Secure Data hiding using Steganography and transmission through Simple Mail Transfer Protocol

Vadivelu A
Assistant Professor – II, Department of Computer Science and Engineering, Velammal Engineering College, Chennai, India.
Email:vadivelu@velammal.edu.in
Hemaraj G
Department of Computer Science and Engineering, Velammal Engineering College, Chennai, India
Email:hemaraj1277@gmail.com
Kushal Chand K
Department of Computer Science and Engineering, Velammal Engineering College, Chennai, India
Email:kushalkataria5@gmail.com

----------ABSTRACT----------

Steganography is a form of security technique. It is the science and art of hiding the existence of a message between sender and intended recipient. Steganography has been used to hide secret messages in various types of files, including digital images, audio and video. Different applications have different requirements of the steganography technique used.

Steganography is the technique of hiding a message in an image file (cover image) so as not to be known by people who do not have permission to access the image file. This insertion utilizes the smallest bit of pixel units in an image file (Least Significant Bit). This type of insertion uses the binary of the ASCII code of a character. This paper presents a new idea of robust steganography using bitwise-XOR operation between stego key image-pixel LSB (Least Significant Bit) value and secret message- character ASCII-binary value. The stego key image is shared in dual-layer using odd-even position of each pixel to make the system robust. Due to image sharing, the detection can only be done with all the image shares.

Apart from only encrypting the message this method also used to transfer the encrypted message within a group or to the person who needs to access the content of the message. Only the people who encrypted the message has the option to send the message.

Keywords - **image steganography, image processing, Simple Mail Transfer Protocol, Least Significant Bit**

I. INTRODUCTION

Today the communication systems have been turned into digital ones to transmit data over the networks. The advancement of networking and digital communication has presented serious threats to secure data transmission. Information security is essential for various purposes, such as confidential data transfer, access control system for Digital content distribution, secret data storing and protection of data alteration, and media database systems. The information security is classified into information hiding and cryptography. The information hiding can be considered as one of the most important algorithms. At this time the type of file that is very often used is an image file. Many types of image file formats can be used depending on the compression used. The PNG format has become the most widely used format. Steganography is used as a way to exchange information by utilizing the weakness of the human eye in viewing image files.

Some of the data-hiding methods are watermarking, steganography, and cryptography. In spite of very high levels of security provided by various advanced cryptographic techniques, illegible nature of `cipher text' easily draws attention of adversaries and, thus, may result in failure of communication.

Steganography is used for embedding high amount of data in covers (image, video, audio etc.). Image based covers are the most frequently used covers. Steganography is divided into spatial and frequency domains. Spatial domain involves embedding of secret message by direct modification of intensity of cover image pixels. The transformed domain coefficients are altered to embed secret data in frequency domain methods. Spatial domain methods require less computational complexity and provide higher embedding capacity than frequency domain methods.

After the message being encrypted the person can transfer the message in PNG format to others within the group through e-mail. The person who encrypted the message can select list of recipients who should receive the message. The protocol used to transfer the mail is Simple Mail Transfer Protocol (SMTP). A common weakness of LSB embedding is that sample value changes asymmetrically.

II. PROPOSED SYSTEM

The proposed system makes use of Least Significant Bit algorithm to embed the message to be transferred with a

PNG image file. The embedded image is known as stego image. This can now be transferred to the receiver by sending the stego image via e-mail. On the receiving end the user has to decode the stego image to read the original message communicated.

2.1Encoding and Decoding the message through Least Significant Bit Algorithm

Least Significant Bit (LSB) is one of the techniques to implement steganography. LSB is a widely used steganography algorithm [5]. LSB utilizes the right far bit of the byte array that make up pixels in an image file. In the order of bits in a byte, there are bits called LSB and some are called MSB. Steganography technique using Least Significant Bit (LSB) modification method is the simplest technique, simple approach to insert information in a digital image (medium cover). Convert an image from GIF or BMP format, which reconstructs the same message as the original (lossless compression) to PNG that is lossy compression, and when it is done it will destroy the hidden information in the LSB [13]. The LSB bit becomes the place where the bit value of the binary arrangement of an information is inserted, because the change in the value only changes 1 bit higher or 1 bit lower than the previous value. So, when the byte values change, the changes that occur in the pixel will not be too meaningful. The LSB algorithm utilizes the weakness of the human eye to see very small colour changes in the stego image produced.

III. ALGORITHM

A. LEAST SIGNIFICANT BIT

A 3x3 pixel grayscale image will be inserted and the information is character 'a'.

a = 0110 0001

and here are 3 x 3 images represented in binary numbers.

11010011 11000010 01000011

10110110 10101100 11001011

11101001 11010011 10101000

The LSB of each pixel in the image will be replaced by the byte of character ‘a’.

11010010 11000010 01000010

10110111 10101100 11001011

11101001 11010010 10101000

Source code

```
a int messageLength = mess.length();
int imageWidth =img.getWidth()
int imageHeight= img.getHeight()
int imageSize = imageWidth * imageHeight;
if(messageLength * 8 + 32 > imageSize) {
    return;
    }
    embedInteger(img, messageLength, 0, 0);
    byte b[] = mess.getBytes();
    for(int i=0; i<b.length; i++)
    embedByte(img, b[i], i*8+32, 0);


    int maxX = img.getWidth()
    int maxY = img.getHeight()
    int startX = start/maxY
    int startY = start - startX*maxY
    int count=0;
    for(int i=startX; i<maxX && count<32; i++) {
    for(int j=startY; j<maxY && count<32; j++) {
        int rgb = img.getRGB(i, j), bit = getBitValue(n, count);
        rgb = setBitValue(rgb, storageBit, bit);
    img.setRGB(i, j, rgb);
                count++;}
        }
```

ASCII

ASCII is an international standard in information exchange. This standard is used by computers to represent a character. ASCII code has a composition of binary numbers of 8 bits. Starting from 00000000 to 11111111 with a total combination of 256.

Overview of SMTP

SMTP is one of the most common and popular protocols for email communication over the Internet and it provides intermediary network services between the remote email provider or organizational email server and the local user accessing it.

SMTP is generally integrated within an email client application and is composed of four key components:

1. Local user or client-end utility known as the mail user agent (MUA)
2. Server known as mail submission agent (MSA)
3. Mail transfer agent (MTA)
4. Mail delivery agent (MDA)

SMTP works by initiating a session between the user and server, whereas MTA and MDA provide domain searching and local delivery services.

The SMTP model is of two type:

1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method is used within an organization. A SMTP client who wants to send the mail will contact the destination’s host SMTP directly in order to send the mail to the destination.

The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP. The client SMTP is the one which initiates the session let us call it as client- SMTP and the server SMTP is the one which responds to the session request and let us call it as receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

IV. SAMPLE IMAGES

V. CONCLUSIONS AND FUTURE WORK

From all the experiments that have been made to PNG image by using LSB can be listed the conclusion as follows:

a. LSB is one technique that can be used to insert information in an image.

b. The size of the message does not exceed the size of the cover image.

c. The larger image resolution, the larger message or information can be inserted.

d. RGB images can hold more information or messages than with Grayscale images of the same resolution.

Apart from encrypting only textual data. The future work will be also to encrypt images and files of medium sizes using images.

VI. ACKNOWLEDGMENT

The authors gratefully acknowledge the works of K. Stefan, P. Fabien, Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt.

REFERENCES

[1] K. Stefan, P. Fabien A.P., "Information Hiding Techniques for,Steganography and Digital Watermarking" , Artech House , London, 2000.

[2] Westfield A, Pfitzmann A. Attacks on Steganographic systems. In: Pfitzmann A, ed. Proc. of the 3 rd Int'l Workshop on Information Hiding. LNCS 1768, Berlin: Springer-Verlag, 1999:61-76.

[3] Abbas Cheddad , Joan Condell, Kevin Curran and Paul Mc Kevitt"Digital Image Steganography , Survey and Analysis of Current Methods".