CONFIDENTIAL COMMUNICATION AND SECRET DATA STORING BY EMBEDDING FILES–SURVEY

Author: V. Shanthi , Godithi Ramya Sree, Prof. Senthil Kumaran.U,VIT University,Vellore,632014.

ABSTRACT:

In this current world every secret message transmissions are done through internet. Most people in this world blindly believe that their messages sent through internet are safe and secure and it's our responsibility to sustain their hope. We can secure our information by covering data within some other files (audio,image).

Digital Steganography is the art of hiding data within data. Steganography is a process that involves hiding a message in an appropriate carrier file i.e an image or an audio file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message.

By embedding the input file with the secret message by working on the LSB, we can produce the files containing the hidden message. The output file is transmitted over the internet; even if the intruder gets the file he cannot retrieve the hidden message without the steganography algorithm using java. Even the mere existence of the secret message is invisible. This can be more secure when compared to other techniques for secret message transmission.This technique provides more security by providing XOR operations and then embedding into the file. The audio or video or image file can be reused since the key is varying according to the XOR operations. It involves encoding and decoding of files in audio or image file[1][5][6].

Keywords: Least Significant Bit,Steganography,XOR Operations

Abbreviation:LSB,ELSB

I. Introduction:

In this project we have taken the any file as the secret message and the cover object can be audio file(music file or any audio file) or image file. Both the files should be converted into bit stream. The bit stream of the voice to be sent secretly should be encoded using XOR operations and then the audio or image steganography is performed. The file is then passed over the internet. Even the presence of the hidden message is invisible. For receiver the "invisible" message of steganographic methods will not be suspicious to anyone. steganography prevents an unintended receiver from suspecting that the data is present. And the security of classical steganography system stays on secrecy of the data encoding system[9].

Related Works

1.Least Significant Bit algorithm

Audio Steganography:

Audio steganography is hiding a secret data inside an audio file, such that the audio file won't be changed. Figure-1 shows the process involved in audio steganography, the secret message is embedded using LSB method in the audio cover file and the stego audio file is created. This stego file is similar to the carrier file and is transmitted . figure 2 shows the reverse process of extracting the secret information from the stego fileat receiver side

Any type of file can be hidden into the audio file but the size of the audio file should be 8 times greater than the secret file. Because each bit in the secret file needs one byte of the audio file and each byte consists of 8 bits. So each byte of secret file needs 8 bytes of audio file.

Figure 1

Embedding Process

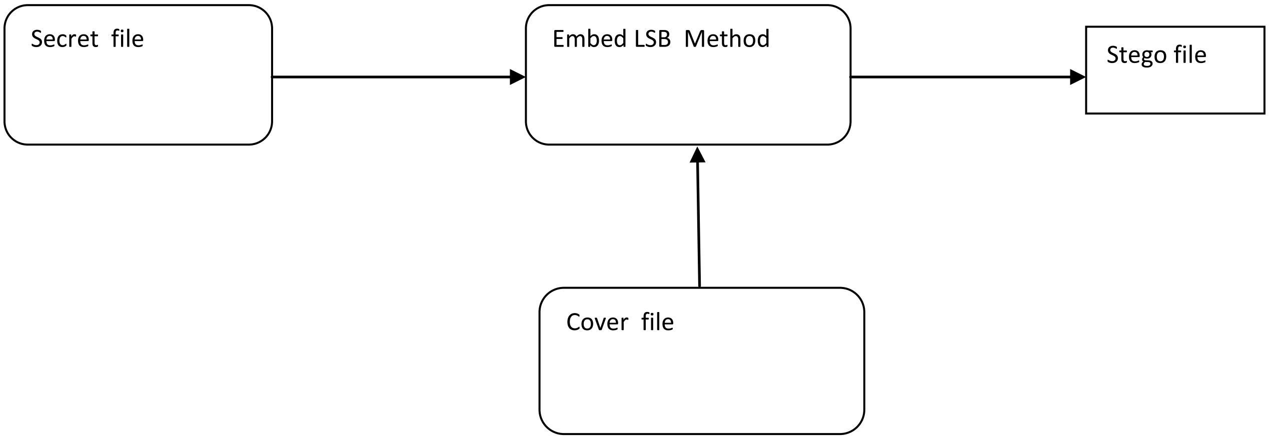


Figure 2

Extracting Process

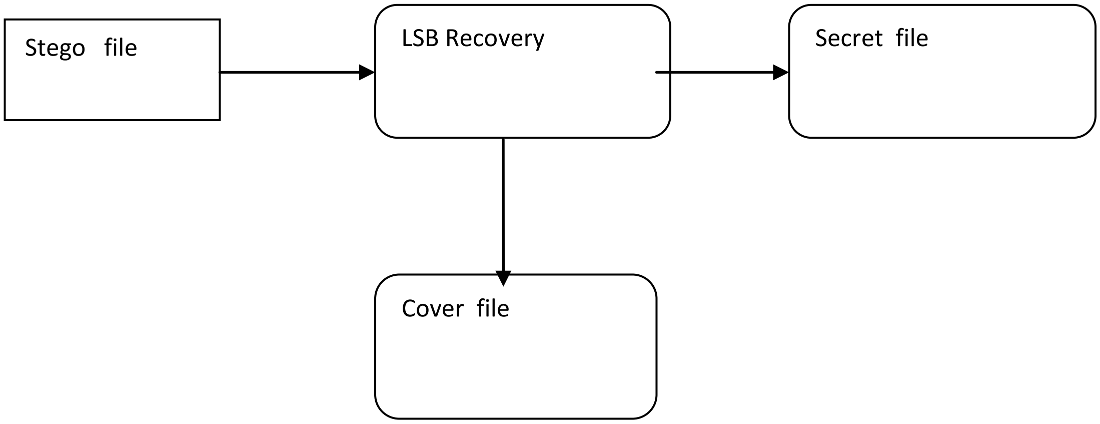


Image Steganography: This LSB technique works good for image steganography. An image file is a file that shows different colors and intensities of light on different areas of an image.It is easier to hide information in high quality and resolution as the image is large in size. The 24 Bitmap image is more suitable for hiding information.Only last bit is used for storing secret message in case of 8-bit image(gray images), but in case of 24-bit image,we can store 1 bits in each red,green and blue color componets in each of the component.Suppose that we have three adjacent pixels (9 bytes) with the RGB

10010101 00001101 11001001

10010110 00001111 11001011

10011111 00010000 11001011

When the number 301, whose binary representation is 100101101 embedded into the least significant bits of the image.Now we are embedding the number 301 in RGB components by Changing the LSB (where bits in bold have been changed)

10010101 0000110**0** 1100100**0**

1001011**1** 0000111**0** 11001011

10011111 00010000 11001010

The number 301 was embedded into the grid, 4 bits only needed to be changed according to the embedded message.[1]

2. LSB Embedding in Images

Detection of hidden data in a 24-bit color image embedded through LSB Steganography. This method uses RGB(Red Green Blue) cube and uses two terms "unique pair" and "close color pair". In a unique pair only one component from RGB differs by one, In a close color pair, each component value i.e all the RGB colors differs by one . Two consecutive pixels (R1, G1, B1) and (R2' G2, B2) are close if

$|R1-R2|=1$ and $|G1-G2|=1$ and $|B1-B2|=1$

Two consecutive pixels (R3, G3, B3) and (R4, G4, B4) are unique if only one of the following is true

$|R3-R4|=1$ or $|G3-G4|=1$ or $|B3-B4|=1$

A variant of the closest color pair method is proposed by Hernandez-Chamorro et af ,where ratios R and R' are calculated for the test image and the payload image respectively as:

$R=P/U$ $R'= P /U$,where

P and U are number of close color pairs and unique pairs in test image P' and U' are number of close color pairs and unique pairs in payload image. A threshold (t) on ratio R/R' is used as a criterion for determining type of image. Generally value of t is taken to be 1.1

```
if (R/R’ >= t) then
 Cover Image
else
Stego Image
Endif    [2]
```

3.Enhanced Least Significant bit algorithm.

Audio Steganography:

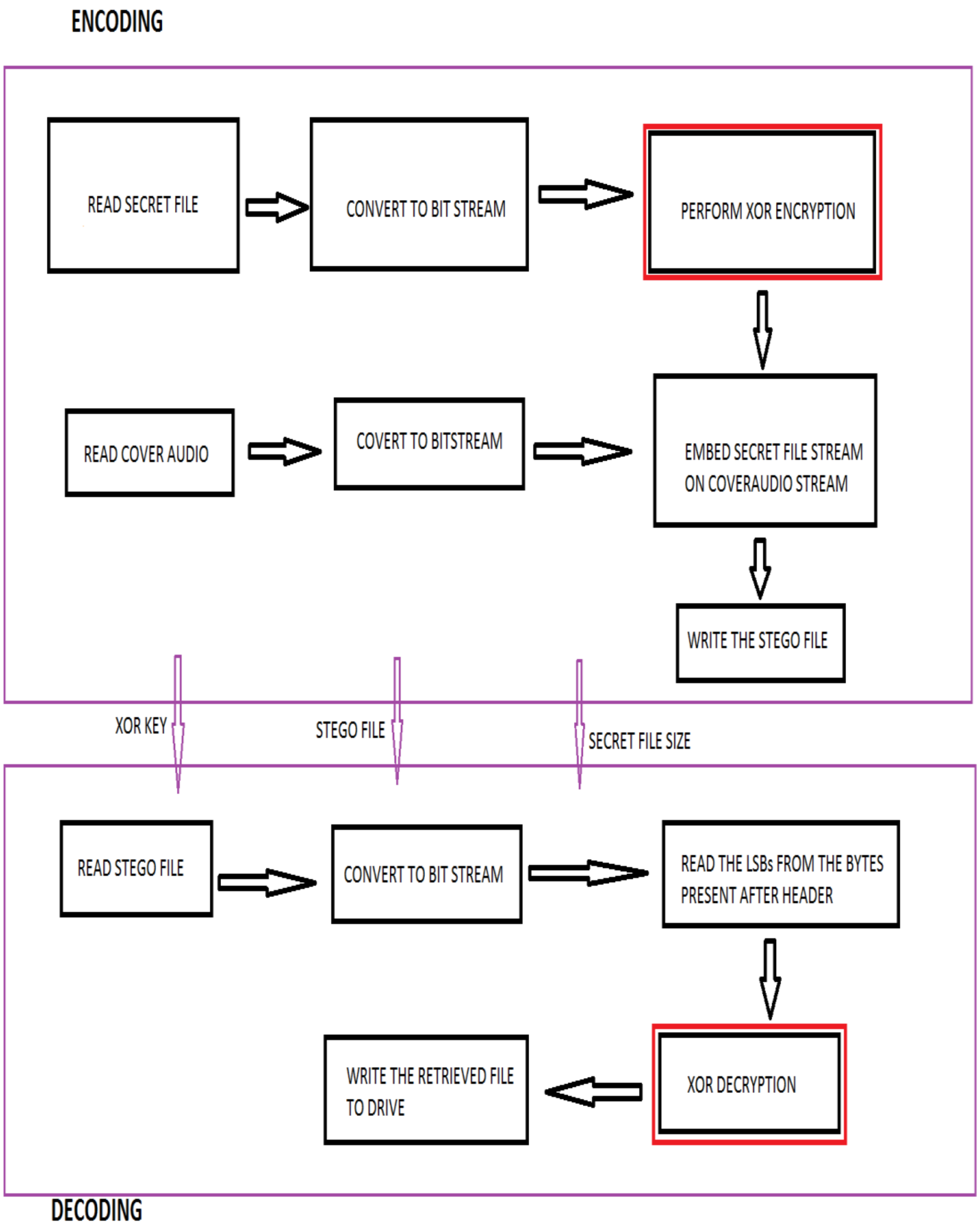
Security can be further increased by performing XOR encoding and XOR decoding operations.Even though if the intruder come to know the existence of secret message in the object file(audio file or image file) that is transmitted over the internet, they cannot obtain the secret message without knowing the algorithm that is used for encoding and decoding.

Main advantage of this ELSB algorithm is that audio file can be reused again and security can also be increased

Image Steganography:

In case of 24-bit image, LSB algorithm all the three components are used for embedding secret message.But in ELSB algorithm only one component among three components(Red, Green, Blue) can be used to store 3 bits of secret message.Since only one component is changed we can minimize the distortion level in the image.Security can be further increased by performing XOR encoding and XOR decoding operations same as in audio steganography.

Main Advantage of Enhanced Least Significant Bit minimizes the distortion level of the image file and security can also be increased [3].



An Improved LSB based Image Steganography

Embedding an image file into the other image we require two files. One is the color image of any object also known as object file. Another is carrier file the message to be hidden. The images can be in BITMAP or JPEG format, but more preferable is BITMAP as it is the profitable format available. Later, the cover image is divided into three planes they are Red, Green and Blue(RGB).In Encoding, object file is inserted for the adjustment of the images with a Least Significant Bit substitution in the order of 2 within Red, 2 with in Green and 4 with in Blue planes. That is, 2 message bits in Red plane, 2 in Green Plane and 4 in Blue Plane. The technique used is LSB. Least Significant Bit is simple approach for embedding data in carrier file .We use image as cover file. The LSB's of the cover file is changed as we need to embed the data ,we need to hide. For example, the image of data uses LSB to hide first eight bytes of three pixels.

Pixels:

(00100111 10101011 111000001)

(11101001 00011001 001110100)

(00101010 11111110 111000111)

Data : 10101010

Result Pixels:

(00100111 10101010 111000001)

(11101000 00011001 001110100)

(00101011 11111110 111000111)

In improved LSB technique, image converted into bits and these bits are substituted in the cover image. Choosing to insert bits in Red,Green and Blue planes reduces noise generated by the use of other methods like Bit Sequence Generator etc. This method uses various processes like edge tapering to smoothen the image to reduce the impact of LSB based pixel. Techniques used are uniform insertion of the simple text images, bit slicing, encoding, decoding, de-interleaving, etc. for the successful implementation of the algorithm.[4]

Study and Analysis

Steganography is a characteristic of object oriented programming. Because an object can only be associated with data in predefined classes,the object can only know about the data it needs to know about. There is no possibility that someone could access the secret data . Therefore, all the data that is not required by an object can be said to be hidden.Confidential Communication and hiding data is the process that involves hiding a message in a carrier file i.ean image or an audio file. The cover file can be sent to the receiver without knowing that it has a hidden data.

M.S. Sutaone said in his paper on Least Significant Bit shows the process involved in audio steganography, the secret message is embedded using LSB method in the audio cover file and the stego audio file is created. Each bit in the secret file needs one byte of the audio file and each byte consists of 8 bits. So each byte of secret file needs 8 bytes of audio file. Roopali Goyall, Sakshi Vijay2, Shweta Agarwae, V. Laxmi4, MS Gauri said in the paper on Difference Steg-Analysis for LSB Embedding in Images , Detection of hidden data in a 24-bit color image embedded through LSB Steganography. This method uses Red Green Blue cube and uses two terms "unique pair" and "close color pair". In a unique pair only one component from RGB differs by one, In a close color pair, each component value i.e all the RGB colors differs by one . Harish Kumar , Anuradha mentioned in the paper of Enhanced Least Significant bit algorithm for audio and image steganography by performing XORencoding and XORdecoding operations. Any Intruder come to know the existance of secret data in the object file(audio file or image file) that is transmitted over the internet, they cannot obtain the secret message without knowing the algorithm that is used for encoding and decoding.

Amritpal Singh,Harpal Singh wrote in the paperAn Improved LSB based Image Steganography technique for Red Green and Blue images says thatLSB insertion is simple approach for embedding data in a cover file .We use image as the cover file here. The least significant bits of the cover image pixels are changed as we need to embed the data to be hidden[5][7].

S.NO	TITLE OF THE PAPER	METHODS USED	ADVANTAGES AND LIMITATIONS
1.	**Least Significant Bit algorithm for audio and image Steganography**	Here methodology used is Least Significant Bit Technique .The LSB bits of the secret file are hidden in to the Cover file LSB bits	1.Less complexity of the algorithm compared with others techniques. 2. Low robustness, due changes of the LSB destroy the coded watermark
2.	**Different Steg-Analysis for LSB Embedding in Images**	Method used is RGB Cube and two terms unique pair and close color pair to identify if a file is cover file or stego file	The property of the ratio between close color pairs and unique pairs is exploited in the above mentioned algorithm for differentiating between a natural image and a stego image
3.	**Enhanced Least Significant bit algorithm for audio and image steganography**	XOR Encoding and XOR Decoding techniques are used	Audio file is reused again and security can also be increased. Enhanced Least Significant Bit minimizes the distortion level
4.	**An Improved LSB based Image Steganography Technique for RGB Images**	The secret message is hidden in the RGB plane using Least significant bit method	1.Enhance security from attacks 2.Cover files cannot be reused

Conclusion

In current years ,it has been proven that many technologies are competing with their own methodologies on any platform that went beyond the expectations. In this paper ,we elaborated on all the important methodologies discovered ,used in data hiding by comparing and contrasting the techniques with advantages and limitations of every method provided in the papers.

Major comparison was based on the methods that were suitable in contributing the efficient method and also based on technology platform .

Among all the methods that have been mentioned above we concentrate and implement the project in Enhanced Least Significant Bit algorithm, in Audio Steganography- Security can be further increased by performing XOR encoding and XOR decoding operations. Even though if the intruder come to know the existence of secret message in the object file(audio file or image file) that is transmitted over the internet, they cannot obtain the secret message without knowing the algorithm that is used for encoding and decoding. Advantage of this ELSB algorithm is that audio file can be reused again and security can also be increased. Enhanced Least Significant Bit algorithm in image steganography- In case of 24-bit image, LSB algorithm all the three components are used for embedding secret message. But in ELSB algorithm only one component among three components(Red, Green, Blue) can be used to store 3 bits of secret message. Since only component is changed we can minimize the distortion level in the image security can be further increased by performing XOR encoding and XOR decoding operations same as in audio Steganography.Advantage of Enhanced Least Significant Bit minimizes the distortion level of the image file and security can also be increased[8][10].

References:

This section will include technical books and documents related to design issues.

1. IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893 www.IJCEM.org IJCEM www.ijcem.org 40 Least Significant Bit algorithm For Audio and Image Steganography.

2. 201O International Conference On Computer Design And Appliations (ICCDA 2010) Topic: Difference Steg-Analysis for LSB Embedding in Images.Author: Roopali Goyall, Sakshi Vijay2, Shweta Agarwae, V. Laxmi4, MS Gaur5 Department of Computer Engg. Malaviya National Institute of Technology Jaipur, India.

3. IEEE-20180 Topic: Enhanced LSB technique for Audio Steganography.Author: Harish Kumarl , Anuradha2 1. Associate Professor(CSE), Krishna Engineering College, Ghaziabad .E-mail - harishtaluja@gmail.com 2. Lecturer, MIET, Meerut,

4. 2015 IEEE Topic: An Improved LSB based Image Steganography Technique for RGB Images.Author: Amritpal Singh Dept. of Computer Science and Engineering Guru Kashi University Talwandi Sabo, India and Harpal Singh University College of Computer Applications Guru Kashi University Talwandi Sabo, India

5. 2015 Third International Conference on Image Information Processing. Topic: LSB Modification based Audio Steganography using Trusted Third Party Key Indexing Method. Author: Vipul Sharma and Ravinder thakur, L R Institute and Technology.India

6. 2015 IEEE Topic: A New Image Steganography Method in Spatial Domain Using XOR.Author: Kamaldeep Joshi Pooja and Dhankhar ,University Institute of Engineering and Technology Maharishi Dayanand University, Rohtak

7. IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893 www.IJCEM.org IJCEM www.ijcem.org 40 Enhanced Least Significant Bit algorithm For Image Steganography

8. 2015 IEEE Topic: Image Based Steganography Using LSB Insertion Technique. Author: M. S. Sutaone Assistant Professor in E &T/C Dept PIET's College of Engineering, Pune and M.V. Khandare PIET's College of Engineering, Pune

9. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February2013 An Overview of Digital Image Steganography.R.Poornima and R.J.Iswarya M.Tech.,,Sastra university,India.poorniajar@gmail.com M.Tech., Department Of Advanced Computing,

10. 2015 Third International Conference on Image Information processing
LSB Modification based Image stegonagraphy using third party key
Indexing method,Vipul Sharma,Ravinder Thakur,Dept. of computer science engineering, L.R. Institute of engineering and technology,Solan,India.