KNOWLEDGECUDDLE PUBLICATION

International Journal of Computer Engineering and Sciences (IJCES) – Volume-1 Issue -2

A Survey of Image Based Steganography

Vikshit Rabara, Aditya Goswami

Information Technology Department
Gujarat Technological University,
Gujarat, INDIA

ABSTRACT: Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet [5]. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes [2]. In image Steganography, secret communication is achieved to embed a message into cover image (used as the carrier to embed message into) and generate a stego- image (generated image which is carrying a hidden message)[1]. In this paper we have critically analyzed various steganographic techniques and also have covered steganography overview its major types, classification, applications [3].

KEYWORDS: STEGANOGRAPHY, STEGO IMAGE, COVER IMAGE, LSB

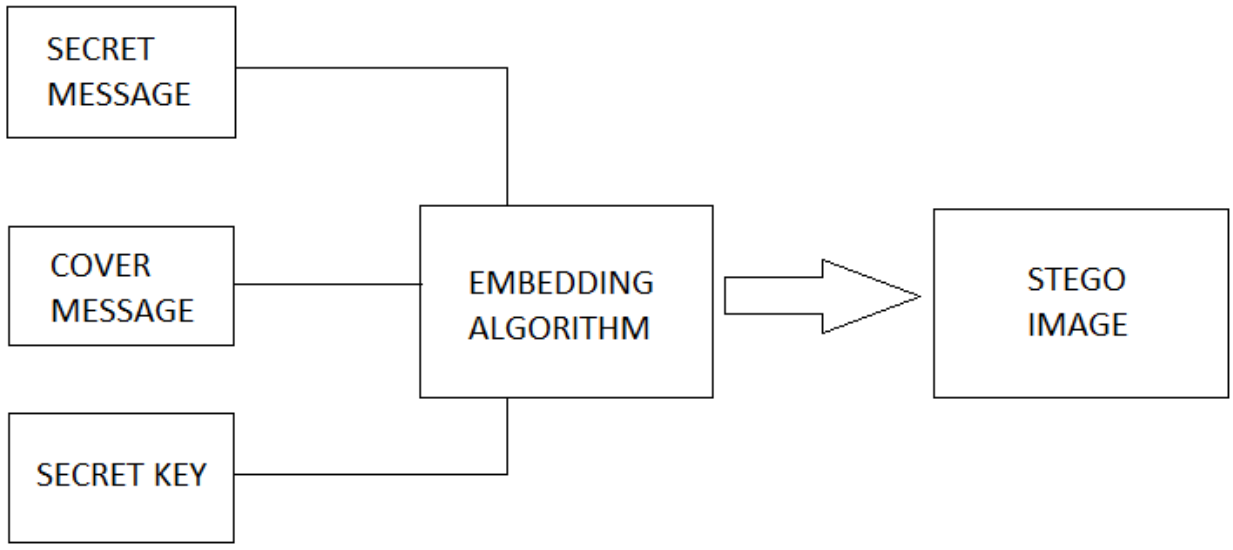
I. INTRODUCTION

Steganography is a technique to transfer information over the public communication channel in such a way that an attacker cannot identify the transmission of secret information on the background of a public communication [1]. Taking the cover object as image in steganography is known as image steganography. Coding secret message in digital image is by far the most widely used of all methods in the digital world of today. Main advantage of this method is that limited power of the human visual system. There are two basic methods implemented in steganography. Least significant bit (LSB) spatial domain based technique and transform-based frequency Domain technique [6].

II. IMAGE BASED STEGANOGRAPHY TECHNIQUE

Image steganography, the covert embedding of data into digital pictures, represents a threat to the protecting of sensitive information and the gathering of intelligence [8]. An image steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method. Someone can then use a proper embedding procedure to recover the hidden message from the image. The original image is called a cover image in steganography, and the message-embedded image is called a stego image [9]. Following figure shows the concept diagram of image based steganography.

ISSN: - 2394-6180(online) www.knowledgecuddle.com



IMAGE

A. BASED STEGANOGRAPHY

Such techniques like LSB, random pixel embedding, pixel value differencing, Discrete Cosine transformation (DCT), distortion, masking and filtering etc. From these, widely used techniques are LSB-Least Significant Method and DCT-Discrete Cosine Transformation. Reason behind this is that, it is easy to implement and hard to detect. Detail view on these two methods is given below [10].

B. LSB TECHNIQUE

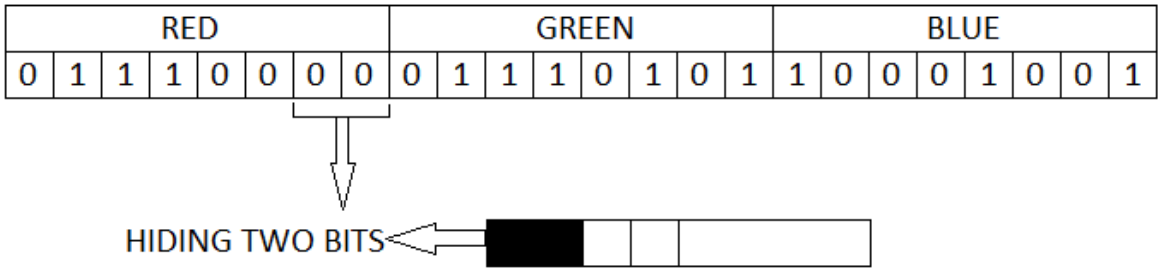
The LSB (Least Significant Bit) based steganography is combined with Genetic Algorithm to enhance security level of the image. Genetic Algorithm modifies the pixel locations of the stego image and hence the hidden data could not be recovered easily. The images are represented with numerical values of each pixel where the value represents the colour and intensity of the pixel [10]. Images are mainly of two types: 8-bit images, 24-bit images

- 8-bit images: In 8-bit images maximum numbers of colours that can be present are only 256 colours [1].
- 24-bit images: Each pixel in these images has 24 bit value in which each 8 bit value refers to three colours red, blue and green [1].

In this method we change the LSB of pixel with the binary code of secret message and then hide it in the original image. For this operation we use one or two bits as LSB and interchange it with message's bit.
Algorithm: Least Significant Bit Hiding Algorithm [8].

Inputs: RGB image, secret message and the password.
Output: Stego image.
Begin
Scan the image row by row and encode it in binary.
Encode the secret message in binary.
Check the size of the image and the size of the secret message.
Start sub-iteration 1:
Choose one pixel of the image randomly
Divide the image into three parts (Red, Green and Blue parts)
Hide two by two bits of the secret message in each part of the pixel in the two LSB

Set the image with the new values.
End sub-iteration 1.
Set the image with the new values and save it.
End
Following figure shows the Least Significant Bit Hiding Technique. In which, we hide the two LSB of the any pixel and replace it by the bit of secret message [10].



In nowadays, 24- bit image is more used in the LSB technique because it uses RGB (red, green, blue) colour scheme to hide the data and it has more than 16 million colour combination while in 8-bit image, we use gray scheme to secure the data. As mentioned above that it has only 256 colour combination, so it is less robust and less secure than the 24-bit image.

C. Advantages of LSB method

It is easiest method in between all the steganographic methods. . A large majority of freely available steganography software makes use of LSB replacement, but there is a more important reason: it can be performed without any special tools at all [2]. We can consider it as worthy of study because of its widespread use.

D. Disadvantages of LSB method

These methods are based on false assumption that LSB plane of natural images is random enough, thus are suitable for data hiding [3]. Such assumption is not always true, especially for images with more smooth regions.

III. DCT TECHNIQUE

DCT based technique insertion of secret information in carrier depends on the DCT coefficients [7]. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information. LSBs of these potential locations in carrier image are replaced with MSBs of the secret image [4].

Embedding Process [5]
Step 1: Select Carrier Image from the set.
Step 2: Find DCT coefficients of Carrier Image.
Step 3: Traverse through each pixel in Carrier Image till end of Secret Image.
Step 3.1: If DCT coefficient value is below threshold then replace LSB(s) with MSB(s) of pixels in Secret Image.
Step 3.2: Insert 1 at that location in the key matrix.
Step 4: Evaluate the Stego Image

IV. CONCLUSION

This paper gave an overview of different steganographic techniques its major types and classification of steganography which have been proposed in the literature during last few years. We have critical analyzed different proposed techniques which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods. And many of them embedding techniques can be broken or shows indication of alteration of image by careful analysis of the statistical properties of noise or perceptually analysis.

REFERENCES

[1]. N. Provos and P. Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Security and Privacy, Mar 2003, 32-44.

[2]. Neil F. Johnson and Sushil Jajodia, Exploring Steganography: Seeing the Unseen, IEEE computer, Feb 1998, 26-34

[3]. G. C. Kesseler, Steganography: Hiding Data within Data, an edited version of this paper with the title Hiding Data in Data, originally appeared in the April 2002 issue of Windows & .NET magazine. Sep 2001.

[4]. S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009).

[5]. C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[6]. K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[7]. J. Rodrigues, J. Rios, and W. Puech "SSB-4 System of Steganography using bit 4", In International Workshop on Image Analysis for Multimedia WIAMIS, May, 2005.

[8]. J. Fridrich, and M. Goljan, "Practical steganalysis: state-ofthe-art", In Proceeding of SPIE Photonics West, Electronic Imaging 2002, volume 4675, pp. 1-13, 2002.

[9]. Tu C. and Tran T D. "Context based entropy coding of block transform coefficients for image compression", IEEE Transaction on Image Processing, Vol.11, No.11, November, 2002.

[10]. Wenqiong Yu, "Blind Detection for JPEG Steganography", International Conference on Networking and Information Technology , pp. 128-132, July 2010.