ISSN:0975-9646

Enhanced Approach to Steganography Using Bitplanes

B.Ramesh Kumar, K.Suresh, S.K.Basheer, M. Raja Krishna Kumar

Dept. of CSE,Geethanjali College of Engg and Tech,
Cheeryal(V),Keesara(M)

Abstract—**Steganography is the concept of embedding information in such a way that its existence is concealed. In this paper we have shown one of the techniques used in Steganography to hide information and deliver the message to the end user using Bit-planes without any loss of data. The method used is to replace lowest 3 or 4 LSB with message bits or image data (assume 8 bit values). We do this method for 8 bits starting from 0 to 7 as 0 is the least significant bit. A bit-plane consists of bits corresponding to same significant level in all the elements.**

Key words—**Bit-planes, cover image, LSB, Stego image, Steganography, Steganalysis.**

I. Introduction

Steganography and cryptography are the concepts used to hide the content of messages. Cryptography is the technique where it focuses mainly in hiding the content of the message whereas Steganography concentrates on existence of message. Steganography can be implemented using an image as a media or a text or an audio file etc. In our paper we have considered image as cover media. The cover media is taken and message is hidden in the image by encrypting using a Stego-key this image is called as Stego-image. The information is retrieved back by the receiver using the secret key which the sender sent to decrypt the message. This is the basic process of Steganography which will be presented using our method.

Bit-plane consists of bits corresponding to the same significant level in all the elements. For example the most significant bit is formed by considering the most significant values of each element.

In this paper a robust Steganography implementation is presented that prevents from extracting the data which is hidden in the cover image. We take the image and hide information in the LSB first and see the results and then implement by changing the pixel values from 1 to 7 bits.

In the next sections we see first what Steganography is followed by encryption algorithm, decryption algorithm Bit-plane methods, Results, Conclusion and Future scope, References.

II.Steganography

Steganography is derived from Greek words which means “covered writing”. Steganography is the art of communication in such a way that the existence of the message is concealed.

II.I STEGO-SYSTEM CRITERIA

Stego system criteria is that cover data should not be significantly modified i.e. perceptible to human perception system. The embedded data should be directly encoded in the cover and not in the wrapper or header. Embedded data should be immune to modifications to cover. Distortion cannot be eliminated in the image so error correcting codes need to be included whenever required.

II.II PARAMETERS

Embedding capacity: It refers to the amount of data that can be inserted into the cover-media without deteriorating its integrity.

Perceptual transparency: It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.

Robustness: It refers to the ability of embedded data to remain intact if the stego-image undergoes various transformations such as scaling, rotation, cropping or compression.

Tamper resistance: It refers to the difficulty to alter or forge a message once it is embedded in a cover-media, such as replacing a copyright mark with the one claiming legal ownership.

Computational complexity: Computational complexity of steganography technique employed for encoding and decoding is another consideration and should be given importance.

II.III PLACES TO HIDE INFORMATION

Information can be hidden in various cover media’s such as images, audio files, video files, text files. In this paper we focus on images as cover media.

Steganography in images are stored in array of numbers representing RGB values for each pixel. Common images are in 8-bit/pixel and 24-bit/pixel format. 24 bit images are colour images which have a lot of space for storage but are huge and invite compression. 8 bit images i.e. gray-scale image are good option taking memory into consideration.

The basic process in hiding the message and delivering the message through the Stego-image using the cover media as the image is shown in FIG 1; the retrieving of the message from the obtained Stego-image at the receiver side is shown in FIG 2.

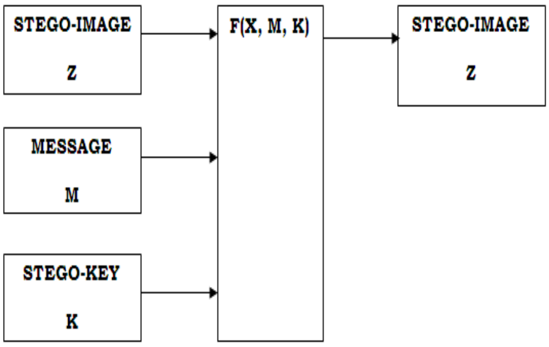


FIG1: HIDING THE MESSAGE IN COVER IMAGE

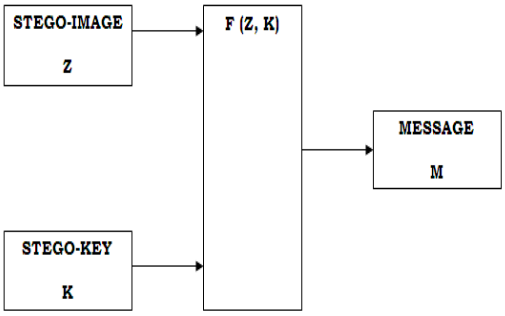


FIG2: RETRIEVING THE MESSAGE FROM THE STEGO IMAGE

II.IV IMAGES IN BMP FORMAT

A BMP file format also called bitmap or DIB file format (for device-independent bitmap), is an image file format used to store bitmap digital images. JPEG file formats gets changed if any change in pixel occurs and easily identified by the third party that some information is been hidden in the image. Even if large amount of data is to be hidden in the image JPEG is not the correct choice.BMP file formats are best suited to hide quite large message. BMP is most suitable for applications, where the first focus is on the amount of information to be transmitted and then on the secrecy of that information.

III BOOLEAN XOR OF COMPLEMENTED MESSAGE ENCRYPTION ALGORITHM(BXCMEA)

- **STEP1:** Convert the message string into binary format.
- **STEP 2:** Find the 2's complement of the string.
- **STEP 3:** XOR the 2'complemnt string with the secret key.
- **STEP 4:** Encrypted txt obtained.

IV BOOLEAN XOR OF COMPLEMENTED MESSAGE DECRYPTION ALGORITHM(BXCMDA)

- **STEP 1:** The encrypted text is taken and XOR operation is performed with the secret key used during encryption.
- **STEP 2:** Find the 2's complement of the value obtained after XOR operation.
- **STEP 3:** Message decrypted.

V BIT-PLANE METHOD

A Bit plane consists of the bits corresponding to the same significant level in all the elements. For example, the most significant bit plane is formed by considering the most significant bit (MSB) of each element. The elements of a gray scale image have a maximum value of 255 and hence can be represented in binary domain using 8 bits. Higher order Bit planes of an image carry a significant amount of visually relevant detail. Lower order Bit planes contribute more to fine details.

Variations include:

- Using a combination of pixel locations at which to hide the bits.
- Put bits at only certain locations in image such that change in gray-value would not be visually perceptible.

The algorithm of the Bit plane is as follows:

- **STEP 1:** Select the image and convert into grayscale.
- **STEP 2:** Choose the number of bit planes where the text is to be inserted.
- **STEP 3:** Encrypt the text using a key and convert into binary.
- **STEP 4:** Embed the encrypted text into the image.
- **STEP 5:** Now decrypt the text from the image using the key.
- **STEP 6:** Retrieve the text.

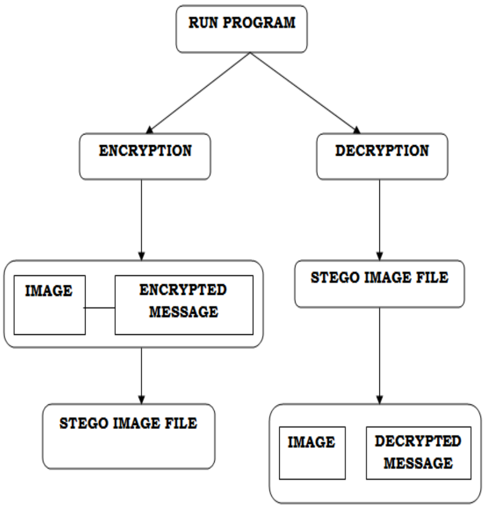


FIG 3: EMBEDDING ENCRYPTED MESSSAGE AND DECRYPTING OF MESSAGE

The results obtained after the whole process is as follows:

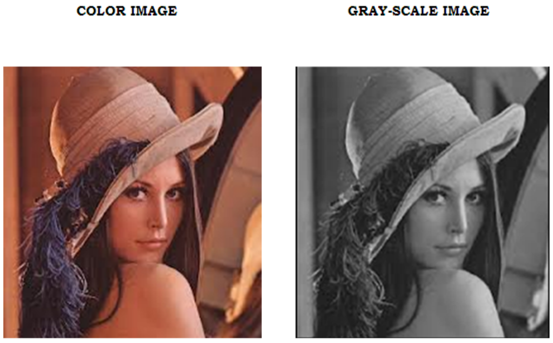


FIG4: CONVERSION OF COLOR IMAGE TO GRAY

In our method the message bits are placed in the plane in such a way that they are not arranged linearly. This gives security to the message. The arrangement of bits cannot be traced out by any unwanted user, for example the encrypted message **10011100** is arranged when we consider number of bits say n=0 see FIG 5.In the same way when we consider the number of bits is equal to 1,2,3 and so on can be arranged in the same manner. Let us have a look of the arrangement of bits .in FIG 5.1for n=1

FIG 5.2 for n=2 and FIG 5.3for n=3 this can be done up to n=8.

For example:

Binary representation for ‘a’

01100001

Let the key be 3. Then

Key=00000011

After encryption of the message using given key

Encrypted Message=10011100

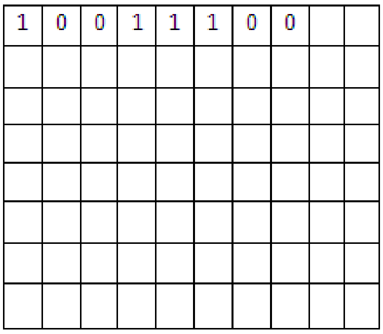


FIG5: LSB 0 BIT-PLANE

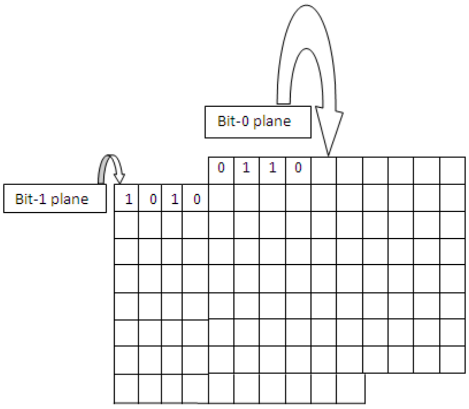


FIG 5.1: 2-BIT PLANES ARE CONSIDERED

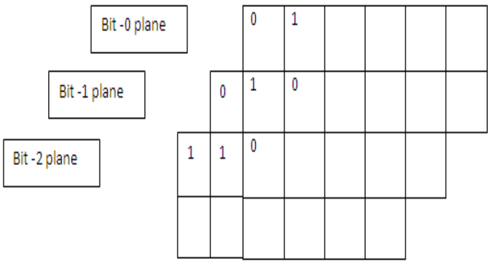


FIG 5.2: 3-BIT PLANES ARE CONSIDERED

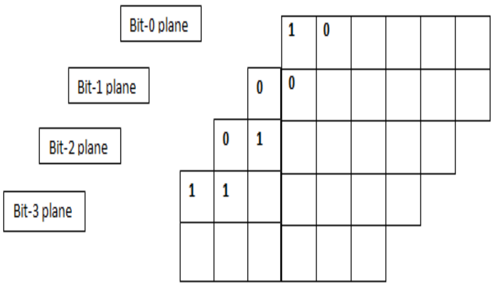
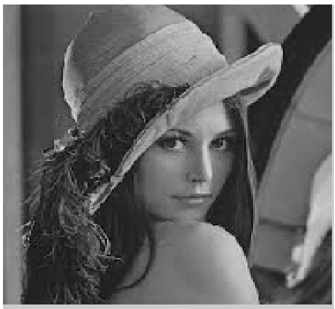


FIG 5.3: 4-BIT PLANES ARE CONSIDERED

VI EXPERIMENTAL RESULTS

ORIGINAL IMAGE

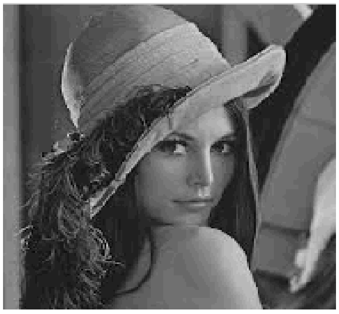


1-BIT PLANE(LSB) STEGO IMAGE

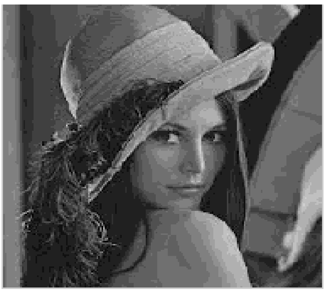
2-BIT PLANES STEGO IMAGE

3-BIT PLANES STEGO IMAGE

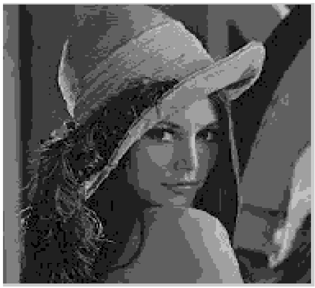
4-BIT PLANES STEGO IMAGE



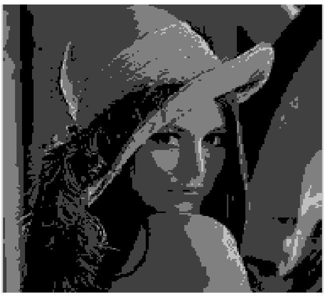
5-BIT PLANES STEGO IMAGE



6-BIT PLANES STEGO IMAGE



7-BIT PLANES STEGO IMAGE



8-BIT PLANE STEGO IMAGE

VI CONCLUSION AND FUTURE SCOPE

We built a Steganography algorithm based on embedding into the bit planes of the cover image. We even tested our method for RS steganalysis, using a steganalysis tool “vsl1.1”. The analyzer failed to detect the text which has been sent to the end user and LSB decryption which failed to detect the message; by this we can say that our method is efficient.

Few more implementations can be made like extending from gray-scale images to color images. Take high quality measures to pass more data in safe way making it not easy to detect the presence of messages or extract the messages from unwanted users.

REFERENCES

[1]Secure Bit-plane based Steganography for Secret Communication. Cong-Nguyen BUIya), Nonmember, Hae-Yeoun LEEyy, Member, Jeong-Chun JOOy, and Heung-Kyu LEEy, Nonmembers.

[2]Implementation of LSB Steganography and its Evaluation for Various File Formats. V. Lokeswara Reddy Department of CSE.

[3]R.C.Gonzalez and R.E.Woods, *Digital Image Processing second edition* .Addition-Wesley Publications, Prentice-Hall, 2001.

[4]A.K. Jain, Fundamentals of Digital Image Processing. Prentice-Hall, 1989.

[5] www.jjtc.com/stegdoc/steg1995.html

[6]Steganography Using Least Signicant Bit Algorithm Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav.

[7]http://vsl.sourceforge.net

[8] Multi Bit Plane Image Steganography, Bui Cong Nguyen, Sang Moon Yoon, and Heung-Kyu Lee Department of EECS, Korea Advanced Institute of Science and Technology,Guseong-dong, Yuseong-gu, Daejeon, Republic of Korea *{*nguyenbc, pisces*}*@mmc.kaist.ac.kr

[9]A high quality steganographic method with pixel-value differencing and modulus function, Chung-Ming Wang a, Nan-I Wu a, Chwei-Shyong Tsai b, Min-Shiang Hwang b,*

[10]Steganographic Techniques of Data Hiding using Digital Images Babloo Saha and Shuchi Sharma Institute for Systems Jaipur Institute of Engineering and Technology.

[11]A New Image Steganography Based On First Component Alteration Technique Amanpreet Kaur1, Renu Dhir2, and Geeta Sikka3 Department of Computer Science and Engineering. National Institute of Technology, Jalandhar, India

[12**]**Review:Steganography – Bit Plane Complexity Segmentation (BPCS) Technique, SHRIKANT S. KHAIRE Department of Electronics and Telecommunication, Dr. Babasaheb Ambedkar Technological University

AUTHORS

B.Ramesh Kumar, is a final year undergraduate student in the department of Computer Science and Engineering of Geethanjali College of Engineering and Technology, Hyderabad.

K.Suresh, is a final year undergraduate student in the department of Computer Science and Engineering of Geethanjali College of Engineering and Technology, Hyderabad.

S.K.Basheer, is a final year undergraduate student in the department of Computer Science and Engineering of Geethanjali College of Engineering and Technology, Hyderabad.

M. Raja Krishna Kumar is an Associate Professor in the department of Computer Science and Engineering of Geethanjali College of Engineering and Technology and a Part Time Research Scholar in JNTUH, Hyderabad. He received Master of Technology in Image Processing from JNTUH, Hyderabad and AMIETE in Information Technology from IETE, New Delhi. His main research interests include Image Processing, CBIR and allied fields