International Journal of Information Sciences and Application (IJISA). ISSN 0974-2255, Vol.11, No.1, 2019, (Special Issue)
© International Research Publication House. http://www.irphouse.com

IMAGE STEGANOGRAPHY USING LSB ALGORITHM

Avni Aggarwal, B.tech, IMS Engineering College, Ghaziabad.

Arpit Sangal, B.tech, IMS Engineering College, Ghaziabad.

Aditya Varshney, B.tech, IMS Engineering College, Ghaziabad.

Abstract

Steganography is the process of hiding one file inside another such that others can neither identify the meaning of the embedded object, nor even recognize its existence. The main objective of Steganography is mainly concerned with the protection of contents of the hidden information. Images are ideal for information hiding because of the large amount of redundant space is created in the storing of images. Since this can be done in several ways, image steganography is studied and one of these methods has been used to demonstrate it here i.e., the LSB technique in which the least significant bit of every byte is altered to form the bit-string representing the embedded file. Altering the LSB will only cause minor changes in color, and thus is usually not noticeable to the human eye. While this technique works well for 24-bit color image files, steganography has not been as successful when using an 8-bit color image file, due to limitations in color variations and the use of a color-map. During its implementation, after the process of compression, a text message is hidden in the final, compressed image. This hidden information can be retrieved only through proper decoding technique.

1. LITERATURE SURVEY

A. Image Steganography and Data Hiding

Rutuja Kakade1, Nikita Kasar2, Shruti Kulkarni3, Shubham Kumbalpuri4, Sonali Patil

Student, Dept of Computer Engineering, PCCOE, Maharashtra, India

Associate Professor, Dept of Computer Engineering, PCCOE, Maharashtra, India

B. Review Paper on Image Steganography

Ashadeep Kaur*1, Rakesh Kumar2, Kamaljeet Kainth3

1 Research Scholar, Sachdeva Engineering College, For Girls, Gharuan, Mohali, India

Department of Computer Science & Engineering, Sachdeva Engineering College, For Girls, Gharuan, Mohali, India

2. INTRODUCTION

The word steganography is derived from the Greek words ‘stegos’ meaning ‘cover’ and ‘grafia’ meaning writing. In image steganography the information is hidden exclusively in images. The most common and popular method of modern day steganography is to make use of LSB (least significant bit) of picture’s pixel information. This technique works best when the file is longer than the message file and if image is grayscale. When applying LSB techniques to each byte of a 24-bit image, three bits can be encoded into each pixel.

Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

A: 01000001

Result: (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The three underlined bits are the only three bits that were actually altered.

LSB insertion is easy to implement, at the same time, easily attacked. Today steganography is being incorporated into digital technology. The techniques have been used to create the watermarks that are in our nation’s currency, as well as encode music information in the ever-popular mp3 music file. Copyrights can be included in files, and fingerprints can be used to identify the people who break copyright agreements. While Slight modifications in the color palette and simple image manipulations will destroy the entire hidden message.

3. PROPOSED TECHNIQUE

After reviewing the current products on the market for steganography, it was determined that there was not a practical implementation for 8-bit images. Although network speed is increasing, and bandwidth problems are decreasing, file size is still of utmost importance and smaller file sizes are optimal in network communication. Thus, the current steganographic use of 24-bit images leads to slower communication and thus development of an 8-bit image format would be beneficial. The aim of this research is to create a practical steganographic implementation for 8-bit images. A 24-bit bitmap image would be converted to an 8-bit bitmap image while simultaneously encoding the desired hidden information. An algorithm would be created to select representative colors out of the 24-bit image to create the palette for the 8-bit image. This palette would then be optimized to an 8-bit colormap that could be applied with minimal changes to the quality of the original image. This process of compressing the image from a 24-bit bitmap to an 8-bit bitmap resulted in minor variations in the image, which are barely noticeable to the human eye. However, these slight variations aid in hiding the data. Since there would not be an original 8-bit image to compare with the stego-image, it would be impossible to discern that the slight variations caused by hiding the data are different from the slight variations caused by compression. A practical steganographic implementation for 8-bit images enabled smaller file sizes to be utilized in steganographic communications. While also limiting the size of the hidden file, this implementation addressed issues that have been passed by in other applications, and provided a more compact vehicle for those secret communications that do not require a large cover-file.

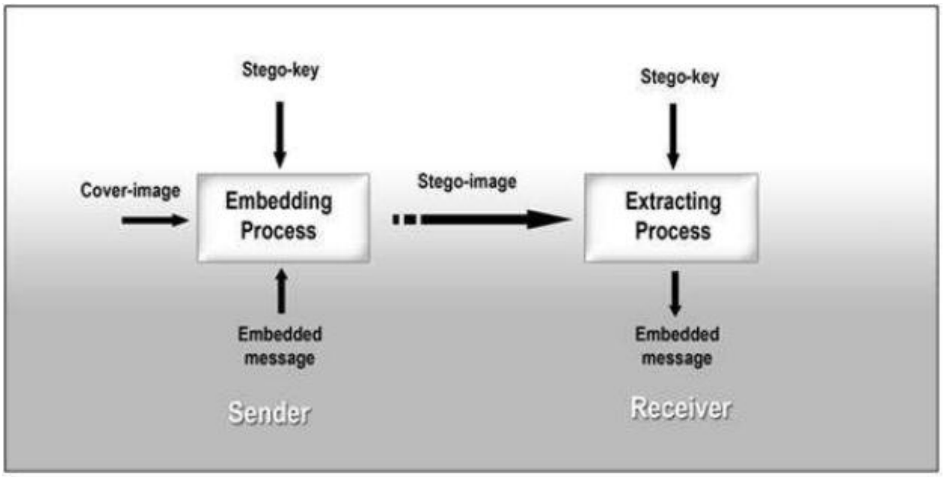

Fig.no. 1: The outline structure of image steganography

4.IMPLEMENTATION OF PROPOSED SYSTEM

In this proposed system, the secret message is used to hide in a cover bmp image. Firstly each character of secret message and each pixel of cover bmp image are converted into binary values. The user has to input stego-key as the password (stego-key is used to embed the secret message in a cover file).

After inserting secret message into cover image file, the resulting stego-image is sent to the receiver through the desired communication channel. While defining the starting point of embedding LSB, the stego-key is firstly collected from the user. The summation of the ASCII value of each character of stego-key is calculated and then the average of those characters value is computed. While substituting the secret message into LSB of cover image, the first LSB position is chosen according to the calculated average value of input stego-key characters. Then the substitution processing will continue until the end of secret message.

A. The embedding algorithm at the sender side

Step (1) : Get the input cover image and secret message.
Step (2) : Accept the stego-key from the user and calculate average value of them.
Step (3) : Convert each character of secret message and each LSB bit of cover image (R channel) from the position of average of stego-key.
Step (4) : Substitute the LSB bit of cover image (R channel) with binary values of secret message with respect to the starting point until the end of secret message.
Step (5) : Insert the end character value at the end of secret message.
Step (6) : Calculate the PSNR, SNR of original and resulting images.
Step (7) : Send a stego-image to the receiver.

B. The extracting algorithm at the receiver side

Step (1) : Get the input stego calculate average value
Step (2) : Load the stego-image that is sent from the sender.
Step (3) : Extract each of LSB bit from the stego image until to find out the end bit.
Step (4) : Reconstruct the collecting LSB bits from the stego-image.
Step (5) : Transform the LSB bits to correspondent characters.

Fig.no.2: Cover Image(Sample 1)

Fig.no.3: Stego Image

Fig.no.4: Cover Image(Sample 2)

Fig.no.5: Stego Image

Here, we have taken two cover medium in which the secret message is to be embedded. After the entire process of image steganography we can see that both the input images and the output image embedded with the message looks exactly similar.
This indicates that the LSB technique does not alter the image in a way that can be detected by the human eye but the image does contain a secret message within it. Hence, it is a secure technique for hiding a message within an image.

5.CONCLUSION

This paper describes a technique to successfully embed data in an 8-bit color image. Additional features that could be added to this project include support for file types other than bitmap, and implementation of other steganographic methods. However, this research work and software package provide a good starting point for anyone interested in learning about steganography.

6.REFERENCE

[1] B.Schneier, “Terrorists and Steganography”, 24 Sep. 2001, available: http://www.zdnet.com/zdnn/stories/comment/0,5859,2814256,00.html.

[2] Y. Linde, A. Buzo, and R. M. Gray, “An Algorithm for Vector Quantizer Design,” IEEE Transactions on Communications, pp. 84-95, January 1989.

[3] Andersen, R.J., Petitcolas, F.A.P., On the limits of steganography. IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection 16 No.4 (1998) 474–481.

[4] Johnson, Neil F. and Jajodia, Sushil. “Steganography: Seeing the Unseen.” IEEE Computer, February 1998, pp.26–34.

[5] C, R, Ravinder, A, R, Roja, Department of Master of Computer Appliccations, Teegala Krishna Reddy Engineering College, Medbowli, Meerpet, Hyderabad, “The Process of Encoding and Decoding of Image Steganography using LSB Algorithm”, International Journal of Computer Science and Engineering Technology”, Vol.2, Issue 11, Nov 2012. [6] Eric Cole ,"Hiding in Plain Sight: Steganography and the Art of Covert Communication"

[7] Gregory Kipper,"Investigator's Guide to Steganography "

[8] Stefan Katzenbeisser and Fabien, A.P. Petitcolas ," Information Hiding Techniques for Steganography and Digital Watermarking "

[9] Hiding secrets in computer files: steganography is the new invisible ink, as codes stow away on images-An article from: The Futurist by Patrick Tucker

[10] Ismail Avcıbas,, Member, IEEE, Nasir Memon,Member, IEEE, and Bülent Sankur, Member, "Steganalysis Using Image Quality Metrics," IEEE Transactions on Image Processing, Vol 12, No. 2,February 2003..

[11] Niels Provos and Peter Honeyman, University of Michigan, "Hide and Seek: An Introduction to Steganography" IEEE Computer Society IEEE Security &Privacy.

[12] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001.