Steganography Secure –A Review Paper

Nadeem Ahmad,Moin Khan ,Manoj Kumar

IMS Engineering College

Abstract

Study of invisible communication is called as steganography . Steganography is used to maintain secrecy between two communicating parties. In the image steganography, Secrecy can be achieved by embedding data into cover image and generating a stego-image . There are different types of steganography techniques and each have its own strengths and weaknesses. In this paper, we will be reviewing the different security and data hiding techniques that are widely used for implementing a steganography such as LSB.

Keywords —*Steganography, Cryptography, LSB*

1.INTRODUCTION

In modern day world, the communication is the the basic necessity of every area. Each and everyone wants the secrecy and safety of their data. In our day to day life, we are using many secure ways like internet or telephone for sharing information, but it's not secure. In order to share the information in a reliable manner we can use steganography. Steganography techniques have been developed to keep share safe and secure. Steganography hides the existence of data so that no one can detect its presence. Steganography is the process of hiding information datat inside multimedia content such as image , audio, video. For the increase of the confidentiality of the communicating data it works in efficient manner.

2.STEGANOGRAPHY

Steganography is a Greek word. The "steganos" means "covered " and "graphical " means "writing" .Steganography is not only the act of data hiding but also hiding the fact of transmission of data. Thus, Steganography helps in hiding of the secret data in another file in such a way that receiver knows the existence of data. People transmit the data in the form of text, images and audio over the internet. The multimedia object such as audio, images are used as a wrap sources in hiding of the data.

A) Types of Steganography

1. *Image Steganography:* Image steganography is referred as hiding the data by taking the wrap object as image. Pixel intensities are used to hide the data in image steganography. Images are widely used as wrap source In digital steganography.

2. *Audio Steganography:* Image steganography is referred as hiding the data by taking the wrap object as audio file. This method is widely used to hide the data in WAV, AU and MP3 sound files. We have used LSB encoding in our project.

B. Steganography Terminology

Steganography consists of the two terms which are message and wrap image. Message is the data that needs to hide and wrap image is the carrier that hides the message in it.
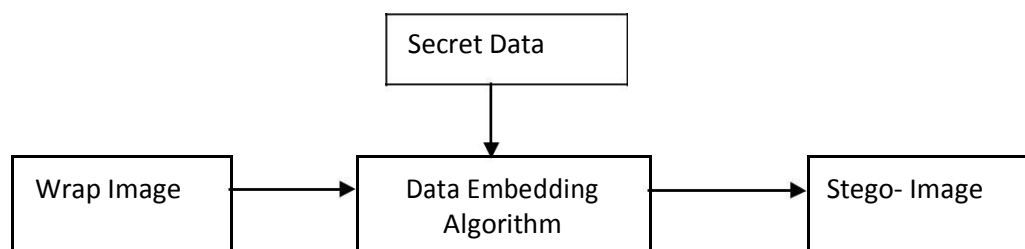

Fig 1 : Steganography Diagram

C. Steganography Techniques

    1 LSB: LSB is the method which is commonly used for hiding of data. In LSB method the embedding of data is done by replacement of the least significant bits of image pixels with the bits of secret data. The image which is obtained after embedding is almost similar to the original image.

    2 Distortion Techniques: In distortion technique the secret message is stored by distorting the signal. A sequence of modification are to be applied to the cover by the encoder. The decoder will measures the differences between the original cover and the distorted cover.

E. Application of Steganeography

  i)Confidential Transfer of Data
  ii) Protecting the Data
   iii) Digital Content Distribution
  iv) E-Commerce
  v) Media
  vi) Database Systems

3.CONCLUSION AND FUTURE WORK

In this project we get to know that steganeography has wide future scope .By reviewing various papers we observed that most of the steganography work is done in the year 2012 and 2013. In these years, LSB method of steganeography is the most widely used technique for steganography. This project deals with various aspects of steganeography . The different security and data hiding techniques are used to implement steganography using LSB .

REFERENCES:

[1]   Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., *"Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography"*, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[2]   Swati malik, Ajit   "Securing Data by Using Cryptography with Steganography" International   Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[3]   Ishwarjot Singh ,J.P Raina,‟ *Advance Scheme for Secret Data Hiding System using Hop field & LSB"* International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[4]   G. Manikandan, N. Sairam and M. Kamarasan *"A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme "*, Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[5]   Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, *"Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique"*, International Conference on   Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[6]   Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, *"Extracting spread-spectrum hidden data from digital media "*, IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.

[7]   Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., *" A new Steganographic method for color and gray scale image hiding",* Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[8]   Bailey, K., and Curran, K., *"An Evaluation of Image Based Steganography Methods"*, Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[9]   Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, *"Triple-A: Secure RGB Image Steganography Based on Randomization",* International Conference on Computer Systems and Applications (AICCSA-2009), pp: 400-403, 10-13 May 2009.

[10] R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq and John Bosco Balaguru Rayappan , *"Colour Guided Colour Image Steganography"* Universal Journal of Computer Science and Engineering Technology , 16-23, Oct. 2010, pp. 2219-2158.