International Journal For Technological Research In Engineering
Volume 3, Issue 12, August-2016 *ISSN (Online): 2347 - 4718*

STUDY OF STEGANOGRAPHY INFORMATION HIDING IN IMAGE USING VARIABLE BIT INSERTION BASED ON PIXEL DIFFERENCE

Nirmala Yadav[1], Chetna[2]
[1]M.Tech (CSE), [2]Assistant Professor, Department of CSE, MRKIET(Rewari)

Abstract: Steganography is the science of "invisible" communication. The purpose of Steganography is to maintain secret communication between two parties. In this paper we have study and compared two techniques of data hiding in image. Two steganographic techniques based on LSB and PVD are implemented in using MATLAB software. In first method information is hidden in LSB of image. In second method information is inserted in last 2-3 bits of image pixel based on difference of neighbor pixels. Second method gives better results regarding security and capacity. It also avoids abrupt changes in the image during data embedding procedure. The proposed method achieves higher embedding capacity, imperceptibility and can be used for both gray scale and colour image than LSB with security key. Also with same capacity it gives security to basic PVD method. The embedded confidential information can be obtained properly from the stego-image without the assistance of the host-image.

Keywords: Least significant Bit(LSB), steganography , MSE, PSNR, Cryptography

I. INTRODUCTION

Now days the rise of the Internet, security of information became one of the most important factors of communication and information technology. With increasing number of Internet users, the concept of Internet security also became more important. Everyday a lot of data is transferred over internet through various ways like, e-mail, audio-video sharing sites, file sharing sites, social networking sites etc. So to transmit information securely various encryption and hiding methods have been developed. As the number of Internet users is increasing, the concept of Information security has also gaining importance. In the current world, most of the business is based on online selection and transaction over "INTERNET". So most important concerns for network and information are Necessity of data security, so that no other unauthentic person can access it illegally and Transfer of data over internet accurately without errors control. Encryption provides an obvious approach to information security, and encryption programs are readily available. However, encryption clearly marks a message as containing "interesting" information, and the encrypted message becomes subject to attack. Furthermore, in many cases it is desirable to send information without anyone even noticing that information has been sent. The word steganography comes from the Greek Steganos, which mean covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing.

The main goal or steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [16].Cryptography and steganography are associated to each other. The most important difference between cryptography and steganography is that cryptography scrambles the message so that it becomes difficult to understand whereas steganography hides the very existence of a message. Steganography plays the central role in secret message communication. Several message hiding techniques have been developed and implemented in the past using digital images, audio/video files and other media. [17]The main terminologies used in the steganography systems are: the cover message, secret message, secret key and embedding algorithm. Image, video, audio, text, protocol are used by the encrypting algorithm to send the secret message. The secret message is the data which is wanted to be hidden in the suitable furtive digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to encrypt the secret data in the stego image.

II. DATA HIDDING USING LSB INSERTION

This method is implementation of LSB method given by S. M. M. Karim, M. S. Rahman and M. I. Hossain in "A New Approach for LSB Based Image Steganography using Secret Key" [11]. It improves the present LSB insertion methods to increase the security level of hidden message. It is a new way to replace LSB of a RGB true color image. The new security idea hides secret information within the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users. [11] In general, in LSB methods, hidden message is stored into a specific position of LSB of image. For this reason, knowing the retrieval methods, anyone can extract the hidden information.Here hidden information is stored into different position of LSB of image depending on the secret key. The insertion of hidden information is totally controlled by the secret key. As a result, it is difficult to extract the hidden information knowing the retrieval methods.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. The following formula is used in this method.

Cover image + secret key + hidden information = Stego image.

A. Data Hiding Procedure

In this method a RGB image is taken as cover image. This image is divided into three matrixes (for Red, Green and Blue). Message data (text or image or any bit convertible file) is converted as a 1-D bit stream (figure 1). A secret password is used to protect this information. ASCII values of password are calculated and then it is converted in a continuous bit stream. Red matrix and password bits give the information about embedding bit position.

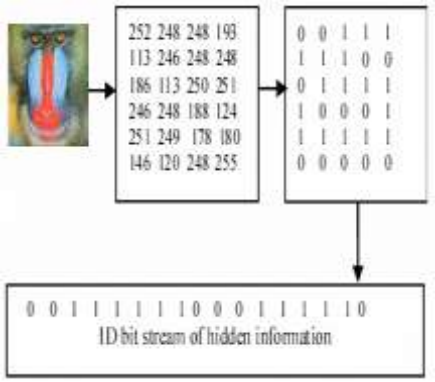


Figure 1 1D array representation of hidden information

Each bit of secret key is XOR with each LSB of Red matrix. The resulting XOR value decides that the 1 bit of hidden information will be placed with either LSB of Green matrix or Blue matrix. The same process will be continued until the hidden information is finished. The procedure to hide hidden information into cover image is shown in Fig. 2. Information about size of message data is inserted in last 100 bytes of cover file same as data insertion in the message file.

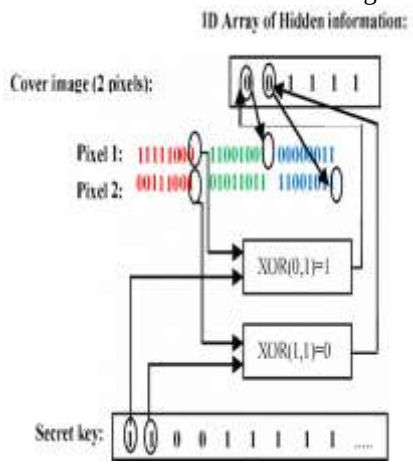


Figure 2 Process of data hiding

B. Data Extraction Procedure

The extraction process is just inverse process of data imbedding. Stego file is having information of both cover file and message data. Stego file is divided in RGB colour matrixes. Now secret key or password that was used for encryption is used again. Password is converted into ASCII codes and then a continuous bit stream. Now first last 100 bytes of stego file are extracted in order to get message file dimensions. Then each LSB of Red matrix is XOR with a bit of secret bit and as per result LSB of Green or Blue matrix is extracted. This bit is inserted in a continuous bit stream. Then again binary stream is converted into 8 bit data matrix with dimension as extracted from last 100 bytes. In case the password is not same as the one used for encryption the size as well as the data extracted will be corrupt.The process of data extraction is as shown in figure 3. If dimensions of message file are not extracted correctly the message will contain false entries and so the information will not be visible.

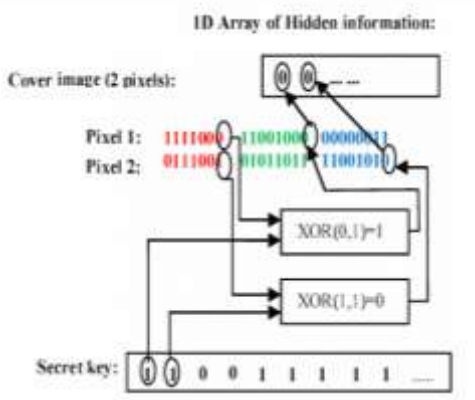


Figure 3 Process to recover hidden information from stego image

c. Data Hiding

In this method, grey level difference near target pixel is used to determine data embedding capacity of that pixel. If pixel is in edge area more bits can be embedded than smooth area. Once the embedding capacity is determined, data can be inserted as simple as LSB method. In this method capacity of each pixel is determined by Pixel value difference method. Then password is used to hide data. If password character ASCII value is even, data is inserted directly. Otherwise inverted data is inserted into the pixel. Thus somewhere data is inserted inverted and at other places it is hidden directly. Without knowledge of secret key if data is extracted then it is not of any use. Other main point is that size of embedded bit is unknown without key. So with wrong key, the message can't reshape. For a message as image, extracted file will have some random dimensions which make it useless.

The data embedding process is as following:

1. Read cover image and create RGB matrixes. Insert secret key and convert it into bit stream.
2. Determine gray level variation near target pixel and thus determine capacity of that pixel say 'n'.
3. If password character has even ASCII value, 'n' bits of message data are embedded in cover pixel. Otherwise data is inverted before embedding.
4. A step 3 is repeated till whole data is embedded.
5. Then Size of message file is embedded into last 100 bytes using same procedure.
6. Data is written in form of image file to obtain stego-image.

D. Data Extraction Process

For reconstruction of message file two things are required. First is all embedded data and second is the size of file. Data is protected with password but it is not same as combining

cryptography and steganography. In that case data is first encrypted and then embedded. Here data is embedded and encrypted simultaneously. Thus even if someone is able to collect all embedded data, he need cover file to reconstruct it. So any modification in image will make it unrecoverable. Thus any kind of unauthorized tricks applied on image will make it blocked.

Extraction of data can be done as follow:

1. Open stego file and divide it in RGB matrixes.
2. Enter password and convert it into 1D bit stream.
3. Extract last 100 bytes of stego image to get message file sizs.
4. Calculate capacity of stego pixels.
5. Now extract last 'n' bits of stego pixel as message data.
6. If password character has even ASCII value insert data to message bit stream directly, else invert data first and then insert to bit stream.
7. Repeat steps 4-7 till full size of message data is obtained.
8. Now reshape message data.

III. DATA HIDDING USING VARIABLE BIT INSERTION BASED ON PVD

Human visual system is more sensitive to the alteration in plane or smooth areas of a image. Thus embedding data in smooth area may cause detection of steganography. On other hand variation in edges of image where gradual changes are present, doesn't attract any attention. This is the main principle behind PVD Steganography. In LSB, each byte of cover file can hide one bit of message in it. If two or three bits are inserted in a byte, there is a chance of detection at smoother areas. On other hand, in PVD edge areas are detected in order to insert more bits in a single byte and less bits in smooth area. So capacity is increased without compromising invisibility of message data[13].While LSB steganography method is very secure to unauthorized access, it gives a very low embedding capability, which is 1 bit par 3 byte. But without password it is almost impossible to recover hidden message. On other hand PVD method gives very good embedding capability, in between 1-3 bits par byte. This is more than 3 times to LSB method. But if any third person knows the embedding process, he can easily recover message. By combining both techniques a secure as well as high capacity stego system can be achieved.

A. Data Hiding

In this method, grey level difference near target pixel is used to determine data embedding capacity of that pixel. If pixel is in edge area more bits can be embedded than smooth area. Once the embedding capacity is determined, data can be inserted as simple as LSB method. In this method capacity of each pixel is determined by Pixel value difference method. Then password is used to hide data. If password character ASCII value is even, data is inserted directly. Otherwise inverted data is inserted into the pixel. Thus somewhere data is inserted inverted and at other places it is hidden directly. Without knowledge of secret key if data is extracted then it is not of any use. Other main point is that size of embedded bit is unknown without key. So with wrong key, the message can't reshape. For a message as image, extracted file will have some random dimensions which make it useless.

The data embedding process is as following:

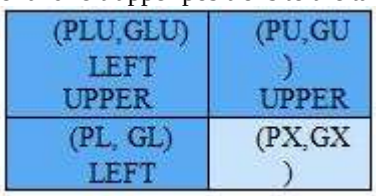
1. Read cover image and create RGB matrixes. Insert secret key and convert it into bit stream.
2. Determine gray level variation near target pixel and thus determine capacity of that pixel say 'n'.
3. If password character has even ASCII value, 'n' bits of message data are embedded in cover pixel. Otherwise data is inverted before embedding.
4. A step 3 is repeated till whole data is embedded.
5. Then Size of message file is embedded into last 100 bytes using same procedure.
6. Data is written in form of image file to obtain stego-image.

Secret key or password was taken same as the cover file name, i.e.

Data embedding Capacity:

Capacity of a pixel can be determined as follow [12][13]:

- First row and column of cover image are not used for insertion. Target pixel is selected starting from position (2, 2).
- Find gray level G of a pixel at position P for left, upper and left upper positions to the target pixel P_X.



Now difference of maximum and minimum gray level is determined as[1]

Gmax = Max(GL, GU, GLU);
Gmin = Min(GL, GU, GLU);
Difference d = Gmax – Gmin;

Embedding capacity 'n' is calculated as:

n = 4 ; d >15
= $\log_2(d)$; 1<d<16
= 1 ; d < 2

Data embedding capacity is restricted to 4; over this, cover image quality may degrade. In smooth areas where variation in colour is negligible, two bits are inserted. In edge area this can go to 1-4 bits in a byte.For a RGB image this process is applied independently on each colour matrix. Variation in gray level is more significant than colours, so capacity of gray scale image is higher than RGB image for same size.

B. Optimum Pixel Adjustment Procedure

To improve image quality OPAP can be applied to stego image. For n bits insertion in a pixel; if difference in original pixel and stego pixel is in b/w $|2^{n-1}$ to $2^n|$ then OPAP restrict this difference to $|2^{n-1}|$. If cover pixel has gray level R and stego pixel has gray level R',Then new gray level R" will be

R"= R' – 2^n if 2^{n-1}<R' - R< 2^n; R'> 2^n
=R' + 2^n if -2^{n-1}>R' –R>-2^n; R'< 256 - 2^n
=R' else

Thus quality of stego image is improved.

C. Data Extraction Process

For reconstruction of message file two things are required. First is all embedded data and second is the size of file. Data is protected with password but it is not same as combining cryptography and steganography. In that case data is first encrypted and then embedded. Here data is embedded and encrypted simultaneously. Thus even if someone is able to collect all embedded data, he need cover file to reconstruct it. So any modification in image will make it unrecoverable. Thus any kind of unauthorized tricks applied on image will make it blocked.

Extraction of data can be done as follow:

1. Open stego file and divide it in RGB matrixes.
2. Enter password and convert it into 1D bit stream.
3. Extract last 100 bytes of stego image to get message file sizs.
4. Calculate capacity of stego pixels.
5. Now extract last 'n' bits of stego pixel as message data.
6. If password character has even ASCII value insert data to message bit stream directly, else invert data first and then insert to bit stream.
7. Repeat steps 4-7 till full size of message data is obtained.
8. Now reshape message data.

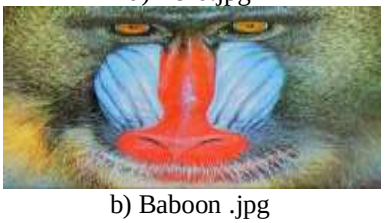
IV. EXPERIMENAL RESULT

Two steganographic techniques based on LSB and PVD are implemented using MATLAB software. In first method information is hidden in LSB of image. In second method information is inserted in last 2-3 bits of image pixel based on difference of neighbor pixels.

Experimental results are demonstrated using some standard RGB images of dimension 255x255.

Stego image is obtained by adding message file to cover file. Password is used to encrypt the process. As jpg/jpeg is a compressed file format some data may get corrupt while writing stego file, so stego images are saved with PNG extension. If jpg files are to be used then while writing the file, lossless compression should be used. Stego images corresponding to cover images are as shown in figure 4. They look similar and are imperceptible to human eyes.

a) Lena.jpg



b) Baboon .jpg

c) Pepper.jpg

Figure 4 Original Cover images (255x255)

When data is extracted from these stego file, it recovers the message file same as original file only if correct password is provided. If secret key or password provided is wrong then it recovers some irrelevant images. This file may have random dimension with no pattern or colour combination. Same image will produce different image pattern with different passwords. They may have size variation, colour variation etc.

Comparison Result

We can say by seeing results of above two methods that cover image and stego images look alike. We can't differentiate them on visual basis. But all of them are having some differences. So to distinguish there quality wrt cover image PSNR is used.

A. Peak Signal to Noise Ratio

We can say by seeing results of above two methods that cover image and stego images look alike. We can't differentiate them on visual basis. But all of them are having some differences. So to distinguish there quality wrt cover image PSNR is used. PSNR or peak signal to noise ratio is a measure to the image quality. It compares mean square error of stego image with peak signal modification. MSE is the easiest way to calculate PSNR.MSE can be calculated as,

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

Here m and n are no. of rows and columns respectively. L is the stego image pixel while K is the pixel of original image. The PSNR is defined as:

$$PSNR = 10.\log_{10}\left(\frac{{MAX_1}^2}{MSE}\right) = 20.\log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right)$$

Table I. Peak Signal to Noise Ratio

Cover image	LSB PSNR (dB)	PVD method
Lena.jpg	49.7618	47.5925
Baboon.jpg	48.1558	45.8689
Pepper.jpg	48.7869	46.8673

B. Comparison of capacity LSB With PVD.

Second important term required to compare these methods is payload capacity. Method that can achieve higher payload capacity is better. Third term is security. A more secured system is required to keep the data private.

Table II. Capacity omparison of LSB With PVD.

Cover image	LSB Capacity	PVD method
Lena.jpg	196608	391135
Baboon.jpg	196608	464904

Pepper.jpg	196608	407147

V. CONCLUSION

In this paper we have studied about Steganography and comparison of two techniques of data hiding in image. Second method gives better results regarding security and capacity. It also avoids abrupt changes in the image during data embedding procedure. The PVD method achieves higher embedding capacity, imperceptibility and can be used for both gray scale and colour image than LSB with security key.

REFERENCES

[1] N. F. Johnson and S. Jajodia, "Exploring steganography, seeing the unseen," IEEE Computer Magazine, vol. 31, no. 2, pp. 26-34, February, 1998.
[2] K. Curran and K. Bailey, "An evaluation of image based steganography methods," International Journal of Digital Evidence, vol. 2, no. 2, pp. 1-40, Fall, 2003.
[3] N. F. Johnson, Z. Duric, and S. Jajodia, "Information hiding, and watermarking - attacks & countermeasures," Journal of Electronic Imaging, vol. 10, no. 3, pp. 825-826, 2000.
[4] C. S. Lu, "Steganography and digital water marking techniques for protection of intellectual property," in Multimedia Security, Idea Group Publishing, Singapore, 2005, pp. 75-157.
[5] R. H. Alwan, F. J. Kadhim, and A. T. A. Taani, "Data embedding based on better use of bits in image pixels," International Journal of Signal Processing, vol. 2, no.1, pp. 104-107, 2005.
[6] N. Wu and M. Hwang, "Data hiding: current status and key issues," International Journal of Network Security, vol. 4, no. 1, pp. 1-9, 2007.
[7] L. M. Marvel and C. T. Retter, "The use of side information in image steganography," presented at IEEE International Symposium on Information Theory and Its Applications, Honolulu, Hawaii, USA, November 5-8, 2000.
[8] W. Luo, "Object-related illustration watermarks in cartoon images," Master"s Thesis, Department of Simulation and Graphics, Otto-vonGuericke University Magdeburg, Germany, February 2004.
[9] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," IEEE MultiMedia, vol. 8, no. 4, pp. 22-28, October 2001.
[10] M. Juneja and P. S. Sandhu, "Performance evaluation of edge detection techniques for images in spatial domain," International Journal of Computer Theory and Engineering, vol. 1, no. 5, pp. 614-621,December 2009.
[11] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain. "A New Approach for LSB Based Image Steganography using Secret Key." IEEE 14th International Conference on Computer and Information Technology (ICCIT 2011) pp.286-291,2011
[12] Han-ling ZHANG, Guang-zhi GENG, Cai-qiong Xiong, "Image Steganography using Pixel-Value Differencing", Second International Symposium on Electronic Commerce and Security, pp- 109 - 112, 2009.
[13] Ankita Sancheti, "Pixel value differencing image steganography using secret key". International Journal of Innovative Technology and Exploring Engineering. Volume-2, Issue-1, December 2012.
[14] Ali K. Hmood, B.B. Zaidan, A.A. Zaidan and Hamid A. Jalab, 2010. An Overview on Hiding Information Technique in Images. Journal of Applied Sciences, 10: 2094-2100.
[15] A. Joseph Raphael, Dr. V Sundaram, "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3),pp.626-630,2011
[16] B B Zaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15): 1650-1655, 2010.
[17] Mamta Juneja and Parvinder S. Sandhu, "An Improved LSB Based Steganography Technique forRGB Color Images" International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013.
[18] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An overview of image Steganography."
[19] Komal Patel, Sumit Utareja, Hitesh Gupta. "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Applications, Volume 63– No.13, February 2013.
[20] Gandharba Swain, Saroj Kumar Lanka. "A Quick review of Network Security and Steganography" International Journal of Electronics and Computer Science Engineering, ISSN-2277-1956/V1N2-426-435, 2011.
[21] J. K. Mandal and Debashis Das. "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow." David C. Wyld, et al. (Eds): CCSEA, SEA, Cloud, DKMP, CS & IT 05, pp. 93–102, 2012.
[22] K.Yugala, "Steganography", International Journal of Engineering Trends and Technology (IJETT) Volume 4 Issue 5,pp 1629–1635, May 2013

