International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 4, ISSN (Online) 2249 –071X, ISSN (Print): 2278 – 4209

Secure and Efficient Image Hiding Method and Model for Digital Content Access Control

Kirandeep Saini
M.Tech. (C.S.E)
Guru Nanak Dev Engineering College, Ludhiana
kirandeep.saini@gmail.com

***Abstract* — This paper introduces a best approach for Least Significant Bit (LSB) based on image steganography that enhances the existing LSB substitution techniques to improve the security level of hidden information. It is a new approach to substitute LSB of RGB true color image. The new security conception hides secret information within the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users. In LSB methods, hidden information is stored into a specific position of LSB of image depending on the secret key. We have used the Peak Signal to Noise Ratio (PSNR) to measure the quality of the stego images. The obtained results show that the proposed method results in LSB based image steganography using secret key which provides good security issue and PSNR value than general LSB based image steganography methods.**

***Keywords* — cover-image, steganography, stego-image, LSB.**

I. INTRODUCTION

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography derived from Greek, literally means "covered writing." It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spycraft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not.

In the past, people used hidden tattoos or invisible ink to uncover steganographic content. Today, computer and network technologies provide easy to use communication channels for steganography. But privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly. Steganography is a technique to hide information from the observer to establish an invisible communication. Generally a steganographic system consists of cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message. To hide hidden information, steganography gives a large opportunity in such a way that someone cannot know the presence of the hidden message. The goal of modem steganography is to keep its information undetectable.

Generally secret information is stored into the specific position of Least Significant Bit (LSB) of a cover image which is the carrier to embed messages. Anyone can ensure that the specific position of LSB contains secret information. So it is easy to recover the secret information for anyone by using retrieval method. The main intention of image steganography is to ensure security of hidden information. For security purpose, we have introduced a new approach of LSB based image steganography. Here we are adding a secret key which ensure the security of hidden information. The insertion of hidden information is totally controlled by the secret key. This secret key decides the appropriate position of hidden information. It is very difficult to retrieve the hidden information without the same secret key. So by using a secret key, we can increase the security level of the hidden information in LSB based image steganography.

We know that in every image, there are pixels. Each pixel contains three bytes named as Red, Green and Blue channel. The best approach for Least Significant Bit (LSB) based on image steganography that enhances the existing LSB substitution techniques to improve the security level of hidden information. It is a new approach to substitute LSB of RGB true color image. The new security conception hides secret information within the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users. In LSB methods, hidden information is stored into a specific position of LSB of image depending on the secret key. We have used the Peak Signal to Noise Ratio (PSNR) to measure the quality of the stego images. The obtained results show that the proposed method results in LSB based image steganography using secret key which provides good security issue and PSNR value than general LSB based image steganography methods. Here we proposed an efficient LSB based steganographic method that utilizes the secret key to hide the information into an input pixel of cover image without producing perceptible distortions. Here a bit of hidden information is placed in either LSB of Green or Blue matrix of a specific pixel which is decided by the secret key. So anyone cannot exactly make a decision that the bit of hidden information is placed in either LSB of Green or Blue matrix. As a result, the security level of image steganography is attained.

A. Image Files

The simplest approach to hiding data within an image is called least significant bit (LSB) insertion. For 24-bit true color image, the amount of changes will be minimal and

indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Now suppose we want to hide the following 9 bits of data **101101101**. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed) pixels:

10010101	00001100	11001001
10010111	00001110	11001011
10011111	00010000	11001011

The following formula provides a very generic description of the pieces of the steganographic process:

cover image + hidden information = stego image

In this perspective, the cover image is the main image in which the *hidden information* will be embedded. The resultant image is the stego image (which will, of course be the same type of image as the cover image).

To measure the quality of stego image, Peak Signal-to-Noise Ratio (PSNR) is calculated. PSNR is a statistical measurement used for digital image or video quality assessment. PSNR is most easily defined via the mean squared error (MSE) which for two $m \times n$ monochrome images I *and* K where one of the images is considered a noisy approximation of the other is defined as:

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$\text{PSNR} = 10.\log_{10}\frac{MAX_1^2}{MSE} = 20.\log_{10}\frac{MAX_1}{\sqrt{MSE}}$$

Larger PSNR indicates better quality of the image or in other terms lower distortion. The larger the PSNR value the smaller the possibility of visual attack by human eye.

B. File Compression

Two kinds of compression are lossless and lossy. Both methods save storage space but have different results, interfering with the hidden information, when the information is uncompressed. Lossless compression lets us reconstruct the original message exactly; therefore, it is preferred when the original information must remain intact (as with steganographic images). Lossless compression is typical of images saved as GIF (Graphic Interchange Format) and 8-bit BMP (a Microsoft Windows and OS/2 bitmap file). Lossy compression, on the other hand, saves space but may not maintain the original image's integrity. This method typifies images saved as JPEG (Joint Photographic Experts Group). Due to the lossy compression algorithm, which we discuss later, the JPEG formats provide close approximations to high-quality digital photographs but not an exact duplicate. Hence the term "lossy" compression.

C. Embedding Data

Embedding data, which is to be hidden, into an image requires two files. The first is the innocent-looking image that will hold the hidden information, called the *cover image*. The second file is the message-the information to be hidden. A message may be plain text, ciphertext, other images, or anything that can be embedded in a bit stream. When combined, the cover image and the embedded message make a *stego image*. A stego-key (a type of password) may also be used to hide, then later decode, the message.

Most steganography software neither supports nor recommends using JPEG images, but recommends instead the use of lossless 24-bit images such as BMP. The next-best alternative to 24-bit images is 256-color or gray-scale images. The most common of these found on the Internet are GIF files.

In 8-bit color images such as GIF files, each pixel is represented as a single byte, and each pixel merely points to a color index table (a palette) with 256 possible colors. The pixel's value, then, is between 0 and 255. The software simply paints the indicated color on the screen at the selected pixel position.

II. PROPOSED METHODS

We know that in every image, there are pixels. Each pixel contains three bytes named as Red, Green and Blue channel. The algorithm uses mapping method for data hiding and LSB method for indication that data is hidden here.

The basic concept is to convert secret message into ASCII code. As ASCII code is a 7 bit code. So for matching bits every byte only 7 MSBs of each channel will be used and the LSB of all the three channels are free to work as a indicator. In this paper, we have taken the binary representation of the hidden information and overwrite the LSB of each byte within the cover image. Here we have introduced a secret key to protect the hidden information. The following formula, we have used in our proposed method is:

cover image + secret key + hidden information = Stego images

We implement the main algorithm (mapping method and LSB method) on Matlab tool using following steps:

1) Read cover image, convert it into three channels R, G, B.
2) Read secret message, convert it into ASCII code, store in variable C.
3) Extract message length and store it into variable L.
4) Hide message length into the first row of cover image, inside blue channel only, by using LSB method.
5) Start from second row of cover image. Take first pixel of second row.
6) Take next character from C.

7) Select indicator channel pair, depending upon the pseudo random number.
8) Match the character with 7 MSBs of red channel of pixel.
9) If there is a match-between character bit sequence and 7 bits of red channel, then set LSB of indicator channel1 and indicator channel2 equal to 0.
10) Set L= L-1. Go to step no. 18.
11) If not matched, then Match the character with 7 MSBs of green channel of pixel.
12) If there is match between character bit sequence and 7 bits of green channel, then set LSB of indicator channel1= 0 and indicator channel2= 0.
13) Set L = L-1. Go to step no. 18.
14) If not matched, then match the character with 7 MSBs of blue channel of pixel.
15) If there is match between character bit sequence and 7 bits of blue channel, then set LSB of indicator channel1= 1 and indicator channel2= 0.
16) Set L= L-1. Go to step no. 18.
17) If character does not match with any channel of this pixel, then set LSB of indicator channel1 =1 and indicator channel2=1. Go to next pixel and go to step no. 7.
18) Go to next pixel.
19) Check if L>0. If yes go to step no. 6.
20) Stop when all characters are consumed and L is equal to zero.

III. Experimental Result and Discussion

Experimental results are given in this section to demonstrate the performance of our proposed method. We used some standard ROB (true color) images as the cover image. Small size image is used as the hidden information.

A. Encoder

In this we just need to read image by using imread function. Than simply break into three blocks named Red, Green and Blue. Check or read text file and convert it into ASCII codes. Now check by loop whether first character's ASCII codes. If found than note address or message location in index file and again move to next character and if not found in three of matrices of red, green and blue than you can do it by using protocol by adding special character null to your index file and next to this as such ASCII code of your character. If character found in red matrix than before saving location in index file just save special character value 1 to show that it's from red matrices. And if in green than 2 and if in third that is green than 3 if not found only than 0 and then character code. Than repeat last step for complete message and then found mean of index and mean to same index after dividing index address and save index file named index.mat. and send this file to decoder. Figure 1 show the encoded image and original image.

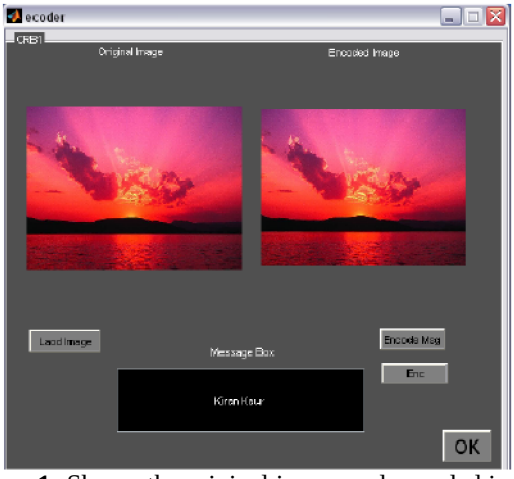

Figure 1: Shown the original image and encoded image

B. Decoder

Read index file and get mean from last of index file. Now multiple mean with its element of index array. After that read same image file that was used for encoding and extract three different arrays named Red, Green and Blue. Now search take a message named string with initial empty string. Now look for index array value and look for address values and check whether it's 1, 2, 3 or 0.

a) If 1 than use next index address to read from red matrices.
b) If 2 than use next index address to read from green matrices.
c) If 3 than use next index address to read from blue matrices.
d) If 0 than use next index address to directly as character.

Read up to last or mean value of index array. Figure 2 show the decoded image.

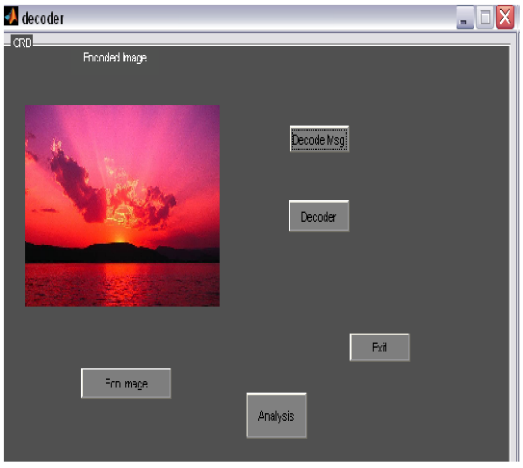

Fig.2. Decoded image

Figure 3 and 4 show the peak signal to noise ratio (PSNR) and histogram of encoded image 1 and image 2.

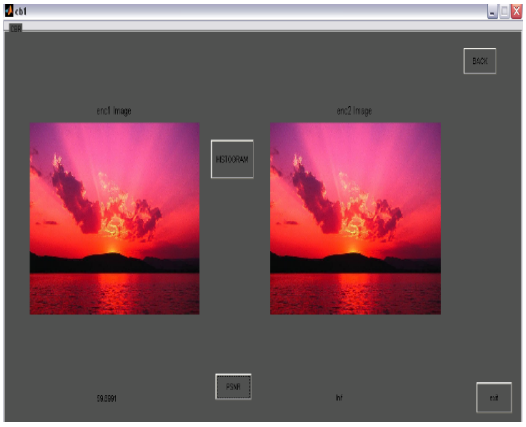

Fig.3. Peak signal to noise ratio (PSNR).

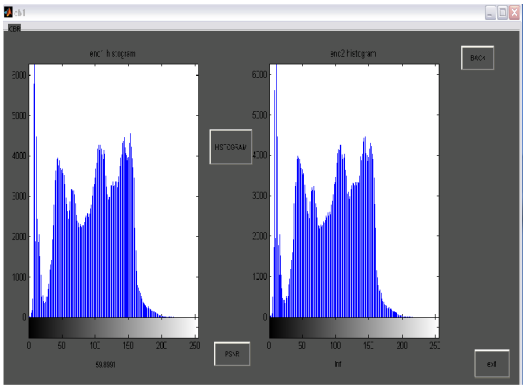

Fig.4. Histogram of enc image 1 and enc image 2

IV. CONCLUSION

The experimental results show that the proposed method is an effective way to integrate hidden information reporting without significant distortion. And it is very difficult for the unauthorized users to identify the changes in stego image. The use of the secret key gives a way to secure the information from illegal user. It used a secret key to hide hidden information into cover image. This process provides a new dimension for image steganography. It is very difficult to recover the hidden information for third party without knowing the secret key. This method provides better PSNR value where larger PSNR indicates better quality of the image or in other terms lower distortion.

REFERENCES

[1] M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation", Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.

[2] Mohammed F. Al-Hunaity et al. "Colored Digital Image Watermarking using the Wavelet Technique" American Journal of Applied Sciences (2007)658-662.

[3] Chiang-Lung Liu and Shiang-Rong Liao. 'High-performance JPEG steganography using complementary embedding strategy'. 2008 Elsevier Ltd All rights reserved, 2945-2955.

[4] Evelyn Brannock et al. 'Watermarking with Wavelets: Simplicity Leads to Robustness'.2008 IEEE, 587-592.

[5] Harmsen J and Pearlman W A, " Steganalysis of additive noise modelable information hiding," Proc. Of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents VI. SanJose, CA, 2003: 131-142.

[6] Ker A D, "Steganalysis of LSB Matching in Grayscale Images," IEEE Signal Processing Letters, vol. 12, no. 6, pp. 441-444, June 2005.

[7] Q.Tang P.Lu, X.Luo and L.Shen, "An improved sample pairs method for detection of LSB embedding," vol. 3200, pp.116 –27, 2004.

[8] R. J. Anderson and F.A.P Petitcolas, "On the limits of steganography," IEEE Journal of Selected Areas in Communications,(Special issue on copyright and privacy protection), vol. 16, 1998.

[9] R. Du J. Fridrich and L. Meng, "Steganalysis of lsb encoding in color images," Proceedings of IEEE International conference on Multimedia and Expo New York City, NY, Jul 30 - Aug2, 2000.

[10] Z. Tao and P. Xijian, "Reliable detection of lsb steganography based on the difference image histogram," Proc. IEEE ICAAP, Part III, pp. 545–548, 2003.

AUTHOR'S PROFILE

Kirandeep Saini
M.Tech. (C.S.E)
Guru Nanak Dev Engineering College, Ludhiana
kirandeep.saini@gmail.com