VIGNAN'S
Foundation for Science, Technology & Research
(Deemed to be UNIVERSITY)
-Estd. u/s 3 of UGC Act 1956

ONLINE
Driving your future

Project Synopsis

Name	Sujay Biswas
USN	231DD01434
Elective	Computer Science and IT
Title of the Project	STEGANOGRAPHY

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 knowing the hidden information but it is 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 includes an array of secret communication methods that hide the message from being seen or discovered.

Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images. The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding

- **What is Steganography?**

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.

- **Problem Statement**

A problem statement in steganography typically focuses on the need to securely conceal the existence of a secret message within a carrier file (like an image, audio, or video) without visually altering the carrier, ensuring that only authorized parties can extract the hidden information while evading detection from potential adversaries.

- Hiding the message:

The primary challenge is to embed a secret message within a seemingly normal file in a way that does not reveal the presence of the hidden data to the naked eye or casual observation.

- Maintaining carrier quality:

When embedding data into a carrier file, the goal is to minimize any distortion or degradation in the quality of the carrier file to avoid suspicion

• Objectives of the Project

The primary objective of a Steganography is to develop a system that can effectively hide sensitive data within seemingly ordinary files like images, audio, or video, thus concealing the existence of the secret information from unauthorized users while allowing authorized parties to extract it securely; essentially, the goal is to achieve covert communication by embedding secret messages within a carrier file without noticeably altering the carrier file itself.

Key aspects of a Steganography project objective include:

- Data Embedding**:**

To develop algorithms that can seamlessly embed secret data (text, files, etc.) into a cover file (like an image) without significantly impacting its visual quality.

- Data Extraction:

To design methods for extracting the hidden data from the stego-file (modified cover file) using a secret key only accessible to authorized recipients.

- Security:

To ensure the embedded secret data remains hidden from casual observation and can resist attempts to detect its presence.

- Robustness:

To develop techniques that can withstand potential manipulations or distortions to the stego-file without compromising the integrity of the hidden data.

- Efficiency:

To optimize the process of embedding and extracting data to minimize computational overhead and file size increase.

- **Research Methodology**

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file.

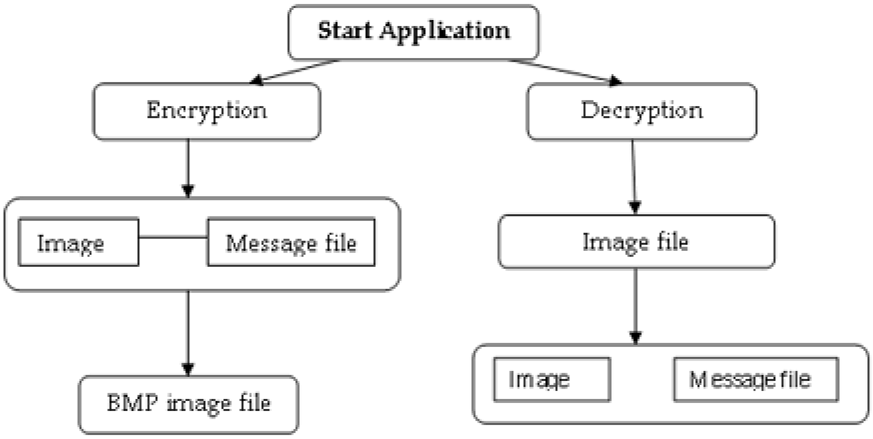
This project has two methods – Encrypt and Decrypt.

In encryption the secrete information is hiding in with any type of image file.

Decryption is getting the secrete information from image file.

- **Graphical representation**

The graphical representation of Steganography system is as follows:



- **Software Requirements:**

1. .NET Framework 3.5
2. Front End : C#
3. Operating System: Microsoft Windows 7 or above

- **Hardware Requirements:**

Processor: Preferably 1.0 GHz or Greater.

RAM : 512 MB or Greater.

- ## Limitations

The limitations of steganography software include: limited data capacity within a carrier file, potential for image degradation when embedding large amounts of data, susceptibility to detection by steganalysis techniques, potential for misuse by malicious actors to hide harmful content, and increased processing time due to the complex embedding process; making it crucial to carefully select the appropriate steganography method based on the intended use case and security requirements.

Key limitations in detail:

- **Capacity constraints:**

The amount of data that can be hidden within a carrier file (like an image or audio) is limited, meaning large files may not be able to be fully embedded without noticeable distortion.

- **Image quality degradation:**

When embedding large amounts of data, the quality of the carrier file can be significantly impacted, making the hidden message potentially detectable by visual inspection or specialized steganalysis tools.

- **Steganalysis vulnerability:**

Advanced techniques can be used to detect the presence of hidden data within a file, potentially exposing the secret message.

- **Misuse potential:**

Malicious actors can exploit steganography to hide malicious code or sensitive data within seemingly innocent files, making detection and prevention challenging.