www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 9912-9915

An Improved Steganography Technique of LSB Substitution Method

[1]Neha Jain, [2]Sudhir Goswami
Computer Sci. & Engg Deptt. ACET,
Baghpat, India
neha.miet@gmail.com

Computer Sci. & Engg Deptt. MIET,
Meerut, India
sudhirgoswami.miet@gmail.com

Abstract: In this paper we have discussed the art and science of Steganography in general and proposed an algorithm which is the variant of LSB substitution method. It efficiently and effectively hides data with the help of a key in JPEG colored digital image. Security of hidden data is proportional to the length of key used. Proposed algorithm is capable to hide more data in cover image as compared to the many existing algorithm and require no pre-processing. Successful implementation of this algorithm opens the track for proposed algorithm to be used in data hiding and secure transmission

.

Keywords: Steganography, LSB substitution

I. Introduction

The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". Steganography is one such pro-security innovation in which secret data is embedded in a cover [1]. The notion of data hiding or steganography was first introduced with the example of prisoners' secret message by Simmons in 1983.There are many techniques which are used to hide the data in different formats. Most general one is the **Least Significant Bit (LSB)** substitution method, which is commonly used due to its simplicity. It provides protection to data by hiding it in digital image. But simple use of this approach is more vulnerable to attack [2]. The least significant bit (LSB) embedding method is one of the most commonly used techniques; it targets the LSB's of the host image to hide the data.

Now a days, maintain the security of the secret information has been a great challenge. Sender can send messages habitually through a communication channel like Internet, draws the attention of third parties, hackers and crackers, perhaps causing attempts to break and expose the unusual messages. Steganography is a promising region which is used for secured data transmission over any public media. Substantial amount of research work has been accepted by different researchers on steganography [3]. One of the best-known steganographic methods is the least significant-bit (LSB) substitution. The simple LSB substitution method replaces the length-fixed LSB with the fixed length bits. Although the technique is efficient, it is rather easy to create a noticeable distortion for the human eye or can be detected by some program. Therefore, several adaptive methods have been proposed for steganography in order to decrease the distortion caused by the LSB substitution [4] [5].

II. Proposed Algorithm

The steps of proposed algorithm are as follow:

1. Input a 24-bit color image having JPG format.
2. Divide the columns of the input image in to sets of size 3 as shown in following figure:

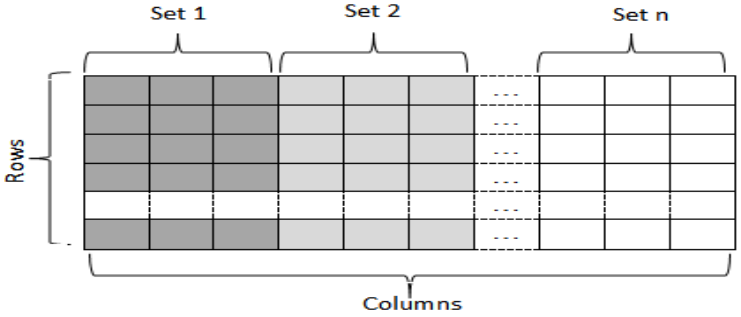


Fig. 1(a): Cover Image in 2-D View

3. Number the pixels of a set in the following manner in RGB plane :

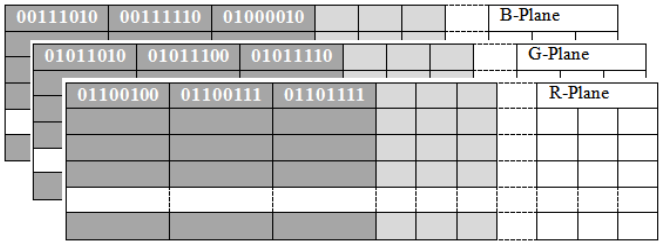


Fig. 1(b): Cover Image in 3-D View

4. ow input the secret message and key which is used to hide the message in the input image.
5. If the secret message has the first character 'A' and key used to hide this message has the first value '4' then this character is hided in the set 1 of the input image as follow:

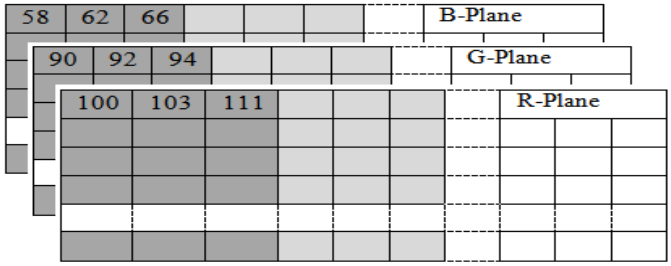


Fig. 1(c): 9-(decimal) values in set 1 Of Cover Image

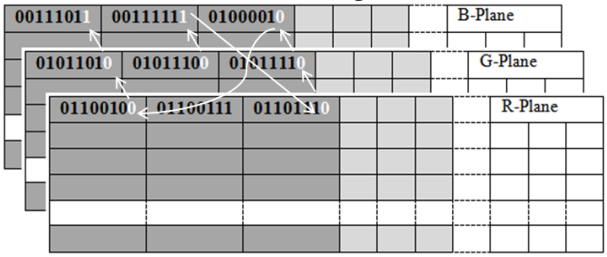


Fig. 1(d): 9-(binary) values in set 1 of Cover Image

Hiding of character 'A' (01000001) in set 1 of RGB plane is performed in the following manner:

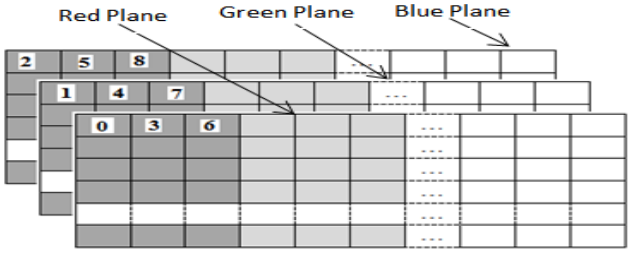


Fig. 1(e): Hiding of character 'A' (01000001) in stego image

6. Similarly next character of the message is hided with the next value of the key field. Key values are chosen in the circular way to hide the complete message.

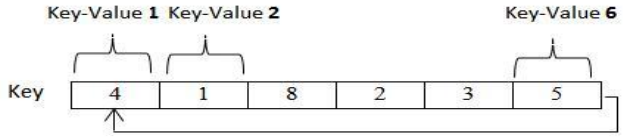


Fig. 1(f): Key-value of key is accessed clockwise in a circular way

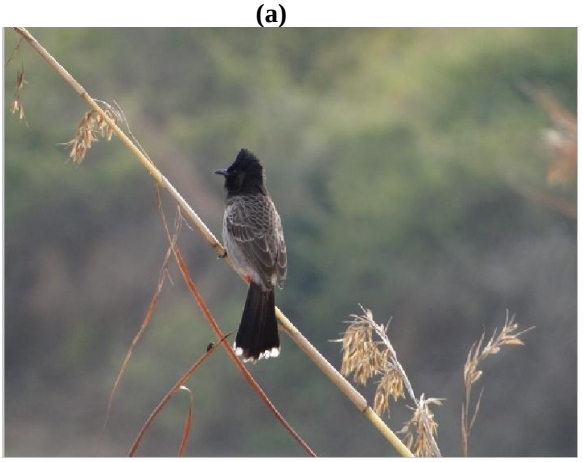
III. Result Analysis

The first step in steganography is that to embed and hiding information is to pass both the secret message and the cover message in to the encoder, inside the encoder, one or several protocols will be implemented to embed the secret information into the cover message.

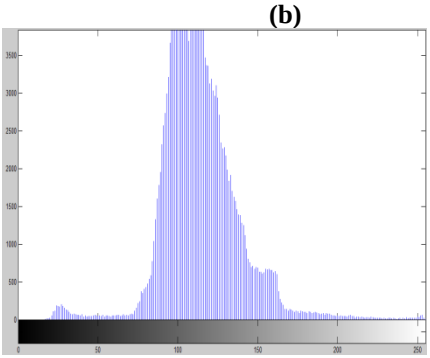
N

A key is needed in the embedding process. By using the key we can reduce the chance of third party attackers getting hold of the stego object and decoding it to find out the secret information.

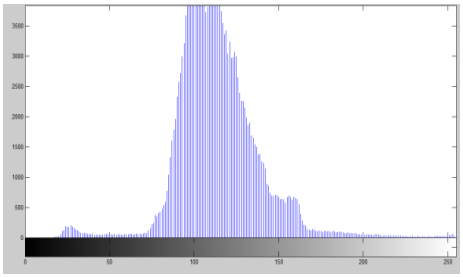
(a)



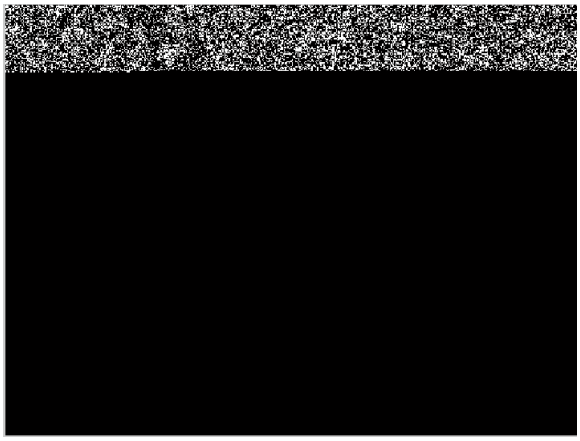
(b)



(c)



(d)

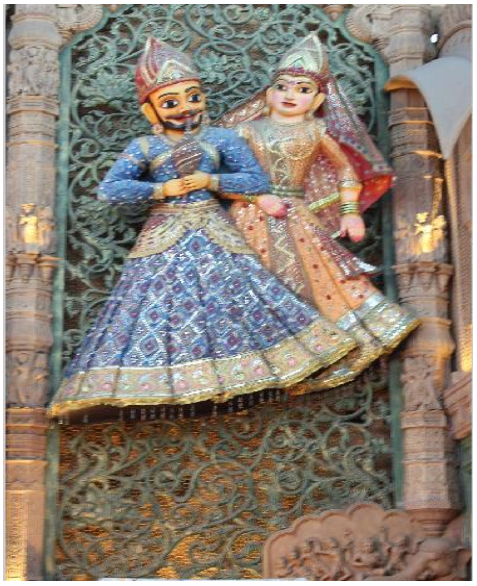


(e)

Fig. 2 (a) Cover image (b) Stego image (c) Histogram of cover image (d) Histogram of stego image (e) Effected area

In Fig. 2 we have taken image of size 605673 bytes, message size is 10452 characters and key is 8765432112345678765. But in Fig 3 image size is large i.e 2152812 bytes and message is of small size i.e 1050 characters and key is 234156783**.**

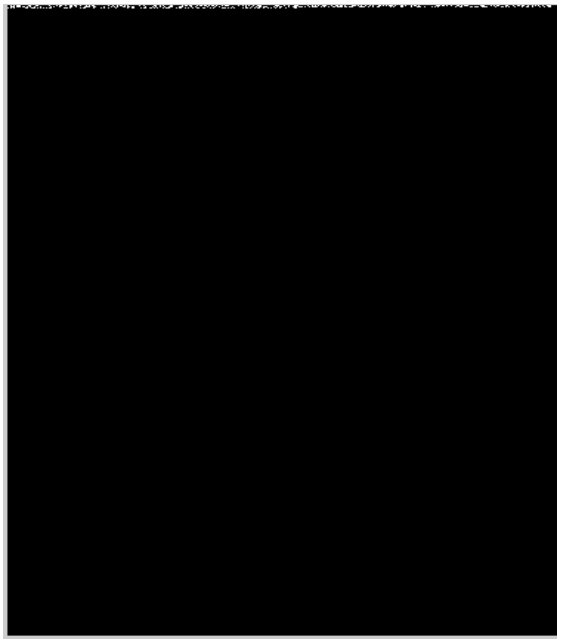
A stego image is the original cover image with the secret information embedded inside. This image should look almost identical to the cover object as otherwise a third party attacker can see embedded information. Having produced the stego object, it will be sent off via some communication channel. At the receiving end the stego object is fed into the system the public or private key that can decode the original key that is used inside the encoding process is also needed to detect the secret information.



(a)

In Figures 2(e) and 3(c) the salt and pepper noise in effected area gives us the information of embedded secret data in stego image. If size of image is large and message is small then the effected area is small. If size of image is small and message is large then the effected area is large.

(b)



(c)

Fig. 3 (a) Cover image (b) Stego image (c) Effected area

IV. Conclusions And Future Work

In this paper we propose a new and efficient method for an image which embeds large data. Our three layer approach extends the size of message storage. The experimental results demonstrate that our approach provides a better way for embedding more secret data into cover image. This method makes the data embedding process to alter more LSBs of a pixel to increase the capacity of the steganography. The proposed method makes the steganalysis hard. Hence the security, capacity will get improve.

References

[1] Mehboob,B.; Faruqui, R.-A."A stegnography implementation" Biometrics and Security Technologies. ISBAST pp. 1-5,2008.

[2] Xiaozhong Pan; BoTao Yan; KeNiu "Multiclass detect of current steganographic methods for JPEG format based re-stegnography" Advanced Computer Control (ICACC), 2nd International Conference pp. 79-82 ,2010.

[3] Saravanan, V.; Neeraja, A. "Security issues in computer networks and steganography" Intelligent Systems and Control (ISCO), 2013 7th International Conference pp. 363-366 , 2013.

[4] Bajwa, I.S.; Riasat, R "A new perfect hashing based approach for secure stegnography"Digital Information Management (ICDIM), 2011 Sixth International Conference pp. 174-178,2011.

[5] Mahmoud, H.; Alghathbar, K "Novel algorithmic countermeasures for Differential Power Analysis attacks on smart cards" Information Assurance and Security (IAS), Sixth International Conference pp. 52-55, 2010.

[6] Hao-Tian Wu; Jiwu Huang "Secure JPEG steganography by LSB+ matching and multi-band embedding" Image Processing (ICIP),18th IEEE International Conference pp.2737 -2740,2011.

[7] XikaiXu; Jing Dong; Tieniu Tan "Universal spatial feature set for video steganalysis"Image Processing (ICIP), 19th IEEE International Conference pp.245 – 248,2012.

[8] Moon, S.K.; Kawitkar, R.S. "Data Security Using Data Hiding" Conference on Computational Intelligence and Multimedia Applications, Vol. 4 pp. 247 – 251, 2007.

[9] Parah, Shabir A.; Sheikh, Javaid A.; Bhat, G.M. "Data hiding in intermediate significant bit planes, a high capacity blind steganographic technique" Emerging Trends in Science, Engineering and Technology (INCOSET) pp. 192 – 197, 2012.

[10] Mayuzumi, R.; Kojima, T "An improvement of steganography scheme based on complete complementary codes" Information Theory and its Applications (ISITA), pp.638 – 642, 2012.

[11] Ching-Nung Yang; Yao-Yu Yang; Tse-Shih Chen; Guo-Cin Ye "New Steganography Scheme in Halftone Images" Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP, pp. 1520 – 1523, 2008.

[12] Iuon-Chang Lin; Yang-Bin Lin; Chung-Ming Wang "An Efficient Steganography Scheme for M-Commerce" Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP, pp. 122 – 125, 2007.

[13] HuiTian; Ke Zhou; Hong Jiang; Yongfeng Huang; Jin Liu; Dan Feng, "An adaptive steganography scheme for voice over IP" Circuits and Systems, ISCAS, pp.2922 – 2925,2009.

[14] Kai Fan; Weidong Kou"A secure steganography scheme based on (N,t) threshold" Advanced Information Networking and Applications, pp. 536 - 539 Vol.2,2004.

[15] Fan, K.; Kou, W "Steganography scheme for m-commerce" Electronics Letters Vol. 41, pp.117 – 119, 2005.