Research Paper

Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

NEW APPROACH FOR STEGANOGRAPHY IN COLOR IMAGES WITH AN IMPROVED PSNR AND LSB TECHNIQUES

Information Technology

KEYWORDS : Steganography, LSB, PSNR, Smooth areas, Edge areas, MSE.

G.S.Raman	Associate Professor, Department of Information Technology, KLN College of Information Technology, Sivagangai, India
R.T.Subhalakshmi	PG Student, Department of Information Technology, KLN College of Information Technology, Sivagangai, India

ABSTRACT

Steganography is an art and science of writing hidden message in the cover image. This paper proposes a new approach for a steganography in color image based on detection technique combining two transform for dividing an image into edge and smooth areas. LSB insertion techniques are used to hide information at the edge areas whereas another LSB substitution technique is used to hide message at the smooth areas. Input cover image is divided into edge and smooth areas using transform. Based on the LSB insertion and adaptive LSB substitution techniques the messages are hiding at edge and smooth areas. The Proposed methods achieve the high eminence of the stego-image with direct accomplishment of the edge areas being high in contrast and frequency can tolerate more changes in their pixel values than smooth areas by comparing with the PSNR.

Introduction

Steganography is an art of hiding secret information into a multimedia data such as audio, video, image etc. The basic structure of Steganography is made up of three components: the "carrier", the message, and the key [3]. The carrier can be a image, a digital image, an mp3, even a TCP/IP packet among other things. It is the object that will 'carry' the hidden message. A key is used to decode or decipher or discover the hidden message [3]. The basic model shows the basic process involved in Steganography which consists of delivery service, information and Password. Carrier is also known as cover image, in which message is embedded and serves to hide the presence of the message [1]. The data can be any type of data such as plain text, cipher text or other image that the sender wishes to remain confidential. Code word or Password is known as stego-key, which ensures that only beneficiary who knows the corresponding decoding key will be able to extract the message from a cover image. The cover-image with the secretly embedded message is then called the stego-image [1]. Steganography is based on two steps. They are given below

a. Identification of redundant bits in cover object. Redundant bits are bits which can be modified without corrupting quality or destroying the integrity of cover image.

b. The embedding process then selects the subset of the redundant bits to be replaced with data from secret message. The stego image is created by replacing selected redundant bits with message bits [3].

Image steganography techniques can be classified into two categories. They are Spatial-domain or Image domain based steganography and frequency domain or Transform domain based steganography. In spatial domain method, the secret messages are embedded directly. The most common and simplest steganography method is the least significant bits (LSB) insertion method [1]. The other methods used in spatial domain method are Hiding Gray Images Using Blocks Method, Hiding Secret Message in Edges of the Images Method, Grey Level Modification Steganography Method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are modified before embedding. Transform domain techniques hide data in mathematical functions that are in compression algorithms [6].

Related Work

LSB (Least Significant Bit) Method

The majority steganography technique is to hide information by replacing only the least-significant bits (LSB) of an image with bits from the file that is to be hidden. This technique is commonly called as LSB encoding. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image [1].

Example is specified as follow as:
Pixels: (10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)
Secret message: 01000001

Result: (10101110 11101001 10101000)
(10100110 01011000 11101000)
(11011000 10000111 01011001)

The three bold bits are the only three bits that were actually altered. Since the 8-bit letter A only requires eight bytes to hide in ninth byte of the three pixels that can be used to begin hiding the next character of the hidden message. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte [1]. This increases the hidden information capacity of the cover image but the cover image is degraded more and therefore it is more noticeable [5].

Other variations on this technique include ensuring that arithmetic changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid color. While LSB insertion is easy to implement, it is also easily attacked. Slight modifications in the color palette and simple image manipulations will destroy the entire hidden message [5]. Some examples of these simple image manipulations include image resizing and cropping. Since the steganalysis of LSB method is easier. Therefore, it is suggested that the image should be first manipulated before the embedding of the message into it.

The Steganography algorithm for LSB is Non-filtering algorithm as shown in figure 1. This algorithm is the simplest method based in the use of LSB. The embedding process consists of the chronological replacement of each LSB of the image pixel for each bit of the message. This method can camouflage a great volume of information. It is obligatory only a chronological LSB reading starting from the first image pixel to extract the secret message. This method also generates a deranged distribution of the changed pixels, because the message is embedded at the first pixels of the image, departure unaffected the remaining pixels.

The carrier image is divided into non overlapping blocks of size 8×8 and applies DCT on each of blocks of cover image using forward DCT. Now perform Huffman encoding on the 2D secret image of size M2xN2, to convert it into 1D stream. Huffman code is decomposed in 8-bits blocks [1]. The least significant bit of all of the DCT coefficients inside 8×8 block is changed to a bit taken from each 8 bit block from left to right. Now, perform the inverse block DCT using inverse DCT and obtain a new image which contains secret image. At the receiver side, the stego-image is

received, which is in the spatial domain [2].

Solution Proposal
The new approaches for image steganography are based on LSB with the following steps and the original image or cover image is mentioned in figure 1.

LSB Technique at Edge areas
Image is represented as arrays of values which represent the intensity pixel values. Each and every pixel value is represented R as Most Significant Byte, then G and B are Least Significant byte. A LSB based steganography method introduces two components out of three components is based on visual perception of color image. Blue component is minimum, average for green component and maximum for Red color. Integrate maximum changes in Blue component and average changes in green color and less change in red color without making much difference in color image.

Figure 1. Cover image or Before Embedding secret message

Procedure for embedding data in Edge areas are mentioned below:

a. Extract all the pixels in the given image and store it in the pixel-array.
b. Extract all the characters in the given text file and store it in the character-array.
c. Extract all the characters form the stego key and store it in the key array.
d. Choose first pixel and pick characters from key-array and then place it in the eight bits of the first component.
e. Suppose we have more characters in key array then we place rest in the four bits of its second component and then to the next pixel and so on. Then we obtain the stego-image.

LSB Technique for smooth areas
In this technique variable numbers of LSBs are utilized for embedding secret message bits according to the algorithm. First of all every pixel value in this image are analyzed and then checking process is employed for all the three bytes. If the value of the pixel is in the range from 240 to 255, then we embed four bits of secret data into the LSBs of the pixel. If the value of pixel is 224 to 239 then we embed three bits of secret data into the three bits of secret data into the LSBs of the pixel. If the value of the pixel is ranges from 192 to 223 then we embed two bits of secret data into the two LSBs of the pixel. In other cases we embed one bit of data into one LSB of the pixel.

Procedures for embedding data in the smooth areas are given below:
a. Calculate the number of bits based on the techniques mentioned above.
b. Place the remaining characters from character into an available bit of a pixel array
c. These steps are repeated until we reach and end of a character array.

The stego image is mentioned in figure 2 after the data are embedded in the cover image.

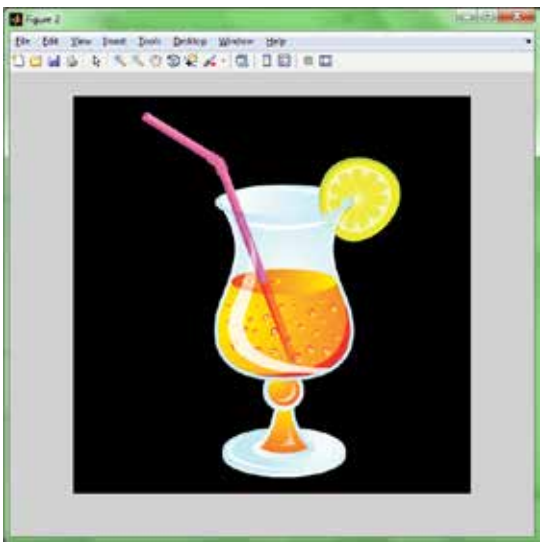


Figure 2. Stego-Image or After Embedding secret Message

Measures of Image Quality
Two measures are used they are MSE and PSNR. Peak Signal-to-Noise Ratio is often called as PSNR. It is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the dependability of its representation. PSNR is the most commonly used to measure the image quality. Mean Square Error is often called as MSE. MSE is used to quantify the difference between values implied by an estimator and the true values of that quantification are being estimated.

The MSE between two images such as $g(x,y)$ and $\bar{g}(x,y)$ is mentioned in equation (1)

$$e_{MSE} = \frac{1}{M} \sum_{n=1}^{M} \sum_{m=1}^{N} \left[\bar{g}(n,m) - g(n,m) \right] \cdots (1)$$

PSNR avoids the problem which occurs in MSE by scaling according to the image range is mentioned in equation (2)

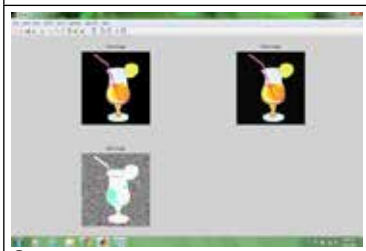
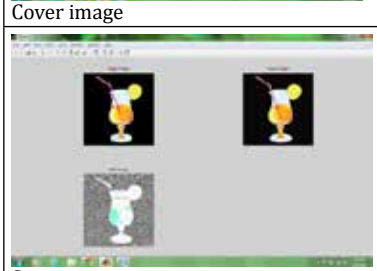
$$PSNR = -10 \log_{10} e_{MSE} / S^2 \cdots (2)$$

Here, S is the maximum pixel values. PSNR is measured in decibels (DB).The PSNR is a good measure for comparing restoration results for the same image.

Conclusion
In this paper a new approach of LSB steganography is proposed. In this two LSB techniques are used for to hide data in separate areas such as smooth areas and edge areas. This algorithm is not only to embed the secret message but also to predict the length of the secret message in color images. A new technique for information hiding presents an improved method for non-adjacent and random pixel location in edges of image and selected pixels in smooth images. Experimental results shows the evaluated the enhanced data hiding techniques by utilizing all pixel values with the PSNR values based on RGB are shown in TABLE I.

Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

TABLE I
Experimental Results for Cover image and Stego image

Image, Noisy image and Mse image	PSNR			MSE		
	(:,:,1)	(:,:,2)	(:,:,3)	(:,:,1)	(:,:,2)	(:,:,3)
 Cover image	32.5454	32.3877	32.4660	36.4702	37.8191	37.1434
 Stego image	32.5410	32.3691	32.4788	36.5071	37.9810	37.0339

REFERENCE

[1]"Study and Analysis of Various Image Steganography Techniques" Jagvinder Kaur, Sanjeev Kumar, Amritsar College of Engineering and Technology, Amritsar, India. IJCST Vol. 2, Issue 3, September 2011. | [2]"An Overview of Image Steganography" T. Morkel, J.H.P. Eloff , M.S. Olivier, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa. | [3]"Data Structures: Image Steganography" Nick Nabavian Nov. 28, 2007. | [4]"Evaluation of Various LSB based Methods of Image Steganography on GIF File Format" Namita Tiwari, Dr.Madhu Shandilya International Journal of Computer Applications (0975 – 8887) Volume 6– No.2, September 2010. | [5]"Improving the Steganographic Algorithm LSB". Juan José Roque, | Jesús María Minguet. Universidad Nacional de Education a Distancia. | [6] "Statistical Signal Processing", Ying Wang; Moulin, P,IEEE, 56(11) : 339 – 342, 2003. | [7] "A high capacity data-hiding scheme in LSB- based image stegnography" A Thesis Presented to The Graduate Faculty of The University of Akron In Partial Fulfillment of the Requirements for the Degree Master of Science Rajanikanth Reddy Koppola May, 2009. | | [8] "Feature Extraction on Images through a Mathematical Morphological Operation Using Watershed" G.S.Raman R.T.Subhalakshmi Associate Professor, Department, PG | Student, Department of Information Technology, KLN College of Information Technology, Sivagangai, India, IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) Volume 2, Issue 2 (Mar. – Apr. 2013), PP 10-14 e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197 | [9] "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format"Namita Tiwari Asst.Prof. Deptt.of computer science MITS, Gwalior,India Dr.Madhu Shandilya Professor,Deptt.of Electronics, MANIT Bhopal,India, International Journal of Computer Applications (0975 – 8887)Volume 6– No.2, September 2010 | [10]"Steganalysis of LSB Image Steganography using Multiple Regression and Auto Regressive (AR) Model "Souvik Bhattacharyya1 and Gautam Sanyal2 1Department of Computer Science and Engineering, University Institute of Technology The University of Burdwan, West Bengal, India, e-mail: (souvik.bha@gmail.com) 2Department of Computer Science and Engineering, National Institute of Technologyy West Bengal,India, e-mail: (nitgsanyal@gmail.com) Souvik Bhattacharyya et al, Int. J. Comp. Tech. Appl., Vol 2 (4), 1069-1077 | [11]"Detection of LSB Matching Steganography in Decompressed Images" Jun Zhang and Dan Zhang IEEE SIGNAL PROCESSING LETTERS, VOL. 17, NO. 2, FEBRUARY 2010 |