Steganographic Technique for Color Image Using BPCS and Watermarking

Ms.Shaheen M. Nadaf[1], Prof. A. B. Palave[2], Prof. S. B. Chaudhari[3]
Department of Computer Engineering
[1, 2, 3]Trinity College of Engineering and Research, Pune

Abstract*-Information security is the most important factor in todays world. The data that is transfered must be secure. Hence there are different techniques evolved for secret communication. Cryptography technique used to encrypt the secret information while Steganography used to hide the secret information. There are several methods of data hiding like audio, video image, text etc but all these techniques have restricted amount of data hiding capacity. Bit Plane Complexity Segmentation (BPCS) Steganography is a method has 50% data hiding capacity. Data is hidden into the bit planes of the cover image. This method based on the characteristics of human perception system in which a human unable to see any information. Hence By combining two techniques more security will be achieved. So, in this paper Cryptography technique AES and Steganographic technique BPCS is proposed along with Watermarking.*

Keywords-Steganography, Information Hiding, Bit Planes, Cover Image, Secret image, BPCS, Watermarking

I. INTRODUCTION

Steganography is method of hiding information such ways that prevent the diagnosis of hidden messages . Steganography means secret writing. In cryptography data is encrypted such that it is unreadable by a third party. But the goal of steganography is to conceal the data such that it is not seen by the third party. In steganography, mainly contains three component cover image,stego image,secret data .The cover carriers are may be images, audio, video, or text which will hold the secret informatio. A secret data is the information hidden and it may be images, audio,video etc The cover image and the embedded data create a stego image Data embedding mainly requires a stego,key such as a password. The most popular cover objects used for steganography is image.In that image is used as a cover object.

Basic structure of steganograhy model is as shown in the diagram. Steganography is a model composed of three component Embedded message that the sender wishes to hide without any suspicion which a can be audio,video, image or text. Cover Image second component i.e. the cover the original image, audio file, video file, in which the secret message is to be embedded. It is not necessary that the cover and the message should have homogeneous structure. For example, text message or an audio file can also be be hidden into video or image.There are mainly two Steganographic techniques

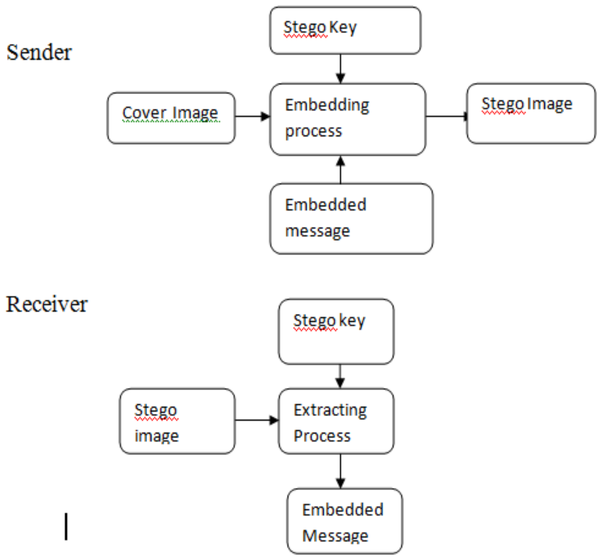

Fig.1. Steganography Model

The Image Domain: It is known as Spatial Domain technique.It insert secret data in the intensity of the pixels. Least significant bit (LSB)-based steganography is among this domain.It replace LSB bit of cover image with the secret data.It does not introduce any distortion.

The Transform Domain: It is also called as frequency domain.In this method , The secret data is inserted in the image after transformation of image.It has advantage over other techniques as they conceal information in areas of the image which is least exposed to transformation such as Image processing,Compression. There are various Substitution technique for steganography is used .It mainly uses only the LSB of the cover object is replaced with the bits of secret data It is easy to implement but it has limited data hiding capacity.

BPCS (Bit Plane Complexity Segmentation) method is proposed in this paper.It mainly consist of finding noisy block and replace it with information. It mainly provides 50% of high data hiding capacity. BPCS mainly increases the embedding capacity by deepen operation on sharpen image. For BPCS- Steganography Canonical Gray coded bit planes are more suitable.It protects against eavesdropping on the embedded information also BPCS Steganography program for each user is easy.

II. PROPOSEDWORK

1)AES encryption the secret text is first encrypted using the AES algorithm 2) BPCS steganography to form the stego image and to hide large amount of vessel data 3) Watermarking will be used to check wheather there are any changes in the image by the hacker

Overall system architectural diagram as shown in the fig2.It mainly consist of sender and receiver at the other end .If the sender want to send the secret msg to the receiver he can send it by encrypting it. At the sender side first sender will choose data that want to send he will first upload image on the system then then encryption of data will text place.Then encrypted data will be embedded into the cover image to form the stego image.and then stego image is send to the other end. And at the receiver side he will extract the original image and the original data after the decryption process.But before the decyption first he will check for the watermark.to check is there any changes in the image? or wheather the changes has been takes place by the attacker.

III. REVIEW OF LITERATURE

Vipul J. Patel and Neha Ripal Soni [1] provide a method for image steganography using modified BPCS steganog- raphy.It mainly enhance security and also it increase data hiding capacity.Hiding capacity of image is not utilize by using the of fix block size and inserting information into bit planes.Hence this is replced by variable block size at each bit planes that increases hiding capacity and it mainly increases security.Proposed method increases the embedding capacity and security.Vaishali and Abhishek Kajal[2] has proposed a method for increasing data hiding capacity of carrier image using BPCS steganography. In this technique data is hidden in bit planes of the cover image.and all the complex or noisy blocks are replaced by secret data.Morghany H Mohmed and Loay M.Mohmed[3] shown the image stegnaographic techniques based on substitution method.LSB substituion method is proposed in this paper which mainly involves replacing LSB of cover image with secret data.It mainly increases high data embedding capacity and better image quality,Smita Bansod and Vanita Mane[4] consider modified BPCS steganography using Hybrid Cryptography means it mainly contains BPCS steganography along with two cryptographic algorithm such as RSA and DES(hybrid cryptography).RSA and DES mainly used to encrypt the secret data and encrypted data is embedded in cover image using BPCS.It provides large embedding capacity.and original secret data can be extracted easily from stego image without assisting original image.M.Kameswara Rao and Epsita Saranya[5] proposed the image steganography using MATLAB approach.It mainly removes the limitation of the LSB.The author has tried to show how to protect the steganography by embedding into another medium using MATLAB. F.P.Musa and S Philip[6] shown the implementation of image using the C# programming language.In this paper they have allowed 1 byte for each of the 3 colour of 24 bit RGB bitmap files.Author has mainly shown the application of image steganography.Hemalata S.and Renuka A[7] shown the comparison of color image steganographic techniques between RGB and YCBCR domain.Both the Tech- niques are compared.RGB method of representation is not secure.In this paper[8]author has shown the overview of image steganography techniques and its uses.Also they have shown the requirement of good dteganoghraphic algorithm.also They have shown that diffrent image file format have differnt method of hiding messages.This paper[9]mainly shows the overview of the steganography and steganographic techniques and its application they have shown various method used in steganog- raphy such as such as Spatial Domain Method and Transform Domain Method.This paper[10]shows the study of steganography and various types of steganography

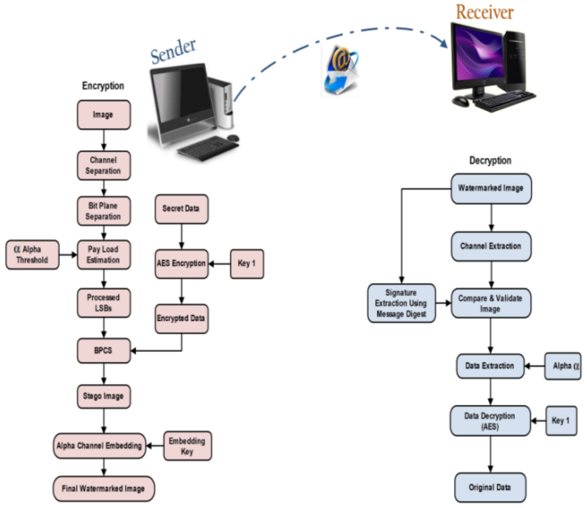

Fig.2. Proposed Architecture

IV. CONCLUSION

Improved LSB has drawback of limited data hiding capac- ity.Hence in this proposed system for hiding large amount of data the BPCS steganographic method for color image is proposed. Also the secret data that is embedded in the cover image is first encrypted by AES algorithm.encrypted data is embedded in cover image using BPCS.It hides 50%of data And it mainly provide resistance to analysis of steganalysis .it has high data embedding capacity.Performance of steganog- raphy will be conveniently tested by using AES algorithm and the design will provide higher security and reliability. Hence by combining steganography and cryptography more security will be achieved.Also watermarking concept is mainly proposed in it which ensures better security

ACKNOWLEDGMENT

I take this opportunity to express my sincere thanks to my guides Prof.A.B.Palve for his valuable guidance, enthusiastic attitude suggestions throughout the period of my research work. I am indeed grateful to Prof.S.B.Choudhari (HOD Comp dept) Trinity College of Engineering and Researchfor providing me the necessary facilities, infrastructure and encouragement for completion of my dissertation work .I wish to express my gratitude thanks to all the staff members of Trinity College of Engineering and Research for their kind co-operation and encouragement.

REFERENCES

[1] Vipul J. Patel Ms. Neha Ripal Soni, Image Steganography System using Modified BPCS Steganography Method,@IJERT volume 3,issue 6 june 2014

[2] aishali, Abhishek Kajal, Increasing Data Hiding Capacity of Carrier Image Using BPCS Steganography@IJSR Volume 4 Issue 5, May 2015

[3] Marghny H. Mohamed and Loay M. Mohamed, High Capacity Image Steganography Technique based on LSB Substitution Method Appl. Math. Inf. Sci. 10, No. 1, 259-266 (2016)

[4] Smita P. Bansod Vanita M. Mane Leena R. Ragha, Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity 978-1-4577-2078-9/122011 IEEE

[5] M. Kameswara Rao, K. Pradeep Reddy and K. Eepsita Saranya Department, Security Enhancement in Image Steganography a MATLAB Approach Middle-East Journal of Scientific Research 23 @IDOSI Publications, 2015

[6] E.P. Musa and S. Philip, Secret Communication Using Image Steganography,@ IEEE Vol 8. No. 3 September, 2015

[7] Hemalatha S, U Dinesh Acharya,and Renuka A, Compariosn of secure and High capacity colour image Steganography Techniques in RGB and YCBCR Domain ”@International Journal of Advanced Information Technology (IJAIT) June 2013

[8] Mr. Falesh M. Shelke1, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni, Comparison of different techniques for Steganography in images @IJAIEM Volume 3, February 2014

[9] Shikha Mohan and Satnam Singh, Image Steganography: Classification, Application and Algorithms, @ IJAIEM Volume 1, Issue 10, January 2015

[10] Rajesh Kumar and A.J.Singh,Understanding steganography over Cryptography and Various Steganographic Technique@IJCSMC,Vol 4,Issue 3 March 2015

[11] X. Liao, and J. Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, @Journal of Visual Communication and Image Representation, vol 22,@2011

[12] E.P. Musa ,S. Philip, Secret Communication Using Image Steganography,@IEEE 2015