An Efficient Data Hiding Approach on Digital Color Image for Secret Communication

Miss. Sayali Shivaji Chavan [#1], Prof. Meena.S.Chavan [*2]

Department of Electronics Engineering, Bharati Vidyapeeth Deemed University college of Engineering Pune, India

Abstract: *In this research paper I have proposed the method of an efficient data hiding approach on digital color image for secret communication. The method is applicable for confidential data transfer, secret communication, copyright protection for digital media and military purpose. Steganography process is used for this. Steganography is the process of hiding secret information behind the original cover file. This file may be audio, video or image file. In this system the digital image is taken as input image and preprocessing of input image is done with the help of MATLAB. Any noise present in image is detected and removed in the image preprocessing technique. A given input image is converted into three different planes i.e. red, green and blue plane. After the plane separation embedding process takes place. Also one password is added at the time of embedding process as well as data extraction process, so that no one can easily hack the data. Chaos algorithm is used for data encryption. After the embedding process stego image is formed. In the data extraction process we have to get back original information. So that Chaos decryption algorithm is used to retrieve secret data and cover image. The primary idea of this project is to increase data hiding capacity and reduce image quality degradation.*

Keywords: *data hiding, secret communication, MATLAB, Chaos algorithm, stego image*

I. INTRODUCTION

Information security is most important part of the secret communication. To increase the information security Data hiding, cryptography, steganography or watermarking techniques can be used. Those techniques are closely related to each other. Cryptography is the study of secure communication also it protects the content of the message alone. Steganography is the art of hiding the secret information into the digital cover image.

Using Reversible data hiding process both the embedding secret information and original cover image can be reconstructed back at the output. Privacy, security and protection are three major aspect of the steganography process. Military, medical, security and legal scenarios are the main applications. Privacy protection is main issue in such applications so the secret information which is to be transmitted is encrypted before transmission and this encrypted information is hidden into the cover image. This data hiding process is called as steganography. There are different methodologies can be used for data encryption and data embedding.

In this system Chaos algorithm is used for data encryption and decryption. This algorithm gives efficient performance for experimental results on audio and image data encryption and decryption. Also this algorithm can be applied for secure real time encryption and safe transmission of confidential data.

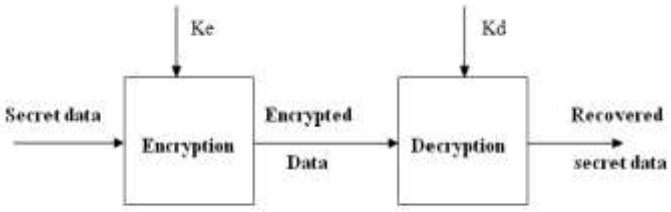

Fig1. Encryption and Decryption procedure of secret data

This technique is used to prevent data from different attacks while sending from transmitter to receiver. At the transmitter side encryption operation is performed and at the receiver side decryption operation is performed. In the encryption process secret data and encryption key (Ke) are inputs and in the decryption process encrypted data and decryption key (Kd) are inputs. After the completion of encryption process the encrypted data is transmitted to the destination. At the destination decryption operation is performed and after decryption secret data is recovered back. So, this technique is used for secret data transmission in different applications.

In proposed system we are using,

- Plane separation, Chaos algorithm , data Encryption, data Extraction using sensitivity, specificity, accuracy, MSE, PSNR, Entropy, Correlation and SSIM.

Advantages:

- Highest security can be provided using steganographic technique for confidential data.
- This technique improves data hiding capacity.
- Data extraction of hidden information from the medium is accurate and reliable.

Applications:

- Confidential data transfer
- Secret communication
- Copyright protection
- Secret data transfer in military

II. REVIEW OF LITERATURE

Steganography is a technique in which the secret message or secret information is hidden into the cover medium. The cover medium may be any type of medium such as text, image, audio or video file. The secret message which can be embedded into the text file has limitation of size, because in text file very less data can be hidden.

A. Related Work:

Previously, cryptography technique was used for data hiding as well as providing data security such as confidential data transfer and trademark. Modern cryptography provides protection in the fields of mathematics, computer science, and electrical engineering. Cryptography is nothing but the encryption. In this technique the readable information is converted into the encoded form. At the receiving side encrypted message is decoded to recover the original information. Applications of the cryptography technique are ATM cards, e-mail privacy, computer passwords, and electronic commerce.

1) ***Stegnography:-***

In the Steganography technique secret information is hidden into secret medium in such a way that only the sender and predefined receiver can sense presence of the secret message. Steganography is Greek word and meaning of this word is "concealed writing" or "covered writing". Images, articles, shopping lists, etc. can be used as cover text in the steganography.

Steganography technique provides more security than that of cryptography technique. Cryptography technique protects the contents of a message. Steganography technique protects both the messages (secret message and cover message) and communicating parties.

Steganography contains the hiding information within the computer files. In digital steganography, document file, image file, program or protocol are also used as a medium for hiding data. Media files are large in size. So, these media files are more effectively used for the steganography technique.

2) ***Watermarking:-***

"Watermarking" is the technique in which digital information is hidden into the carrier signal. The hidden information does not have any relation with the carrier signal in which the digital information is hidden. Digital watermarking technique shows the identity of its owner. This technique is used for verification of authenticity or integrity of the carrier signal. Applications of watermarking technique are broadcast monitoring, ownership assertion, content authentication.

Traditional Watermarking technique is applicable for images or video files. Digital watermarking is applicable for images, audio and video files, texts or 3D models. So many different watermarks can be carried by a signal at the same time. There are different properties of a digital watermarking and they are depending on the applications.

Steganography and digital watermarking technique has similarity that steganographic technique is used to embed data in cover signals. But the difference is, steganography aims for invisibility to human eyes and control the robustness is very important in digital watermarking.

One of the application of digital watermarking technique is source tracking. At the point of distribution different watermarks are embedded into a digital signal i.e. cover signal. Sometime work is found as copied, then the watermarks retrieved from the copy and the source of the distribution is known. This is used to detect the source of illegally copied movies.

The rest of paper is as follows. Block diagram is given in section 3. Section 4 contains implementation and the results. Conclusion, acknowledgment and the references are given the section 5, 6 and 7 respectively.

III. BLOCK DIAGRAM

In this paper I have proposed a secret communication method using digital color images. In this method color images are used as cover images for hiding secret data. This technique is applicable for all type of secret communication.

Using MATLAB I have taken an input image which is digital color image. Different operations are performed on the image such as image preprocessing, plane separation, image encryption, embedding input

image and secret data, formation of STEGO image, image decryption and extraction of input image and secret data.

Following block diagrams shows the data embedding process and data extraction process.

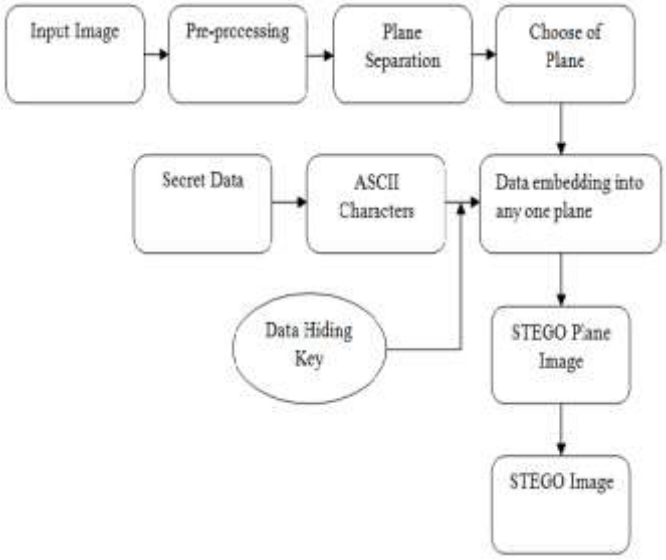

Fig2: Embedding Process Block diagram

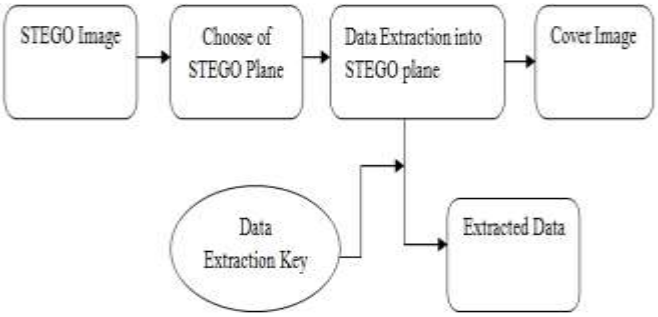

Fig3: Extraction Process Block diagram

This system is applicable for color images. So, digital color image is taken as an input image. This digital color image is separated into the three different planes such as red plane, green plane and blue plane. The secret information which is to be transmitted is converted into the ASCII form for encryption purpose and the secret key is added into that encrypted data for the security purpose.

In chaos algorithm two variables are used. They are constant variables. In the process of encryption threshold value is decided. EX-OR operation is performed in between this threshold value and secret data. Also at the time of decryption EX-OR operation is performed on the input of decryption block i.e. received encrypted data and constant variables.

Then the encrypted secret information is hidden into the R-G-B planes in the embedding process. This process forms R-G-B stego plane images. Combining these R-G-B stego plane images a STEGO image is formed.

In data extraction process STEGO image is taken as input image. Then STEGO plane is selected and data extracted from that STEGO plane. To complete the data extraction process data extraction key must be added. This data extraction key is same as that of the secret key which is used at the time of data encryption. If that data extraction key and secret key are different from each other, then the original data can't be retrieved.

The data extraction key and secret key matches to each other then and then only the secret data and cover image can be retrieved back originally.

IV. IMPLEMENTATION AND RESULTS

The image shown in fig4 is how to create GUI file with the help of MATLAB, fig6 shows the selected input image, fig7 R-G-B plane seperation...

Fig4: GUI file of output window

Fig4 shows GUI file of output window. Which consist of Browse, plane separation, secret data, embedding process, data extraction and validation buttons. Validation window contains sensitivity, specificity and accuracy blocks to show the results.

Fig5: selection of input image

Click on the browse button then it shows a window which contains number of images stored in the current directory. We can choose any one image as a cover image from that current directory.

Fig6: Selected input image

Fig6: shows selected input image.This image act as cover image for hiding secret data. Cover image can be used as any type of image eg. .jpg, .png etc.

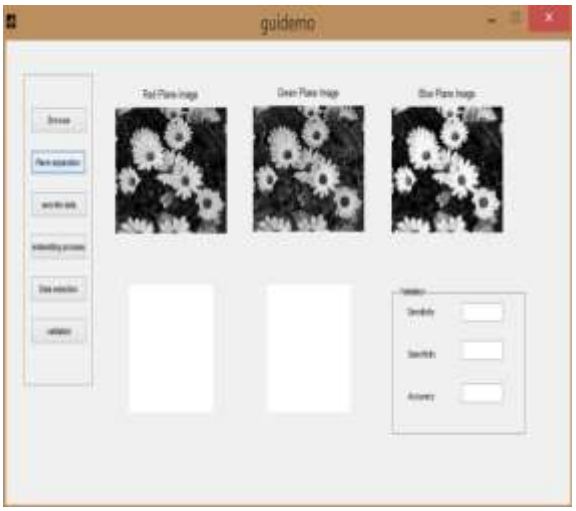

Fig7: R-G-B Plane seperation

Fig7 shows R-G-B Plane seperation of digital color image. This process is used to store secret information which is to be transmitted.

Fig8: Secret data

Fig8. shows the secret data which is to be transmitted. Secret data is stored in the notepad. Secret data may be any type of information such as alphabets, letters, digits or symbols etc.

Fig9:Addition of secret key for embedding process

After seperation of R-G-B plane we have to hide secret data into the planes. First the secret data converted into the ASCII code format. For hiding secret data four digit secret key must be added. Secret key may be any digits, alphabets or any symbols. After addition of valid secret key stego R-G-B images are formed. And the embedding process of secret data and cover image is also started. But the same secret key must be added at the time of data embedding process and data extraction process. Then and then only secret data and cover image can be recovered back at the time of extraction. User cant extract data without correct secret key.

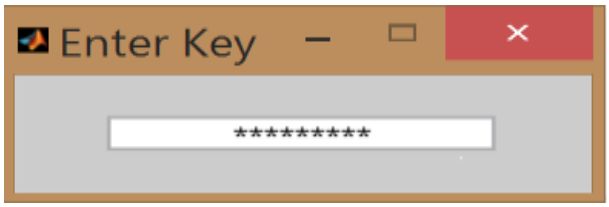

Fig10: Secret key more than 4 digits (Invalid key)

Fig11. Invalid secret key

Less than or more than four digit key is invalid key. If invalid or wrong key gets added then

error will be ocurred, message box display message 'Enter the valid key' and all the process will be closed.

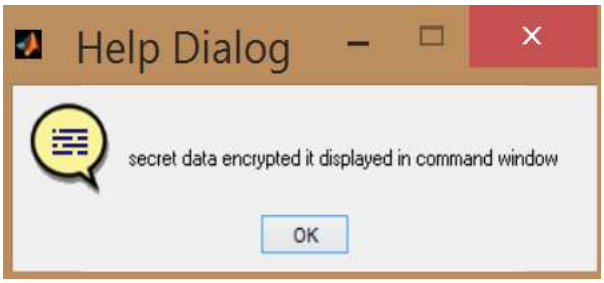

Fig12: Dialog box

After the addition of correct secret key dialog box gives information that 'secret data encrypted it displayed in command window'. Secret data encryption is must be needed for security purpose.

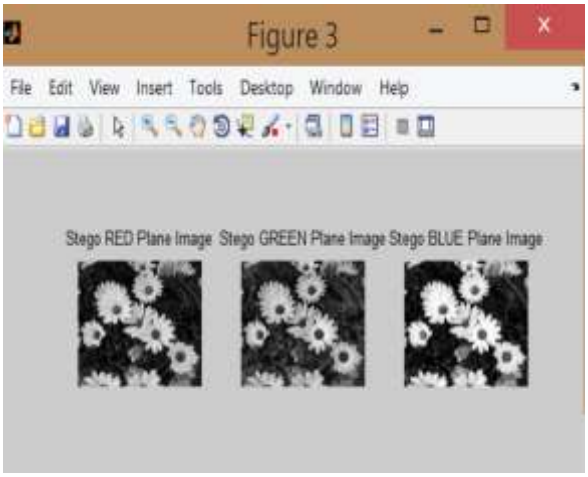

Fig13: STEGO Plane seperation

To form a STEGO image, STEGO R-G-B planes are combined together. STEGO R-G-B planes are the R-G-B planes of cover image in which secret information is hidden. It is part of data embedding process.

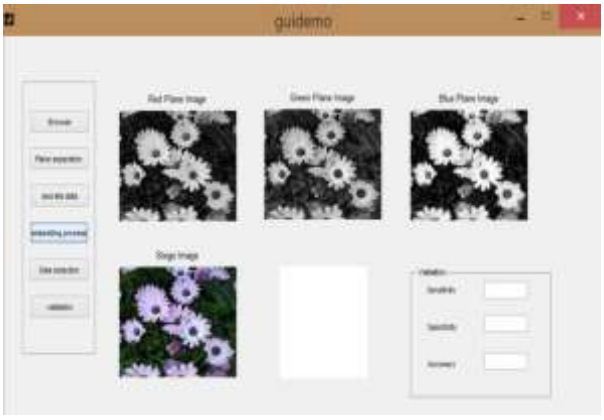

Fig14: Embedding process

Fig14 shows the STEGO image. After addition of the secret key embedding process sarts. In the data embedding process ASCII code of secret data, R-G-B planes of cover image and the four digit secret key are combined together and form a STEGO image. Quality of the STEGO image must be maintained after addition of the secret data for the security purpose. This STEGO image is transmitted to the receiver and data extraction process will be starts.

In this section results of extraction process are displayed. Fig15 shows addition of secret key for data extraction process. Fig17 is the output image of data extraction process. Fig19 is output image of performance metrics. Fig20 shows the output image with all the parameters. Fig 21 shows the extracted data.

Fig15: Addition of secret key for data extraction

In the data extraction process the receiver must be added same secret key which is to be added at the time of data embedding process. When data extraction button is pressed then secret key has been asked. If the correct secret key is added then a message box shows the message 'Secret key successfully added'. Then press OK button. If the wrong secret key gets added then entire process is closed.

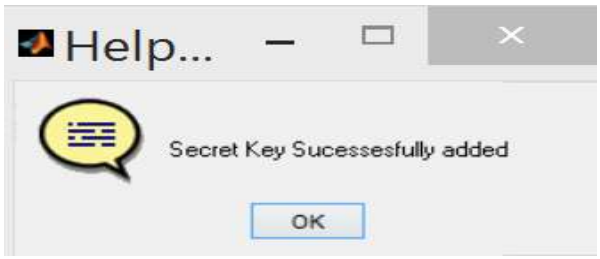

Fig.16: Dialog box

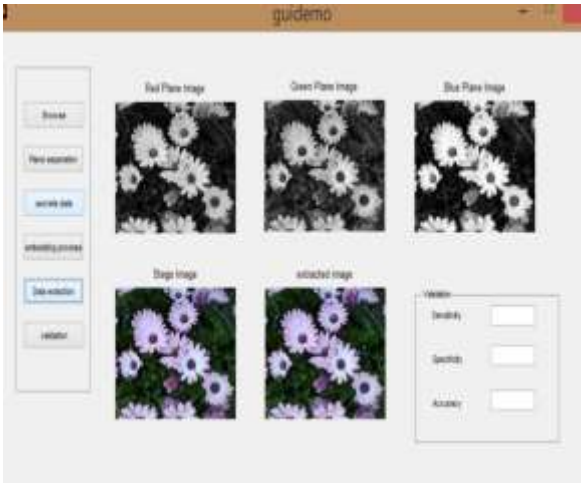

Fig17: Output image of data extraction

Fig17 shows the extracted image. After successful addition of secret key the cover image and secret data are recovered back. The cover image is shown as extracted image in above figure.

Fig.18 Dialog box

Above dialog box gives information that 'Extracted data displayed in command window'.

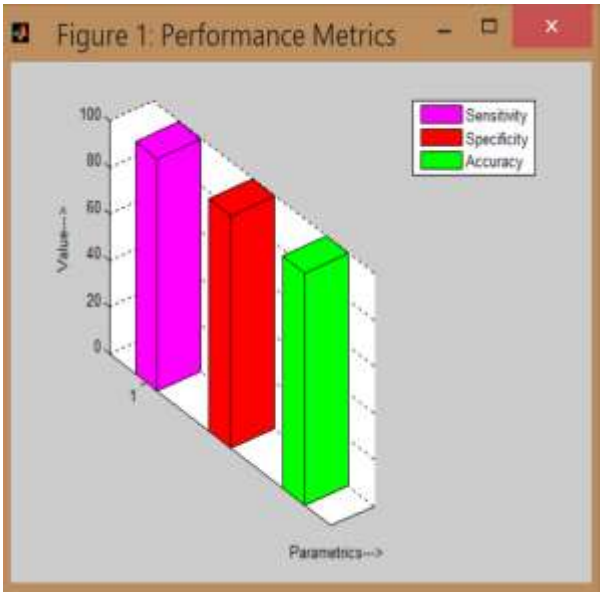

Fig19: Output image of performance metrics

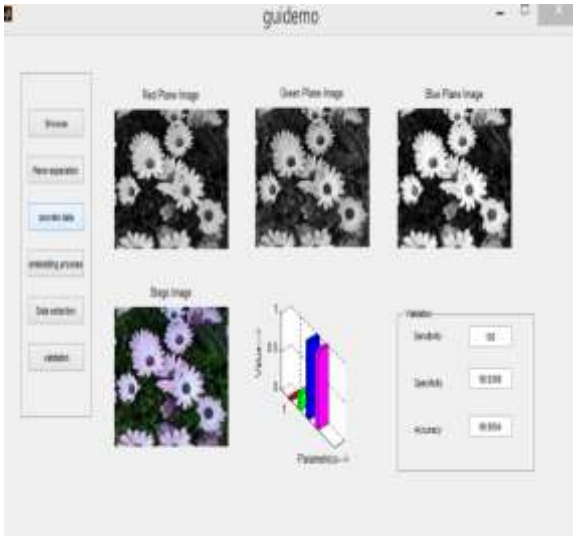

Fig20: output image with all the parameters

When we press the validation button on GUI window we get performance metrics and values for all the parameters. After the extraction of cover image and secret information the quality of image must be maintained. The performance metrics shows the performance in the form of sensitivity, specificity and accuracy and anther graph shows values for MSE, Entropy, Correlation and SSIM.

Fig21: Extracted data

Fig21 shows the extracted secret data, values of MSE, PSNR, Entropy, Correlation, SSIM, Sensitivity, Specificity and Accuracy for the extracted cover image shown in command window.

V. CONCLUSION

In this project we have proposed an efficient data hiding method. This method is applicable for

digital colour images. Steganography technique is used in this system. It is the process of hiding secret information into cover image. So, digital colour image is taken as an input image and encrypted secret data is hidden into the cover image. All the processing is done in MATLAB. R-G-B plane separation and chaos algorithm are used for data embedding process. Data extraction is accurate and reliable. After the data extraction process the cover image and secret data are recovered back originally. System increases data hiding capacity and reduces image quality degradation. Also, the system has wide range of applications.

VI. ACKNOWLEDGEMENT

I am immensely grateful to Prof. Meena S. Chavan who provided support and expertise that greatly assisted the re-search.

VII. REFERENCES

[1] Xiaochun Cao, Senior Member, IEEE, Ling Du, Xingxing Wei, Dan Meng, Member, IEEE, and Xiaojie Guo, Member, IEEE "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation" IEEE TRANSACTIONS ON CYBERNETICS, VOL. 46, NO. 5, MAY 2016

[2] Han-Zhou Wu, Student Member, IEEE, Yun-Qing Shi, Fellow, IEEE, Hong-Xia Wang and Lin-Na Zhou "Separable Reversible Data Hiding for Encrypted Palette Images with Color Partitioning and Flipping Verification" 2015 IEEE

[3] Smita Kuldiwar, Deepa Parasar "Reversible Color Transmission of Compressed Fragment–Visible Mosaic Image" 2015 IEEE International Conference on Computational Intelligence and Computing Research

[4] Tomáš Denemark, Mehdi Boroumand and Jessica Fridrich "Steganalysis Features for Content-Adaptive JPEG Steganography" 2015 IEEE.

[5] Deepali G. Singhavi, Dr. P.N.Chatur "A New Method for Creation of Secret-Fragment Visible-Mosaic Image for Secure Communication" ICIIECS'15 2015 IEEE

[6] Milia Habib, Bassem Bakhache, Dalia Battikh, Safwan El Assad "Enhancement using chaos of a Steganography method in DCT domain" 2015 IEEE.

[7] Pradeep H Kharat, Dr.S.S.Shriramwar "A secured Transmission of data using 3D chaotic map encryption and data hiding technique" 2015 IEEE.

[8] K. Sakthidasan@Sankaran and B. V. Santhosh Krishna "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images" International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.

[9] Gyan Singh Yadav, Aparajita Ojha "A Scalable Data Hiding Scheme using Hilbert Space Curve and Chaos" 2015 IEEE.

[10] Prashant Johri, Arun Kumar, Amban. Galgotias University, Greater Noida "Review Paper On Text And Audio Steganography Using GA" International Conference on Computing, Communication and Automation (ICCCA2015)

[11] Richa Khare, Dr. Kuldeep Raghuwanshi "A REVIEW OF VIDEO STEGANOGRAPHY METHODS" International Journal of Research in Advent Technology Volume 2, Issue 1, January 2014

[12] Bingwen Feng, Wei Lu, Wei Sun "Secure Binary Image Steganography Based on Minimizing The Distortion on The Texture" 2013 IEEE

[13] Gunjan Nehru, Puja Dhar "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

[14] Silvia Torres-Maya, Mariko Nakano-Miyatake and Héctor Perez-Meana SEPI, "An Image Steganography Systems Based on BPCS and IWT" Proceedings of the 16th IEEE International Conference on Electronics, Communications and Computers (CONIELECOMP 2006)