Concealing Information

**Mr. Chavan sagar[1], Mr. kadam dhiraj[2], Mr. shete pravin[3], Miss. Rijawana Mulani[4]
Miss. Sukanya Madane[5],Prof. Kiran Jagtap[6]**

[1-5]BE Student, Dept. computer Science, Satara College of Engineering And Management, Limb, Satara, Maharashtra, India
[6]Professor, Dept. computer Science, Satara College of Engineering And Management, Limb, Satara, Maharashtra, India

---***---

Abstract - *Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images/audio there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image /audio steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which Steganography techniques are more suitable for which applications.*

Key Words: steganography, complex, secret message .etc

1. INTRODUCTION

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from thinking that the information even exists. Steganography become more important as more people join the cyberspace revolution.

Steganography is the art of concealing information in ways that prevents the detection of hidden messages Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis. Some modern computer printers use steganography, including Hewlett Packard and Xerox brand color laser printers. The printers add tiny yellow dots to each page.

Characteristics of Steganography

Steganographic techniques embed a message inside a cover. Various features characterize the strength and weaknessof methods. The importance of each feature depends on the application.

Capacity

The notion of capacity in data hiding indicates the total number of bits hidden and successfully recovered by the stegosystem.

Robustness

Robustness refers to the ability of the embedded data to remain intact if the stego-system undergoes transformation such as linear and non-linear filtering: addition of random noise; and scaling, rotation, and loose compression.

Undetectable

The embedded algorithm is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn. Un-detestability is directly affected by the size of the secret message and the format of content of the cover image.

Security

The embedded algorithm is secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the embedded algorithm and secret key.

2. LITERATURE SURVEY

1. Arup Kumar Pal, Kshiramani Naik, and Rohit Agarwal.The secret data embedding into image can be realized into two domains, i.e., spatial domain and transform domain. In this the secret data are embedded into the cover image by directly modifying each pixel value of the cover image itself.

2. Andik Setyono, De Rosal Ignatius Moses Setiadi.Important digital data should be secured so that they cannot be misused by others. Some techniques that are widely used are by hiding or encoding the data before the data is sent. Data

hiding techniques that are widely used are water, marking and steganography.

3. PROPOSED SYSTEMS

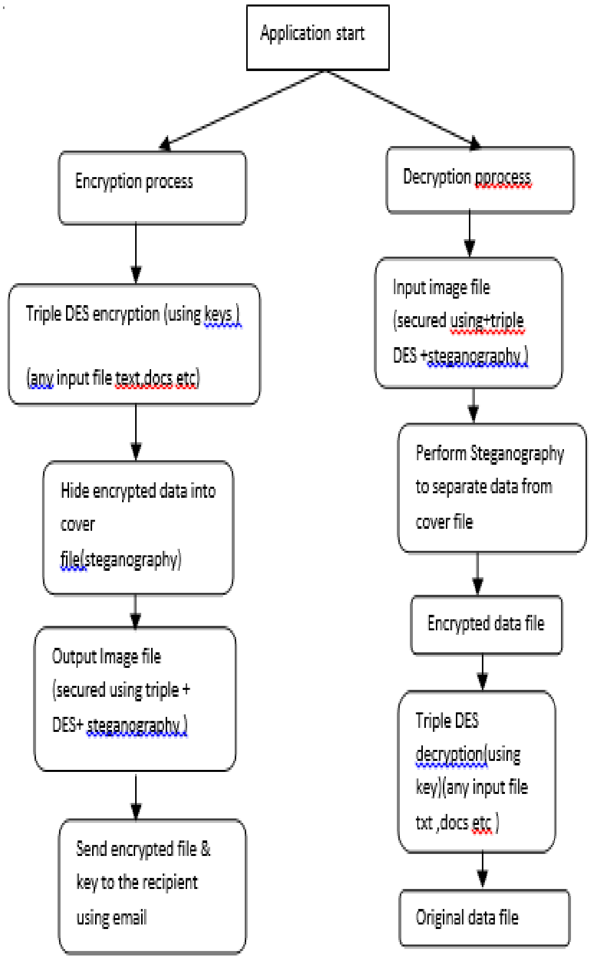

Fig-1: System Architecture

Figure shows the proposed system. In this figure, figure shows the working of the system. We are going to use 'TripleDES' algorithm to encrypt data. To access the image or audio file user will get one time password in the format of key. By using this key user can access the data easily. The uploaded data should be stored in the encrypted format while at the time of downloading; data should be in the decrypted format. By using one time password key, security of the system should be increased

4. 'TripleDES' algorithm used to encrypt data before applying steganography .

Definition - What does Triple DES mean?

Computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key.

Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. However, the DES algorithm was replaced by the Advanced Encryption Standard by the National Institute of Standards and Technology (NIST). Thus, the Triple DES is now considered to be obsolete. Yet, it is often used in conjunction with Triple DES. It derives from single DES but the technique is used in triplicate and involves three sub keys and key padding when necessary, such as instances where the keys must be increased to 64 bits in length. Known for its compatibility and flexibility, software can easily be converted for Triple DES inclusion. The'refore, it may not be nearly as obsolete as deemed by NIST.

In.net framework there is The 'System.Security.Cryptography' namespace provides cryptographic services, including secure encoding and decoding of data, as well as many other operations, such as hashing, random number generation, and message authentication.

5. CONCLUSIONS

This steganography application software provided for the purpose to how to use any type of image/audio formats to hiding any type of files inside there. The master work of this application is in supporting any type of picture/audio without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in picture/audio to hide the file.

6. REFERENCES

[1] Arup Kumar Pal, Kshiramani Naik, and Rohit Agarwal A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity (The International Arab Journal of Information Technology, vol. 16. No. 1. January 2019)

[2] Andik Setyono, De Rosal Ignatius Moses Setiadi.Imperceptible Improvement of Secure Image Steganography based on Wavelet Transform and OTP Encryption using PN Generator (IOP Conf. Series: Journal of Physics: conf. Series 1196(2019)012031)