

A Survey Paper for Development of Digital Watermarking Algorithm Using Lsb For Security

Sanjana Kishor Kolhe¹, Prof. DR.N. K.Choudhari²

¹Mtech student Department of Electronic and communication Engineering, PBCOE College, Maharashtra, India

²Principal & Professor Department of Electronic and communication Engineering, PBCOE College, Maharashtra, India

-----***-----

Abstract - Steganography is the art of covered or hidden writing. In another word we can say that it is an encrypted form of data. The purpose of steganography is to covert communication-to hide the existence data of a message from a user. This paper is intended the high-level technical introduction to steganography for those unfamiliar with the field. It is directed at forensic computer examiners who need, practical understanding of steganography without delving into the mathematics, although references are provided ,some of the ongoing research for the person who needs or require additional detail. This paper provide the historical context for steganography, the emphasis is on digital applications, focusing on hiding information in online audio or image files. Examples of software tools that employ steganography to encrypt or hide data inside of other files as well as software to detect the such hidden, decrypted files will also be presented.

Keywords— Digital watermarking, Grayscale images, secret data, LSB, PSNR.

1. INTRODUCTION

Steganography differs from cryptography, the art of secret writing, which intended to make a message unreadable by a user but does not hide the existence of the secret communication. The steganography and cryptography are different, there are many analogies between the two, and some authors categorize steganography is form of cryptography since hidden communication is a form of secret writing. Nevertheless, this paper will treat steganography as a separate field. Whereas the term steganography was firstly used at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, tattooed on the scalp of slaves. Invisible ink has been in use for centuries-for fun by children and students ,for serious espionage by spies and terrorists. Microdots and microfilm, a staple of war and spy movies, came about after the invention of photography (Arnold et al. 2003, Johnson et al. 2001, Kahn 1996; Wayner 2002).

Text Stegnography using LSB[Least significant bit] Insertion Method It was proposed by Bhavasna.S1 and K.L.Sudha2 ECE Department, at April 2012

The art of information hiding has been around nearly as long as the need to convert communication. Stegnography, the secret of information ,early as an extremely useful method for convert information transmission. Stegnography is art of hiding secret message within a larger image which is undetectable, this is in contrast to cryptography, The existence of the message itself is not disguised, but the content is obscure. The goal of a stegnographic method is to minimize the visually apparent and statistical differences between the cover data and a stegnogram while maximizing the size of the payload. Current digital image stegnography is the challenge of hiding message in a digital image a way that is robust to image manipulation and attack, This paper explains about how a secret message can be hidden into an image using least significant bit insertion method along with chaos.

image manipulation and attack, This paper explains about how a secret message can be hidden into an image using least significant bit insertion method along with chaos.

An Overview of image Steganography using Lsb Technique They proposed by Nitin Jain ,Sachin Meshram, Shikha Dubey ,July 2012 Steganography is art of hiding the fact that communication is taking place in the form of encrypted data. Many different carrier file format-can be used ,but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. This Paper intends to give an overview of image steganography which uses this technique. For a more secure approach ,this paper encrypts the message using secret key and then sends it to the receiver. The receiver than decrypts the message to get the original one. The rapid development of data transfer through internet made it easier to send the data faster and accurate to the destination. This paper deals with the algorithm based on hiding a large amount of data (image,audio,text) file into color BMP[Bit map image] image.This project gives a brief idea about the image steganographic approach that make use of least Significant Bit algorithm for embedding the data into the bitmap images. The Least Significant Bit embedding technique suggest that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file.

An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution it was proposed by Ankit Chadha, Neha Satam, Rakshak Sood, Dattaray Bade ECE Department, Vidyalankar Institute of Technology Mumbai, India.Sept 2013 In order to improve the data hiding in all types of multimedia data formats such as image and audio and to make hidden message undetectable, a novel method for steganography is introduced in this paper. It is based on Least Significant Bit [LSB] manipulation and inclusion of redundant noise as secret key in the message. This method is applied to data hiding in images. For data hiding in audio, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) both are used. All the results displayed prove to be time-efficient and effective. Also the algorithm is tested for various numbers of bits.

Conclusion-

As per my conclusion the three techniques of steganography of lsb as described above which was presented by, Bhavana and K.L.Sudha ECE Department, April 2012 Nitin Jain, Sachin Meshram, Shikha Dubey ,July 2012 Ankit Chadha, Neha Satam, Rakshak Sood, Dattaray Bade ECE Department, Vidyalankar Institute of Technology, Mumbai, India.Sept 2013 This paper proposed a new LSB based digital watermarking scheme within third and fourths LSB in the gray scale image . After the secret data is embedded in the third and fourth LSB in the image it determine the coordinates, we get watermarked image without noticeable distortion on it. Therefore, this digital watermarking algorithm can be used to hide data inside the image.

REFERENCES-

- [1].Amirthanjan, R.Akila,R & Deepikachowdavarapu, P., 2010. A Comparative Analysis of Image Steganography, International Journal of Computer Application, 2(3), pp.2-10.
- [2]. Chandramouli, R. and N. Memon, 2001. Analysis of LSB based image steganography techniques. Proc. of ICIP, Thessaloniki, Greece.
- [3]. Nedeljko Cvejcic, Algorithms for audio watermarking and steganography, Oulu University Press, Oulu 2004, pp. 40-42.

- [4]. Ajay.B.Gadicha¹, "Audio Wave Steganography", and International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-5, and November 2011.
- [5]. Chan, C.K. Cheng, L.M., 2004. Hiding data in images by simple lsb substitution: pattern recognition.vol 37. Pergamon.
- [6].Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355–372.
- [7].Sanjeev Manchanda, Mayank Dave, and S. B. Singh, "Customized and secure image Steganography through Random numbers logic", Signal Processing: An international Journal, Vol. 1: issue.
- [8]. N. Provos and P. honeyman, "Hide and seek : an introduction to steganography" IEEE Computer Society, 2003.
- [9].Saeid Fazli and Gholamreza Khodaverdi, "Trade-off between Imperceptibility and Robustness of LSB Watermarking using SSIM Quality Metrics", 978-0-7695-3944-7/10 \$26.00 © 2010 IEEE DOI 10.1109/ICMV.2009.68
- [10] Gil-Je Lee, Eun-Jun Yoon, Kee-Young Yoo, "A new LSB based DigitalWatermarking Scheme with Random Mapping Function", 978-0-7695-3427-5/08 \$25.00 © 2008 IEEE DOI 10.1109/UMC.2008.33
- [11] Gaurav Bhatnagar, Balasubramanian Raman, " A new robust reference watermarking scheme based on DWT-SVD", 0920- 5489/\$ – see front matter © 2008 Elsevier B.V. All rights reserved. doi:10.1016/j.csi.2008.09.031.