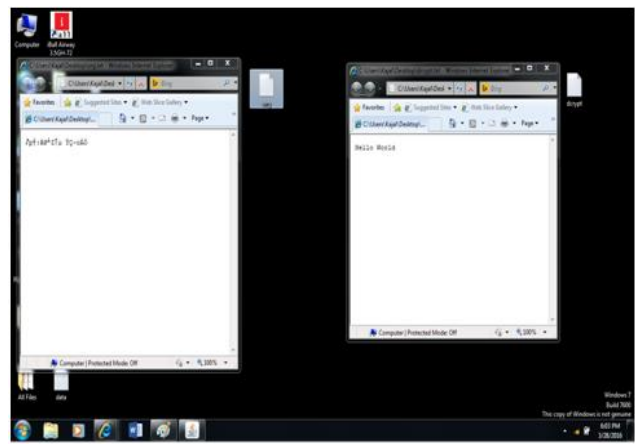
2. BPCS (Bit-plane complexity segmentation):

Step 1 : Taking input as image
 Step 2 : Taking up the 8*8 matrix or divides the image in 8*8 by matrix.
 Step 3 :Taking plane from 8*8 by matrix for hiding the data in any R,G,B plane.
 Step 4: Finding the complexity
 Step 5: if the complexity is less than 0.3 then X-OR with the standard matrix .
 Step 6 : Hide the data in the image and send to the reciver.

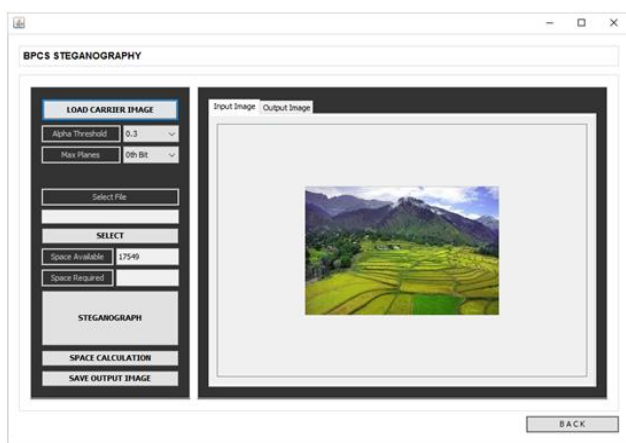
VIII. RESULT



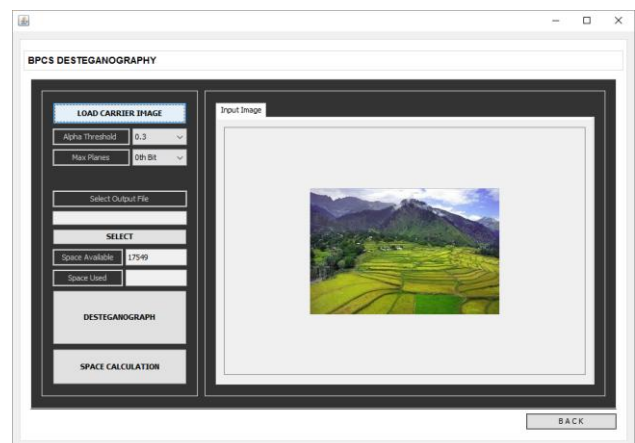
Data encryption



Data Decryption



Steganography



De-Steganography

IX. CONCLUSION AND FUTURE SCOPE

A secured BPCS technique for image steganography has been implemented. An efficient Steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through BPCS method. In this work the image is divided into 8 planes. we also implemented the AES algorithm for encrypting and decrypting data. The future scope of this project is that you can implement or create android application. We do lots of work in future on this project. You can also use the MD algorithm and do modification in this.

REFERENCES

- [1] A New Approach for LSB Based Image Steganography using Secret Key". (S. M. Masud Karim, Md. Saifur Rahman)
- [2] Hash Based Least Significant Bit Technique for Video Steganography (HLSB)" (Kousik Dasgupta, J. K. Mandal, Paramartha Dutta,)

- [3] A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique (Anil Kumar ,Rohini Sharma) L. A. Elrefaey, M. E. Allam, H. A. Kader, andM. Selim,
- [4] Robust blind imageadaptive watermarking, in Proceedings ofthe 25th National Radio Science Conference (NRSC 08), March 2008
- [4] WeiqiLuo, Yuangen Wang, Jiwu Huang, Security Analysis on Spatial 1 Steganography for JPEG Decompressed Images, Signal Processing Letters, IEEE, Vol. 18, Issue No. 1, Pages No. 39 42, Jan., 2011.
- [5] Dr.EktaWalia, PayalJainb, Navdeep, An Analysis of LSB DCT based Steganography, Global Journal of Computer Science and Technology, Vol. 10, Issue No. 1, April, 2010.
- [6] A New Approach for LSB Based Image Steganography using Se- cret Key. (S. M. Masud Karim, Md. SaifurRahman)
- [7] Hash Based Least Signicant Bit Technique for Video Steganography (HLSB) (Kousik Das- gupta, J. K. Mandal, Paramartha Dutta,) XIII
- [8] A Secure Image Steganography Based on RSA Algorithm and Hash- LSB Technique (Anil Kumar ,Rohini Sharma)
- [9] L. A. Elrefaey, M. E. Allam, H. A. Kader, andM. Selim, Robust blind imageadaptive watermarking, in Proceedings of the 25th