A Novel Approach for Image Steganography based on LSB Technique

G. G. Rajput
Department of Computer Science
Rani Channamma University
Belagavi-591156, India
ggrajput@yahoo.co.in

Ramesh Chavan
Department of Computer Science
Rani Channamma University
Belagavi-591156, India
ramesh.chauhan1050@gmail.com

ABSTRACT

Steganography involves communicating secret data in an appropriate digital carrier, e.g., image, audio, and video files. We focus on image based steganography in this paper. A novel approach based on LSB technique for embedding text data i.e. secret image in digital color images is proposed. Secret text is encoded in Least Significant Bits (LSB) of three components of color image namely, red, green and blue (RGB) channels using the angular transformation concept. On the receiving end, the message is extracted by performing the same angular rotation to the stego image. Experiments are performed on standard images and it has been observed that the stego image looks visually the same as like the cover image.

CCS Concepts

- **Computing methodologies → Computer graphics → Image manipulation → Image processing.**

Keywords

LSB; cover image; stego-image; message; text.

1. INTRODUCTION

Steganography is a technique to hide data inside a cover medium in a way that the existence of any communication itself is undetectable. The information that to be hidden is called stego and the media in which the information is hidden is called host. The stego object can be text, image, audio or video.

Basically, the purpose of steganography is to provide secret communication like cryptography. The Characteristic of an effective steganographic scheme must possess the following [5]:

- *Secrecy*: A person should not be able to extract the covert data from the host medium without the knowledge of the proper secret key used in the extracting procedure.
- *Imperceptibility*: The medium after being embedded with the covert data should be indiscernible from the original medium. One should not become suspicious of the existence of the covert data within the medium.
- *High capacity*: The maximum length of the covert message that can be embedded should be as long as possible.
- *Resistance*: The covert data should be able to survive when the host medium has been manipulated, for example by some lossy compression scheme .
- *Accurate extraction*: The extraction of the covert data from the medium should be accurate and reliable.

Image steganography techniques can be divided into two groups [1]: those in the Image Domain and those in the Transform Domain . Image - also known as spatial - domain techniques embed messages in the intensity of the pixels directly, while for transform - also known as frequency - domain, images are first transformed and then the message is embedded in the image.

Taking the advantage of human eye limitation, image steganography uses color image as cover media for embedding secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. Each bit is represented either as a 0 or 1. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye In other words, one can store 3 bits in each pixel. The important quality of image steganography is to retain the originality of cover image (i.e. no distortion) with the embedded secret message. Further, steganography along with encryption gives more security to data.

Image steganography is based on following quantities

- The digital image (Im)- color or gray scale that will hold the secret data
- The secret message (M), a plain text, cipher text or any type of data.
- The stego Encoder (F) and its Decoder (F^{-1})
- An optional stego-key (K) or password to hide and unhide the embedded message.

The block diagram of typical image stenography system is shown in Fig.1

ICCDA '17, May 19-23, 2017, Lakeland, FL, USA
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5241-3/17/05…$15.00
http://dx.doi.org/10.1145/3093241.3093247

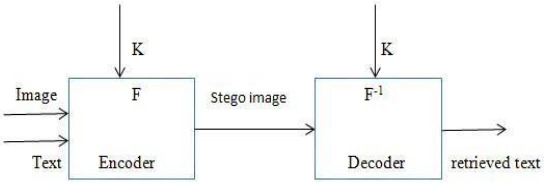

Figure 1. The image steganography system

The effective image steganography scheme allows secret text to be embedded in the image without bringing any noticeable change in the image characteristics. However, the maximum length of the text that can be embedded depends on the image size and dynamic range of intensity contents of the image. Higher the complexed input image higher the data bit hiding in it.

LSB (Least Significant Bit) Substitution based image steganography is the process of modifying the least significant bit of the pixels of the carrier image. We have chosen to implement LSB substitution because of its simple approach and providing variations in embedding the secret message. In this paper, image steganography using color image as cover to hide the secret information is proposed. The text is embedded into three components of the color image namely, red, blue, and green channels.

2. LITERATURE REVIEW

There have been various approaches towards image steganography and some of the methods are described below.

T. Morkel et.al [1] have presented an overview of image steganography, its uses and techniques for hiding the secret text in an image. The requirements of a good steganography algorithm have been discussed. Suitability of image stenographic scheme has been described.

Neil F. Johnson et.al [2] has presented an overview of different steganographic methods which have been proposed in the literature during the last few years. Many flexible and simple methods exist for embedding information in noisy communication channels. Abbas Cheddad et.al [3] presented a discussion on the major algorithms of steganography deployed in digital imaging. The emerging techniques such as DCT, DWT and adaptive steganography are not too prone to attacks, especially when the hidden message is small. Ajit Danti et.al [4] has presented a technique based on randomized bit embedding. Discrete Cosine Transform (DCT) of the cover image is extracted and then the stego image is constructed by hiding with secret message in Least Significant Bit (LSB) of the cover image in random locations based on a threshold. K.P.Adhiya et.al [5] described a method for embedding textual information in wav audio. The audio sample is converted into bits and textual information is embedded in it. In embedding process the message character is converted into its equivalent binary, the last bits 4 bits of this binary is taken into consideration and applying redundancy of the binary code, the prefix either zero or one is used , by using LSB based algorithm.

Hemalata S et.al [6] described an image steganography technique to hide multiple secret images and keys in color cover image using integer wavelet transform (IWT), and results are compared with the results of other techniques. The method exhibits better PSNR value compare to other methods. Ajit Danti et.al[7] have proposed a 2-3-3 LSB insertion method , where in eight bits of secret data at a time is put in LSB of RGB (Red, Green and Blue) pixel value of the cover image in 2,3,3 order respectively to embed a color secret image into a cover image. Information hiding using image morphing has been studied by several authors [8, 9]. In S. Kando et.al [10], the hidden image is transformed into morphing image and use the morphing image as stego image. On receipt of the morphing image, demorphing is done to extract the secret message.

Limitations towards steganographic method can be removed by combining one or more techniques and can achive robustness and acurrate extraction

In this paper, we rely on basic LSB technique to hide secret message by using angular transformation technique. The data is embedded in a color image, in its color components, using 3-3-2 rule, by performing angular transformation of the cover image. Though it combines both spatial and transform domain but sticks to very basic method

3. PROPOSED ALGORITHM

The proposed algorithm works against one of the limitation of steganography i.e. angular transformation of image. Secret data is embedded in LSBs of the color components, RGB, of the image by performing angular transformation. The input image is rotated by 90^0 and starting from the top-left pixel, the secret message is embedded in the LSBs of RGB component of the pixel using 3-3-2 rule, meaning, 3 LSBs bits of red component, 3 LSBs bits of green component, and 2 LSBs bits of blue component.

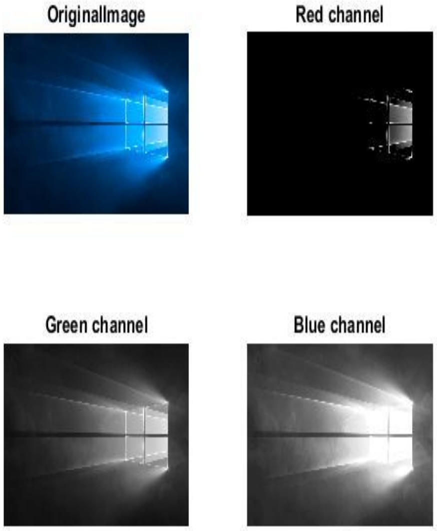

Figure 2. Color image and its additive colors: Red component, Green component and Blue component

The algorithm is described below.

Algorithm: Text hiding in Color Image
Input: Secret text data and RGB color image
Output: Text covered color image
Step 1. Read the cover medium i.e. color image.
Step 2. Read the secret data and perform binarization.
Step 3. Compare size of binarized secret data against size of cover image to ensure that the cover image is not distorted after embedding.
(For example, for true image 24bit of size 20x20 pixels, (8 bits/ pixel) 3200bits of binarized data can be embedded using LSB technique)

```
Step 4. Perform angular transformation to 90 degree of rotation
        to the cover & select LSB bits of red, green, blue
        channels of the cover image
Step 5. Starting from the first pixel (top-left), insert the binarized
        text in the RGB components of the pixel in 3-3-2
        allocation i.e. 3 LSBs of red component, 3LSBs of
        green component and 2 LSBs of blue component.
Step 6. The number of pixels utilized in embedding the text i.e.
        number of bits inserted, is written in LSB of the last
        pixel of the image.
Step 7. Perform reverse angular transformation to retain original
        position of the cover.
Step 8. Output is the stego image
```

Secret Data retrieval is done using the following algorithm

Algorithm: Secret Data retrieval
Input: Secret data embedded cover image
Output: Secret data extracted

```
Step 1. Read the stego image and perform angular transformation
        of 90 degree.
Step 2. Starting form the first pixel position, extract binarised
        data from the red, green and blue components of pixel,
        using 3-3-2 rule, from stego image until the last text bit
        embedded is extracted. The size of the embedded text
        is written in the last pixel of the stego image.
Step 3. Reconstruct the secret message from the extracted bits.
Step 4. Output is the secret message.
```

4. EXPERIMENTAL RESULTS

Windows wallpapers are used to implement the proposed method. The wallpaper images have resolution of 1920x 1200 pixels, 24bit true color.

The original and stego images are presented in Table 1. Histogram of cover image and stego-image for sample image is shown in Fig. 3.

Table 1. Original and stego image

Name	Original	Stego
Img1		
Img2		
Img3		
Img4		

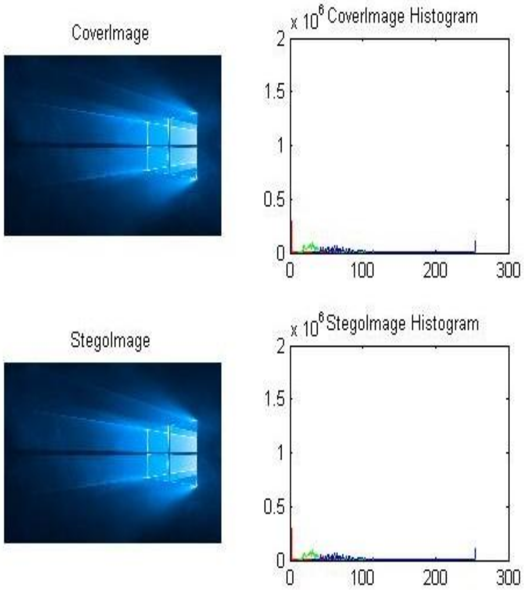

Figure 3. Histogram of Cover and stego image

For stego image, Mean Square Error (MSE) and Peak-To-Signal-Noise (PSNR) [13] ratio is calculated using the following formulas.

$$MSE = \frac{\sum_{MN}\left[I_1(m,n) - I_2(m,n)\right]^2}{M * N}$$

where M and N are the number of rows and columns of image matrix.

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

where R is the maximum fluctuation in the input image data type.

The results of few images are tabulated in the following Table 2.

Table 2. MSE and PSNR of the stego images

	MSE			*PSNR*		
Image	***R***	***B***	***G***	***R***	***B***	***G***
Img1	0.01	0.01	0.01	82.3645	77.1806	78.9295
Img2	0.00	0.00	0.00	80.3657	76.9295	78.8163
Img3	0.02	0.02	0.02	64.3081	65.0079	63.7177
Img4	0.00	0.00	0.00	78.8737	77.0635	78.4470

While the purpose of Steganography is to hide secret information, there are several attacks that one may execute to test for Steganographed images. If, cover image is available, one may compare the stego image with the cover image to check for artifacts. In case of availability of stego-image alone, attacker can perform statistical analysis such as chi-sqaure test to check for possibility of hidden text. The least significant bits can be extracted and processed for extracting the secret text. However, use of complex image and bringing variations in LSB implementation like the one we have proposed in this paper, makes it difficult for attacker to extract the secret text.

5. CONCLUSION

LSB based method for hiding the secret image is proposed in this paper. Text is embedded in the cover image by rotating the image. Different angular rotations can be applied for hiding the text without losing the cover image characteristics. The proposed algorithm is simple and efficient to ensure the information hiding and can be used for various purposes including, storing patients history using his image as cover image, storing significant information about objects in objects image in cloud based environment. The efficiency of the proposed system is tested in terms of visual analysis, PSNR value, and histogram of the both cover image and stego image. The results are satisfactory. It works against the limitations of steganography. The secret message may be encrypted using encryption techniques like RSA and then embedded in the cover image for added security. The proposed system is a basic step towards constructing an efficient stego image and we are working on exploiting the intensity characteristics of cover image to hide the text employing randomness.

6. REFERENCES

[1] T.Morkel, J.H.P.Ellof, M.S.Olivier, "*AN OVERVIEW OF IMAGE STEGANOGRAPHY*". Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), 2005

[2] Neil F. Johnson and Stefan C. Katzenbeisser,Chapter-3, "*A Survey of Steganographic Techniques*", Information Hiding Techniques for Steganography and Digital Watermarking, Artech House London 2000

[3] Abbas Cheddad , Joan Condell, Kevin Curran, Paul Mc Kevitt,"*Digital image steganography: Survey and analysis of current methods*" - Signal processing, 2010 - Elsevier 727–752

[4] Ajit Danti, Preethi Acharya " *Randomised Embedding scheme based on DCT Coefficients For Image Steganography* ". IJCA Special Issue on "Recent Trends in image Processing and Pattern Recognition"RTIPPR,2010

[5] K.P.Adhiya, Swati.A.Patil, "*Hiding Text in Audio Using LSB Based Steganography*" Information and Knowledge Management ,Vol2. No 3.2012

[6] Hemalata S, U.Dinesh Acharya, Renuka A, Priya.R Kamat," *A Secure And High Capacity Image Steganography Technique*",Signal & Image Processing: An International Journal (SIPIJ) Vol. 4, No.1, February 2013

[7] G.R. Manjula , Ajit Danti," *A Novel Based Least Significant Bit(2-3-3) Image Steganography in Spatial Domain"*, Intenational journal of security, privacy and Trust Management(IJSPTM) Vol.4 No 1 february 2015

[8] Kazuki Murakami, Ryota Hanyu, Qiangfu Zhao and Yuya Kaneda, "*Improvement of Security in Cloud Systems Based on Steganography"* International Joint Conference on Awareness Science and Technology & Ubi-Media Computing (iCAST-UMEDIA) 2013 ICAwST.2013.6765492

[9] Bhushan Zope, Soniya Patil, " *Information hiding method based on Stegnography and Image morphing"*, American International Journal of Research in Science, Technology, Engineering & Mathematics, 12(1), September - November, 2015, pp. 27-32

[10] S. Kondo and Q. F. Zhao, "*A novel steganographic technique based on image morphing*," Proc. International Conference on Ubiquitous Intelligence and Computing (UIC06), Wuhan and Three Gorges, China, pp. 806-815, Sept. 2006 (Lecture Notes in Computer Science 4159, Springer)

[11] Krenn.R., "*Steganography and Steganalysis*", http://www.krenn.nl/univ/cry/steg/article.pdf%20

[12] A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment- Bret Dunbar, The information Security reading Room, SANS Institute 2002 https://www.sans.org/reading-room/whitepapers/covert/detailed-steganographic-techniques-open-systems-environment-677

[13] MSE &PSNR http://in.mathworks.com/help/vision/ref/psnr.html