ISSN:0975-9646

An Alternative Approach to Image Steganography and its Evaluation

Aakanksha Agarwal[1],Aditya N. Bhatt[2] and Yogin B. Bhatt[3]

Abstract— **Steganography is a technique of hiding information in image, video or audio files. The algorithms available for the same, aim to hide the data so that it can be shared and stored undetected. This paper proposes a new algorithm to conceal data inside the image pixels which is an alternative to the already existing LSB Technique. The proposed algorithm uses the logical operation Exclusive OR(XOR) in order to change pixels of the image and as a result store the data. The technique is implemented, analyzed and tested which thus determined the potential of the proposed algorithm in terms of security, robustness and integrity.**

I. INTRODUCTION

Information security has turned into a crucial area of concern due to rapid improvement in communication technologies along with an exponential growth of digital information. As secure offline systems are evolving into online systems, sensitive data storage as well as data exchange are in a vulnerable state. In attempt to protect the information and maintain its secrecy, different IT industries and people worldwide have developed different methods. The earliest attempt to serve the purpose of information security was the technique known as cryptography followed by steganography and others. Cryptography is defined as the art and science of mathematical scrambling of information into unintelligible form to preserve confidentiality[1]. Steganography is defined as the combination of two greek origin words stegos and graphic which means secret or covered and writing[2].

Cryptography is aimed to maintain the secrecy of message contents while added advantage of steganography is that alongwith the contents it also helps to keep the secrecy of its sender as well as receiver. Steganography most commonly uses images, audios and texts to protect the secrecy of the information.

II. IMAGE STEGANOGRAPHY

Image Steganography is the technique of embedding the information within the image in such a way that it prevents unauthorized user from detecting the hidden data which helps to maintain the secrecy of the message. Image Steganography can be used for securing private documents, passwords and encryption key[2]. This technique discourages any unauthorized individual or third party from realizing the existence of message hidden in the image even-though they are able to detect the transmission of image. The Least Significant Bit (LSB) method is one of the most basic and primitive methods in image domain in order to hide data and can be easily implemented in any programming language.

Image steganography is considered to be the most efficient,simple and secure way to transfer information on internet with respect to other types of steganography techniques. Less preference is given to text steganography which utilizes digital files, due to small amount of redundancy in text files and on the other hand, Audio/Video steganography is very complex to manipulate and hide information[3].

III. XOR LSB (XLSB) TECHNIQUE

Our proposed technique is a simple alternative of the currently existing LSB technique[2] which leads to a significant change in the number of pixels changed in an image for a sample set of words. The proposed technique instead of depending on the last bits of the pixels, depends entirely on the pixels themselves for the embedding and retrieval of secret information. In this paper we demonstrate the XLSB technique for a hiding a set of words in an RGB image.

A. Algorithm

1) Input : cover image, key and the message to be hidden
2) Choose the first pixel based on the key entered by the Sender and further, select remaining pixels using any pixel selection algorithm such as knight tour algorithm, starting with pixel say, (i,j,k) = $(key,0,0)$ where i,j are the pixel position and k is the plane (R,G,B)
3) Convert the text/data into 7-bit ASCII code and store it in an array of n x 7, where n is the length of text including spaces
4) Now, starting with pixel having position (i,j,k) obtain the binary string for the intensity at that position and compute XOR(say val) of the bits in the binary string.
5) Compare the value(val) from step 4 with the information bits(b) to be embedded into the image

```
If ( b = val )
   Do nothing
Else if ( b != val )
    if ( b = 1 )
     if ( last_bit = 1 )
       intensity(i,j,k) = intensity(i,j,k) - 1
     else
       intensity(i,j,k) = intensity(i,j,k) + 1
    else
```

*This work was not supported by any organization

[1]A. Agarwal is with the Department of Computer Engineering,Institute of Technology,Nirma University, Ahmedabad-382481, Gujarat , India aakanksha.2304@gmail.com

[2]A. Bhatt is with the Department of Computer Engineering,Institute of Technology,Nirma University, Ahmedabad-382481, Gujarat , India aditya.bhattce@gmail.com

[2]Y. Bhatt is with the Department of Computer Engineering,Gujarat Technical University,IIET, Dharmaj-388430, Gujarat , India yogin.bhattce@gmail.com

if ($last\_bit$ = 1)
intensity(i,j,k) = intensity(i,j,k) - 1
else
intensity(i,j,k) = intensity(i,j,k) + 1
end

6) Increment values of i,j and k and repeat steps 4-5 until all the information bits are embedded in the image or the values for i,j and k don't exceed the image size.

The mentioned algorithm is easy to execute in MATLAB or Java with simple availability of image processing libraries. The receiver should have the key used by the sender in order to reveal the information hidden by the sender in the Stego image.

B. Implementation

The XLSB technique has been implemented in MATLAB on a core i5 processor computer. This method is applied to hide a secret message "This is a simple message and it is used to describe the efficiency of XLSB" on lena image. It is apparent from figure 1 and 2 that both the images appear quite similar and no color differences exist in any part of the images.

In image processing, certain evaluation parameters exist for measuring the quality of an image such as mean, entropy and standard deviation. Image entropy marks the level of information embedded in a digital image and thus determines the quality of enhancement by comparing variations across the amount of information. The level of contrast can be associated with the change in standard deviation while the mean would indicate the variations in dynamic image[4].

The proposed method is evaluated based on these image parameters to check its efficacy and the value of these parameters before and after embedding is shown in Table 1[5].

TABLE I
IMAGE PARAMETERS FOR ORIGINAL AND STEGO IMAGE

	Entropy	Standard Deviation	Mean
Before Embedding	3.4046581	59.2957381	124.5978074
After Embedding	3.4046504	59.2958645	124.5976033

Mean Square Error, Peak Signal-to-Noise Ratio and Structural Similarity Index are considered to be one of the most widely used approaches for comparing a distorted image to an original image. MSE can be evaluated by computing the average of squared difference between a distorted image and an original image. PSNR is defined by the proportion of reference signal to the distorted signal in an image, measured in decibels. Greater the value of PSNR, greater is the similarity between distorted image and original. SSIM is established over the fact that human visual system is highly adaptable towards processing of structural information. This algorithm evaluates the variations in this information across the reference and distorted image[6]. When SSIM is calculated for our technique the value attained is 1 which suggests clearly that there is no visual change in the image produced after embedding the textual data in it. In order to get more accurate results, the three mentioned algorithms were used for Caltech-101 dataset[7]. Each image in the dataset is roughly 300 x 200 pixels. Table II shows values for various metrics after the images in the dataset were embedded with data. PSNR values for the dataset ranged from 75% to 87%.

Fig. 1. cover image

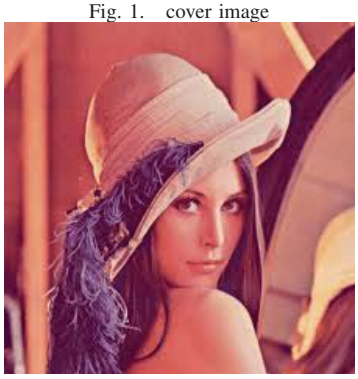

Fig. 2. stego image XLSB

TABLE II
IMAGE QUALITY ASSESSMENT

PSNR	MSE	SSIM	Bit Ratio(Unchanged/Total)
83%	0.0012	1	265/518 = 51%

IV. CONCLUSION

The proposed method has been employed for an android app in order to make a steganography tool for mobile phones in order to share and save important information with high security on the move. The method demonstrated in this paper is not a replacement for LSB technique but rather a different approach for hiding data. This method can be combined with existing cryptographic algorithms in order to come up with a more robust and powerful approach to hide messages and text. Along with encryption, data compression techniques can be used as well in order to hide more amount of data within the image as a result of which a technique will be devised which will be efficient and powerful in almost all aspects. Since this algorithm is new and not been used before it will be resistant to steganalysis for a very long time then the conventional LSB method.

REFERENCES

[1] W. Diffie and M. E. Hellman, "Privacy and authentication: An introduction to cryptography," in Proceedings of the IEEE, vol. 67, no. 3, pp. 397-427, March 1979. doi: 10.1109/PROC.1979.11256

[2] K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," Computer Communication and Informatics (ICCCI), 2014 International Conference on, Coimbatore, 2014, pp. 1-4.

[3] Y. Kakde, P. Gonnade and P. Dahiwale, "Audio-video steganography," Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on, Coimbatore, 2015, pp. 1-6.

[4] Proceedings of the 2015 Chinese Intelligent Systems Conference, Volume 1, Yingmin Jia, Junping Du, Hongbo Li, Weicun Zhang Springer, 21-Nov-2015 - Computers.

[5] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption",International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012, DOI: 10.5121/ijdms.2012.4605 57

[6] Image Quality Assessment (IQA) 1.1.2 by TOM DISTLER, http://tdistler.com/iqa/algorithms.html.

[7] L. Fei-Fei, R. Fergus and P. Perona. Learning generative visual models from few training examples: an incremental Bayesian approach tested on 101 object categories. IEEE. CVPR 2004, Workshop on Generative-Model Based Vision. 2004