INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume2, Issue6)
Available online at: www.ijariit.com

Improved Color Image Steganographic Technique In Transform Domain

K. S. Sadasiva Rao[1], Dr A. Damodaram[2]
1 Associate Professor, Dept of CSE, Sri Indu Institute of Engg. & Technology, Hyderabad, India.
2 Professor of CSE, School of Information Technology, Jawaharlal Nehru Technological University, Hyderabad & The Vice-chancellor, SVU University, Tirupathi, India.
[1]karrisrini@gmail.com, [2]damodarama@rediffmail.com

ABSTRACT: Steganography is the process of embedding original message bits on some carrier file. The carrier file may be text file, image file, audio file or video file etc. If that carrier file is an image file, then that technique is called Image Steganography [1]. If color image is used as a carrier file to embed data bits, then that type of Steganographic technique is called as color image Steganography [7]. In this proposed work, embedding the original message bits in the transform domain of the carrier color image without considering the green plane, hence it is resulting in high quality stego image. Hence this technique is called as improved color image Steganographic technique in transform domain. Here in this paper, DCT (Discrete Cosine Transform) technique has been used.

KEYWORDS: Transform domain technique, Steganography.

I. INTRODUCTION

Image steganography is the process of replacing data bits in the image cover file pixel bits without disturbing the quality of the image. The image files which are used to carry the data bits are called as a cover image or cover file. After embedding the data bits in the image cover file, the cover file is called as stego file. Image Steganographic algorithm, in which the bits of the pixels of the cover image are directly replaced by original message bits, is called as spatial domain Steganographic algorithm.

Most of the image Steganographic algorithms will be using the LSB method as it is not affecting the quality of the cover image after embedding the data bits. Here the carrier file is a color image file, so it is called as color image Steganography [4].

The color image is a combination of three planes Red, Green and Blue. Generally in spatial domain, RGB planes are used to stuff the data bits at least significant bit positions of the pixel. Hence three bits can be stuffed in each pixel among the three planes [6]. But in the transform domain, the pixel values are converted into the transform co-efficient, then those transformed co-efficient to be used to modify the data.

II. RELATED WORK

Steganography is a process of hiding data in other media to transfer the secured information [1]. Most of the Steganographic algorithms are working on gray scale images [5], but some unauthorized user may suspect some useful information is going in gray scale image, because now days nobody is interested in sending the gray scale images as general images [7]. Actually many Steganographic techniques have been implemented either in color or gray scale images.

The Steganographic algorithms are divided into spatial domain technique and transform domain techniques. In spatial domain techniques, the bits in pixels of the carrier color image are directly replaced by the original data bits. But in the case of transform domain techniques, the pixels are transformed into transform domain; those co-efficient are used to embed the secret data bits.

But in the color images, all the three planes RGB have been used to stuff the bits. 3bits/pixel can be added with color images, but the level of distortion is high.

II. PROPOSED SYSTEM

In this work, we applied DCT(Discrete Cosine Transform) Steganographic algorithm to embed the secret data bits on to the carrier color image.

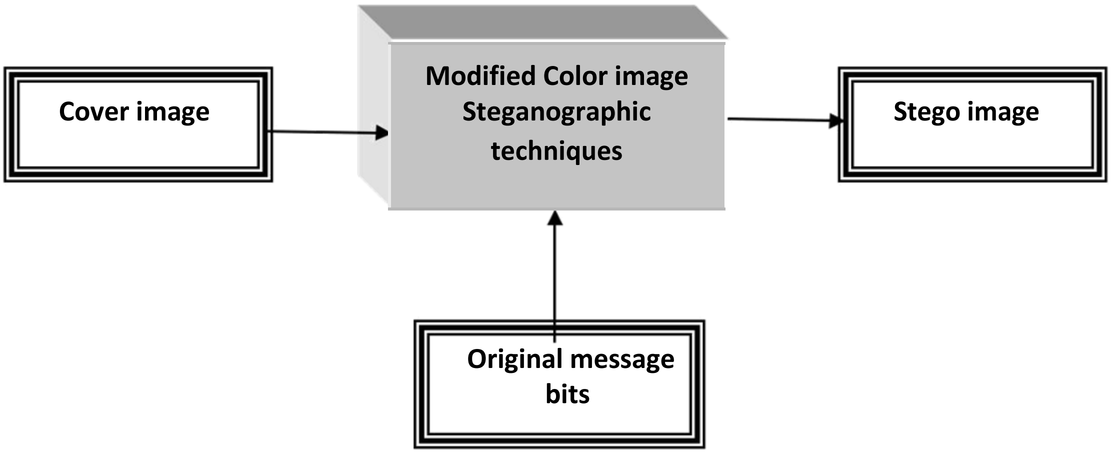

Figure1: Proposed System

In the proposed system, a color image is taken as a carrier file. An image is a group of pixels. Each pixel is represented with 24 bits in the color image, where as 8 bits are used to represent red plane, 8 bits to represent green plane and remaining 8 bits are to represent blue plane. Generally all algorithms in the transform domain will be using all the three planes to embed the original data bits, where as in our proposed work, we found that if green plane is eliminated, it will not affect the quality of an image much [1] [7].

Here a color image is taken as an input carrier file. Only two planes red and blue from each pixel are used to stuff the bits. The least significant 2 – bit positions from red and blue planes are considered to embed the data bits. Hence 4-bits are stuffed for each pixel. So we can embed many number of data bits depending on the image resolution. The same 2-bit LSB algorithm is used for all the three planes RGB, but we found a large disturbance in terms of PSNR and also with human eye, we can identify the distortion in the stego image.

Hence it is proved that' if green plane is modified or stuffed with data bits, we found large remarkable distortion in the stego image'.

IV. PROPOSED ALGORITHM

1. *Read a cover image which is a color image.*
2. *Display the cover image.*
3. *Read the two planes (red and blue) only into twp different variables, these will be converted into matrices.*
4. *Read the original message bits from any input data file.*
5. *Convert the pixels from spatial domain pixel values into transform domain co-efficients.*
6. *Stuff 2-bits of original data bits into 2 LSB positions in co-efficients of pixels of red and blue planes, hence we can embed 4bits/ pixel data.*
7. *Then after embedding convert back into spatial domain and reconstruct a stego image.*
8. *Now whole matrix is converted back to an image using uint8 () function.*
9. *Find mean square error rate (MSE) for red and blue planes, hence green plane is not used as a carrier.*
10. *Find the PSNR value for stego image with following formula*

$$PSNR = 10 \log_{10} \frac{max\ \text{possible pixel values of an image}}{MSE}$$

11. *Display the cover image, stego image and also the PSNR value.*
12. *exit*

V. RESULTS

The following are results of the color image Steganographic algorithm in transform domain (without green plane) with 2-bit LSB algorithm used only on red and blue planes. Secured information bits are stuffed into only two planes Red & Blue (excluding Green plane). Hence the following cover image and stego image will be looking similar. Peak Signal to Noise Ratio (PSNR) is nearly 42 for red and blue planes and infinity for green plane for given stego image which is acceptable, because if PSNR value is more than 20, with human eye we cannot make out the difference between cover image and stego image.

Figure 2: Cover Image Figure

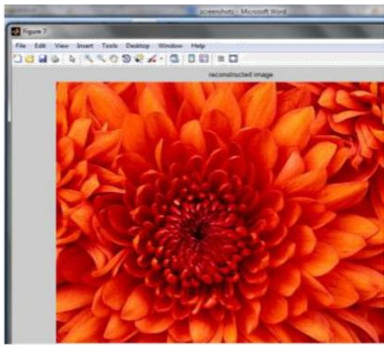

Figure 3: Stego Image

Figure 2 shows the cover image before stuffing the data bits. After stuffing the data bits to this carrier image, it is stego image which is shown in Figure 3.

Mean Square Error (MSE):
Mean square error value is calculated for the stego image and the values are as follows.

MSE=1.6717 (MSE for stego image)

MSE_Blue plane=4.14 (MSE for blue plane of stego image)

MSE_ Red plane=5.08 (MSE for red plane of stego image)

MSE_Green plane=0 (MSE for green plane of stego image is '0' because we did not stuff bits in green plane.)

PSNR for Red plane: 41.1068249 dB
PSNR for Blue plane: 41.9972423 dB
PSNR for Blue plane: ∞

VI. CONCLUSION

In our proposed system, we implemented 2-bit LSB algorithm on only two planes (red and blue planes) of color image. We found better results comparing with applying 2 –bit LSB to all the three planes. Our algorithm is able get a stego image without any distortion and also able to stuff nearly 10, 00,000 data bits. The PSNR value for our proposed algorithm is 42 for the given stego image which is acceptable, because if PSNR value is more than 20, cannot make out the difference between cover image and stego image with human eye.

REFERENCES

1. Niels Provos and Peter Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy, 2003.
2. Saiful Islam, Mangat R Modi, Phalguni Gupta, Edge-based Image Steganography, Springer 2014.
3.
4. Anil Kumar, Rohini Sharma, A Secure Steganography Based on RSA Algorithm and Hash-LSB Technique, International Journal of Advanced Research in Computer Science and Software Engineering, July, 2013.
5.

6. Deepesh Rawat, Vijaya Bhandari, A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image, International Journal of Computer Applications, Volume 64, 2013.
7.
8. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital Image Steganography: Survey and Analysis of Current Methods, Elsevier, 2010.
9.
10. Wien Hong And Tung-Shou Chen, A Novel Data Embedding Method Using Adaptive Pixel Pair Matching, IEEE Transactions On Information Forensics And Security, Volume 7, No. 1, February 2012
11.
12. Niel F Johnson, Sushil Jajodia, Exploring Steganography: Seeing the Unseen, IEEE, 1998.

