SHIV SHAKTI

International Journal in Multidisciplinary and Academic Research (SSIJMAR)

Vol. 10, No. 4, September 2022 (ISSN 2278 – 5973)

Steganography through Grey Level Alteration for Secret Communication

Prof. Pankaj Nandan

Associate Professor in Computer Science

Govt. College for women, Kathua (J&K)

Rakhi Billawaria

Lecturer in Computer Science

GDC Reasi, J&K.

Abstract

Today's industrial informatics has been facing number of issues relating to security, privacy, and malwares, trusted computing, intrusion detection and protection of information. They are significant components for industrial based IT solution. Most of the industrial software systems depend upon third participant vendors to provide the protection. However, this approach has created trust deficit issues over the third party. In this paper, an attempt is made to understand the approach that can provide an effective security and information protection through steganography without any help from the third party trustees. The present paper has discussed steganographic algorithm which is an information hiding method that allow secret *communication to cover and conceal information within the spatial domain of the image. The principle behind the algorithm is to insert information by changing the grey level values of the grey scale image pixels.*

Keywords: Grey Level Alteration, Information hiding, Algorithm, Secret Communication.

Introduction

The success of steganography is dependent on the secrecy of the cover medium, as well as on the robustness of the algorithm used. To protect secrecy, it is required to discover new and better cover mediums as well as design and develop robust algorithm. Steganography is also known a 'covered writing' and includes methods of transmitting secret messages through innocuous cover mediums in such a manner that the existence of the embedded messages is undetectable. Carriers include innocent images, audio, video, text, or any other digitally represented code. The hidden message may be plaintext. Ciphertext or any-thing that can be represented as a bit system. Steganography is used to achieve the goal of disguising the existence of secret communication.If the existence of communication is decoded then this goal is defeated. We note that the use of third party as trustee is one method to provide security and protect our industrial based systems. But the use of steganography is like our own security-guard steganographic technique and algorilhm, which inserts data or information within the spatial domain of the grey scale images by modifying the grey level values of the pixels for our own protection. In this paper, an attempt is made to firstly understand the challenges while solving the problems. An overview of the existent research in image steganography is also analysed in this paper. It also comprises of new techniques in image steganography i.e. Grey level modification.

Challenges of Steganographic Techniques

The application of steganography method for secure information transmission and sharing without third party trustee is our main purpose. However, we face challenges with steganographic techniques because they can be detected by careful statistical analysis.We face two major challenges with any steganographic technique:

(A) Information embedding capacity and,

(b) Robustness of algorithms against detection.

In this paper, an attempt is made to build up a method which can insert a large amount of data in a cover medium with the least amount of changes. So, it is recommended to alter the image in its spatial domain to achieve our objective.

Image Steganography

Existing steganographic mediums and techniques suffer from a myriad of attacks on images, video and audio (Johnson and Jajodia 1998) and (Pal et al. 2002). Researchers have undertaken great efforts to defend the attack by improving cover medium or communication protocols.

A. Defending techniques through covered medium

There are varieties of methods by which information can be hidden in images. Some well know techniques are described here:

Replacing Least Significant Bit

Most data or information concealing methods in steganography are to change the insignificant information in the cover image. For instance, a simple scheme suggested by Chen and Lee (Chen 2001, Lee et al. 20001) is to place the inserting data at the least significant bit (LSB) of each pixel in the cover image. The modified image is called stego image. Altering LSB does not change the quality of image to human perception but this scheme is sensitive to a number of image processing attacks like compression, cropping etc.

Replacing Moderate Significant Bit

Chan and Chang (2001) showed how to employ the moderate significant bits of each pixel in the cover image to insert the secret message. This method upgraded sensitivity to modification but it degrades the quality of stegoimage.

Pixel Modification Techniques

Recently, some Steganographic techniques have been responded which change the pixels to insert data. Some of them(Zincheng et al. 2003, Wu et al. 2003, Xinpeng and Shuozhong. 2003, Soo-Chang and JingMing. 2003,Zincheng et al. (2003) have reported a technique for reversible data hiding which has an embedding capacity of 5Kb to 60kb and PSNR of 48db for a 512x512x8 hit greyscale image. They embedded data by shifting the range of histograms. Wu et al. (2003) proposed the pixel value differencing (PVD) method of steganography which can conceal huge amount of data by altering the different values between pairsof adjacent pixels. Using this method, more data can be placed in areas where differences in the adjacent pixel values is large as pixels in these areas can tolerate more changes and this leads Io good imperceptibility and a high embedding rate. Xinpeng and Shuozhong (2003) pointed out that although PVD steganography is resistant to RS steganalysis is vulnerable lo steganalysis bases on histogram of pixel value differences.

B. Defending techniques through protocols

Fisk et al. (2002) see the weaknesses of the TCP/IP protocol suite and discuss how those weaknesses could be used as secret channels for secret communication, whereas Bao et al. (2002) have shown the application of Communication accessories like email headers etc. for secret Communication. Other familiar information hiding methods employ the transformation domain of digital media to hide information (Chang et al. 2002. and Hsu et al. 19991). Functions including the discrete cosine transform (DCT) and the discrete wavelength transform (DWT) are widely applied (Petitcolas et al. 1999, Chang et al. 2002. and Hsu et al. 19991). These methods hide the messages in important fields of the cover image which makes them vigorous against compression, cropping and other image processing attack. Although, defending methods either through covered medium or protocol are important, it is found that very few researchers had offered breakthrough thinking on alternate approaches to protect information transmission and sharing.

New Techniques: Grey Level Modification

The method proposed here is Grey Level Modification (GLM) Steganography technique. The images that are usedare grey scale images. The grey level modification algorithm is planned with the objective of information concealing rather than image processing. The information that has to be hidden is to be in binary data format. In order to explain this technique, it is pertinent to start by introducing elementary concepts.

A. Images: Image can be viewed as a two dimensional array and each array location can be referred to as a pixel. A digital image can be represented by a two dimensional functional *f*(x, y), where x and y are Spatial coordinates and the amplitude of *f* at any pair of coordinates (x, y) is called the intensity *I*of the image at that point.

B.Image Pixels

Each image is composed of finite element each of which has a definite location and amplitude. These elements are referred as image pixels.

C. Grey Scale Image

A grey scale image is defined as an image whose pixel values span the grey scale.

D. Grey Level Modification

Grey level modification is defined as a method in which the grey level values of the image pixels are altered in accordance with a mathematical function, to represent binary data. Each pixel has a different grey level value which can have an odd or even value. This odd or even value of the grey level is appropriately modified to depict binary data.

Grey Level Modification Steganography

Grey level modification steganography is a method to map data by altering the grey level values of the image pixels. GLM steganography employs the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data (i.e. a bit stream with 1s and 0s) and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The grey level values of those pixels are examined and compared with the bit stream that is to be mapped in the image. Initially, the grey level values of the selected pixels (which are odd) are made even by changing the grey level by one unit. Once all the selected pixels have an even grey level it is compared with the bit stream which has to be mapped. The first bit from the bit stream is compared with the first selected pixel. If the first bit is even (is 0), then the first pixel is not modified as all the selected pixels have an even grey level value. But if the bit is odd (i.e. 1), then the grey level value of the pixel is decremented by one unit to make its value odd, which then would represent an odd hit mapping. This is carried out for all bits in the bit stream and each and every hit is mapped by modifying the grey level values accordingly.

Conclusion

In this paper, an attempt is made to propose new technique for some information transmission, protection and sharing via the steganographic approach. This can be used in industrial scale systems, networks, data and sewer security and protection without employing third party trustees. The approach gives industry organizations a tool to use their security guards rather use third parties. The pragmatic support of this method is the mapping of information data within the spatial domain of the image by altering grey level values of the pixels. This paper shows how employing the concept of odd and even numbered grey values can be used to map binary data. The complexity of our algorithm is of the order O(n). Modifying the grey level values by one unit would not change the image statistics to a great extent. We used this concept and designed our algorithm.

References

Bao, F. (2002). Steganography of short messages through accessories. *In Pacific Rim Workshop on Digital Steganography*, July 11-12, 2002, Kitakyushu, Japan.

Chang, T, Chan, T. & Chung, L. (2002). A Stegnographic method based upon JPEG and quantization table modification. *International Journal of Information Sciences--Informatics and Computer Science, 14*(1-2), 123-138.

Fisk, G. Fisk, M., Papadopoulos, C. Joshua, N., (2002). Eliminating Steganography in internet traffic with Active Wardens. In F.A.P. Petitcolas, ed. 5th*International Workshop on In Information Hiding*, October 7-9, 2002.

Hsu, C. T., Wu, J. L. (1999). *Hidden Digital Watermarks in Images*. In IEEE transaction on Image processing, 8(1), 58-68.

Zmcheng. N.. Yun. U. S.. Anran. N., Wd. S.. 2W3. *Reversnble Dam Hiding*.