International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Significance of Steganography and Implementing it using LSB Technique

Komal Bhaware[1], Shruti Sawakhande[2], Prof.J.Mathew[3]

[1-3]BE Scholar, Department of Computer Engineering, Datta Meghe College of Engineering, New Mumbai, Maharashtra, India

---

Abstract – *Steganography is a type of art of hiding the fact that communication is taking place. Different type of file formats can be used, but most popular are digital image. There are many techniques for hiding secret information in images.Steganography is practice of hiding sensitive information. Steganography is confused along with cryptology because both are similar as used for protecting information. The difference between them is that steganography is for hiding information. If any person sees object he or she will have no idea that something is hidden inside that object and person will not try to decrypt the information.*

Key Words: Steganography, encryption algorithm, decryption algorithm

1. INTRODUCTION

Steganography has been derived from Greek word steganos, meaning secret and graphy means writing. Steganography is type of hidden writing. It consists of invisible ink on paper. Cryptography is scrambling message into code to obscure its meaning. These two technologies can be used individually or combined. For example first encrypting message then hiding in another file for transmission. Steganography exploit human perception, senses of human are not trained to loom for files which have information that is hidden inside of them. Even though there are programs that are available that can do what is called Steganalysis. The use of this method is to hide file inside another file. When information or file is hidden inside carrier file, the data is encrypted with password.

2. LITERATURE SURVEY

2.1 Image Steganography

The Encoding process:

Steganography technique used is LSB technique.

Offset of image is taken from header.

Offset is left as it has to preserve integrity of header and fro next byte then start encoding process.

For encoding first take input carrier file an image file then direct the user to select text file.

The Decoding process :

This method is used to convert from encoding scheme.

It works opposite to encode. It accepts encoding of encoding string to decode it and return original string.

2.2 Audio Steganography :

The Encoding process :

Technique used is LSB coding.

Audio file consists of data in bytes.

For encoding message first find length of string.

Offsetting original file, from which encoding process should start is by default set to 500. It is because the WAV file has header in initial offset and if that header is tampered with then the destination file will not be able to access header inappropriate format.

Encode length which can be up to 256 characters in first 8 bytes of audio file. This will assist in decoding process.

Take each character from message string and convert it into byte and then change LSB of next 8 bytes of audio file as per each bit of character type.

Repeat same procedure till message string gets exhausted.

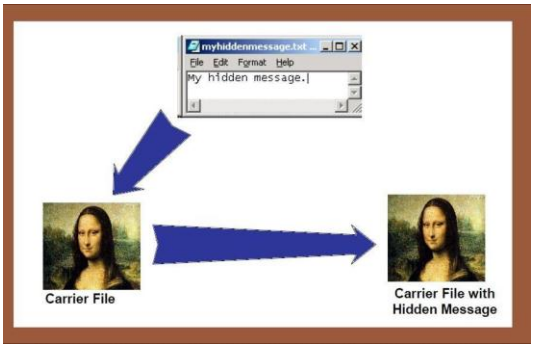
The Decoding process:

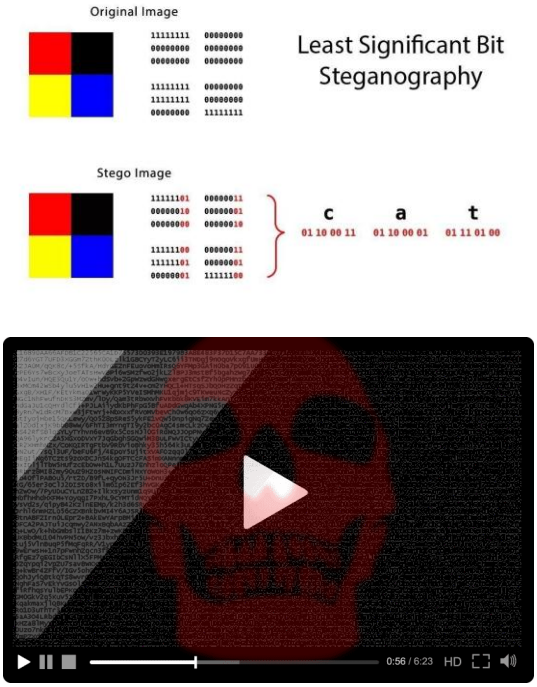
Select from offset that were specified at sending side then take LSB of next 8 bytes to get length of message that will help to get encoding message only from next 8 * Length of bytes of audio file. Continue this process till length of string is reached.

Hence finally we get hidden message from received audio file into provided text box.

Thus we have achieved process of decoding message from audio file.

SUMMARIZED FINDINGS:





3. REQUIREMENT ANALYSIS

3.1 Functional Requirement:

Support embedding of message data without constraints on format of data to be embedded.

Implement additional more complex embedding schemes.

Implement and embedding an extraction scheme that will utilize audio stream.

Develop more sophisticated steganalysis tool.

3.2 Non- Functional Requirement:

The application should be easy to use.

GUI should be clean intuitive and unambiguous.

The system should support appropriate formats.

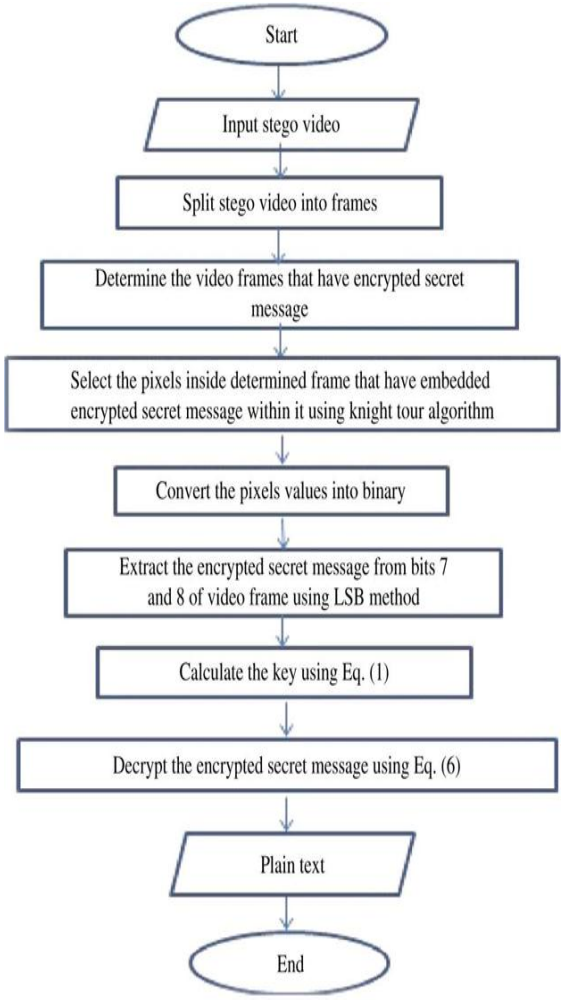
Extraction process should be fast.

Embedding process should be fast.

User should be able to select embedding scheme.

4. PROJECT DESIGN

Flow Chart



5. APPLICATIONS

Steganography is useful for storing sensitive data like hiding passwords within another file.

Network surveillance and monitoring systems will not flag message that contain steganographic data. If someone tried to steal important data they could conceal it within another file and send it an innocent looking email.

6. CONCLUSIONS

This tool can be useful to hide text message in image or audio file.

The message that is sent can be encrypted to support secured steganography.

This technology is easy to use and difficult to detect.

The more you know about its feature the more ahead you will be in game.

The scope of this project is implementation of steganographic tools to hide information consists of any type of information file and image file and path the user wants to save image.

7. REFERENCES

[1] L.Galdino1, A.Edwards2, M.Ionescu2, J.James2, W.Pelouch3, E.Sillekens1.

[2] D.Semrau1, D.Lavery1, R.I.Killey1.

[3] S.Barnes2 , P.Bayvel1 and S.Desbruslais2 1 Optical Networks Group, Dept. of Electronic & Electrical Engineering, University College London, UK 2 Xtera, Bates House, Church Road, Harold Wood, Essex.

[4] Al-Korbi, H.A., Al-Ataby, A., Al-Taee, M.A.: Highly efficient image steganography using Haar DWT for hiding miscellaneous data, I(JJCIT).