IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 143-146
www.iosrjournals.org

Analysis of LSB insertion algorithm for through Digital Steganography

Dr. Shipra Jain
Guru Nanak Institute of Management, Road No.-75, West Punjabi Bagh, New Delhi

ABSTRACT: *Image processing in the field of electrical engineering is defined as any form of signal processing for which the input taken is in the form of an image such as photographs or frames of video; the output of image processing can be either an image or some of the parameters related to that image. Most of image-processing techniques involve treats the image as a two-dimensional signal and applies various standard signal-processing techniques to it.*

The technique on which this research paper presents the general overview of steganography. Steganography is the process of hiding data into an image, without making visible changes to the image. This process is a subset of Image Processing. In this paper, Image Watermarking using Least Significant Bit (LSB) algorithm has been used for embedding the message into the image.

Keywords: *Cryptography , least significant bits, Steganography,Watermarking, JPEG (Joint Photographic Experts Group)*

I. INTRODUCTION

Steganography is the art of writing hidden messages in such a way that no one, apart from the sender and particular recipient, suspects the existence of the message. The word steganography is of Greek origin and means "concealed writing". Generally, messages will appear to be something else: images, articles, shopping lists, or some other covertext and, classically, the hidden message may be in invisible ink between the visible lines of a private letter The word steganography is derived from the Greek words "steganos" and "graphein", which mean "covered" and "writing." Steganography, therefore, is covered writing. In this research paper the LSB(LEAST SIGNIFICANT BIT)method is discussed and also how can it be implemented on BMP image format. In this research paper the main stress is given on the LSB method of performing digital steganography. but along with this other ancient and present day methods and techniques of steganography are also discussed.

II. TYPES OF STEGANOGRAPHY

2.1. Physical steganography

Steganography has been widely used including recent historical times and the present day. Possible permutations are endless and known examples include:

1 Hidden messages written on the paper with the help of secret inks, on the blank parts of other messages.
2 Messages written at the back of postage stamps.
3 Hidden messages written on messenger's body:in ancient time. Messages were tattooed on the person's shaved head,and was hide with the growth of his hair,and when that message was needed to be exposed it was done by shaving his head again.
4 Hidden messages within wax tablets:for example in ancient Greece the people used to write messages on the wood, then that wood was covered with the help wax ,upon which a covering message was written.

2.2. Digital steganography(modern)

1 Concealing the required messages to be sent within the lowest bits of noisy images or sound files.
2 Pictures are embedded in some video material (optionally played at slower or faster speed).
3 Injecting imperceptible delays to packets which are to be sent over the network with the help of keyboard . Delays made in keypressing in some applications (telnet or remote desktop software) can lead to the delay in packets, and that kind of delays in the packets can be used to encode data.

III. Techniques

3.1. Modern steganography Techniques

Masking and Filtering: Is where information is hidden inside of a image using digital watermarks that include information such as copyright, ownership, or licenses. The purpose is different from traditional steganography since it is adding an attribute to the cover image thus extending the amount of information presented.

Algorithms and Transformations: This technique hides data in mathematical functions that are often used in compression algorithms. The idea of this method is to hide the secret message in the data bits in the least significant coefficients.

Least Significant Bit Insertion: The most common and popular method of modern day steganography is to make use of the LSB of a picture's pixel information. Thus the overall image distortion is kept to a minimum while the message is spaced out over the pixels in the images. This technique works best when the image file is larger then the message file.that is the image must have as much space to hide the data inside it.

3.2. Printed steganography

Digital steganography output may be in the form of printed documents.A message, the plaintext, may be first encrypted into some unreadable form by traditional means, and converting that into a ciphertext.after that an innocuous covertext is modified in some way to as to contain the ciphertext resulting in the stegotext.For example, the letter size, spacing,or on other characteristics of a covertext manipulation can be done to carry the hidden message. Only a recipient who knows the technique used can recover that message and then can decrypt it.

IV. RELATION BETWEEN STEGANOGRAPHY AND CRYPTOGRAPHY

4.1.CRYPTOGRAPHY and STEGANOGRAPHY are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect e-mail messages, credit card information, corporate data, etc.

4.2.Cryptography protects information by transforming it into an unreadable format. from Greek, it literally means "covered writing" confidential transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called cipher text via an encryption algorithm. Only those who possess a secret key can decrypt the cipher text into plaintext. Where as Steganography is the process of hiding data into an image, without making visible changes to the image.

4.3.CRYPTOGRAPHY and STEGANOGRAPHY are cousins in the spy craft family: the former scrambles a messages so it cannot be understood by the unauthorized user, the latter hides the message so it cannot be seen. A cipher message, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. because it is not easy to retrieve the data from the images

V. THE VARIOUS SOFTWARES HELP IN PERFORMING STEGANOGRAPHY

OUTGUESS is a steganographic tool that allows the insertion of hidden information into the redundant bits of data In this version the PNM and JPEG image formats are supported.

CAMERA/SHY is the only steganographic tool that automatically scans and delivers decrypted content straight from the Web. It is a only, Internet Explorer-based browser that leaves no trace on the user's system and has enhanced security
F5 is a publicly available steganography software package which hides messages in BMP, GIF, and JPG graphics.
JPHIDE and JPSEEK are programs which allow you to hide a file in a jpeg image.

MP3STEGO will hide information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.

STEGHIDE is a steganography program that is able to hide data in JPG, BMP, WAV, and AU files. The color frequencies are not changed thus making the embedding resistant against first-order statistical tests.

HYDAN steganographically conceals a message into an executable. It exploits redundancy in the i386 instruction set by defining sets of functionally equivalent instructions

VI. STEGANOGRAPHY DETECTION SOFTWARE

STEGDETECT is an automated tool for detecting steganographic content in images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images.with the help of these tool the hidden text or data can be discovered,this can be applied on any kind of steganography technique..

VII. DETECTION

The steganographic contents can be detected with the help of following Detection Methods

7.1. Visual analysis - tries to reveal the presence of secret communication through inspection, either with the naked eye or with the assistance of a computer.

7.2. Compare original with suspect file –any alteration in the original image can be detected by comparing the original file with suspect file.

7.3. Statistical analysis can show whether the statistical properties of the files deviate from the expected norm,this reveals tiny alterations in an image's statistical behavior caused by steganographic embedding.

7.4. Passive steganalysis detects the presence or absence of a secret message in an observed message.

7.5. Active steganalysis extracts a version of the secret message from a stego message.

VIII. LSB – LEAST SIGNIFICANT BIT HIDING (IMAGE HIDING)

This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. Steganography is the process of hiding data inside an image without making noticeable change in image. Digital steganography is also known as Watermarking. In digital world copyright protection is a big problem. Its quite difficult to prove once authority over a digital file. To protect digital content technique of watermarking or steganography is used Practically there can be a number of protocols to implement steganography. The proposed protocol is as follows.

4bytes/character is used

Offset+2bytes =reserved for data length

Couple of LSB's of Imagedata is used to store databits.

For Example

Data Character =A [binary representation 10000001]

Bitmap Data bytes:

Byte1=10000011
Byte2=10000111
Byte3=10001111
Byte4=10001111

After mapping data character bitmap data changes to-

Bitmap Data bytes as:

Byte1=10000001
Byte2=10000100
Byte3=10001100
Byte4=10001110

Since only last two lsb's are used this won't bring the noticeable change in the image. Retrieval process is the inverse of mapping ie the bits of data character that are mapped onto the last two bits of bitmap data bytes are

retrieved again in the specific order and rearranging them on the basis of fact that the least bits of the first bitmap data byte will be the last in the data character being inserted
Bitmap Data bytes after mapping

Byte1=10000001
Byte2=10000100
Byte3=10001100
Byte4=10001110

Retrievel process will be in the order-

Least bits of Byte 4 =10
Least bits of Byte 3 =00
Least bits of Byte 2 =00
Least bits of Byte 1 =01

order will be 4 3 2 1 ie. 10000001 which is the original data character.

IX. LIMITATIONS

9.1.There are limitations on the use of STEGANOGRAPHY . As with encryption, if party A wants to communicate secretly with party B they must first agree on the method being used. without their agreement the technique can not be performed because support is needed from both the parties as this is a case of security.

9.2. Due to the size of the medium being used to hide the data. In order for STEGANOGRAPHY to be useful the message should be hidden without any major changes to the object which is being selected for embedding the data inside it.that means for example if you are using image for hiding the data then that image should have space larger than that of data to be inserted.

X. CONCLUSION

There is a relatively high use of stegonagraphy on the Internet, and the creation of stegonagraphy monitoring and detection systems is important. Although.till now I am only able to perform a research, on few techniques and types of steganography. my finding of material on the work being generated in the field of Steganography is Capable enough to explain that what is steganography and for what purpose it is implemented and how it can be implemented . in this paper I have concentrated on new technique of digital steganography which can be implemented on bmp images.

XI. FUTURE SCOPE

The research paper undertaken definitely has to offer some new concept with respect to data security. With growing demand and new technology arising, there can be lot of improvements that can be made in the field of steganography as in the particular research paper the various techniques are being discussed but the main importance is being given to LSB method of image hiding as it is the easiest way to perform steganography on bmp images. the modern day steganography (digital steganography) can be implemented on all format of images and some algorithms can be made to make this technique much more Reliable and easier for normal user to implement.

REFERENCES

[1] Katzenbeisser, S. and Petitcolas, F(1999).: Information hiding techniques for steganography and digital watermarking. Artech House Books
[2] C. Rey and J.L. Dugelay(2002). A survey of watermarking algorithms for image authentication.EURASIP Journal on Applied Signal Processing, 6:613–621.
[3] N. Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE Security & Privacy Journal 2003.
[4] Frank Hartung, Martin Kutter(July 1999), "Multimedia Watermarking Techniques", Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103
[5] Edin Muharemagic and Borko Furht ―A Survey of watermarking techniques and applications 2001.