**MINI PROJECT – I**

**(2019-20)**

# STEGANOGRAPHY

# 

**SYNOPSIS**



**Institute of Engineering & Technology**

**Team Members**

Keshavi Aggarwal

(171500160)

Harshit Rai

(171500127)

Vanshika Shivani

(171500373)

## Supervised By

**Mr. Pankaj Sharma**

**(Asst. Professor)**

**Department of Computer Engineering & Applications**

**ABOUT THE PROJECT**

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word steganographyis derived from the Greek words ‘STEGANOS’(meaning *hidden*or c*overed*) and the Greek root ‘GRAPHIS’(meaning *to write*).

Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography -- called *hidden text* -- is often encrypted before being incorporated into the innocuous-seeming *cover text* file or data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content.

Steganography is practiced by those wishing to convey a secret message or code. While there are many legitimate uses for steganography, malware developers have also been found to use steganography to obscure the transmission of malicious code.

Forms of steganography have been used for centuries and include almost any technique for hiding a secret message in an otherwise harmless container. For example, using invisible ink to hide secret messages in otherwise inoffensive messages; hiding documents recorded on microdot -- which can be as small as 1 millimeter in diameter -- on or inside legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information.

**MOTIVATION**

All the industries and companies desire to protect their work from theft. In modern days internet has been the mode through which information of any level of confidentiality is shared.

The more the information is vital the more is the risk of its theft. For that steganography is the best way to maintain its privacy.

**FUTURE PROSPECTS**

Our ability to discover hidden information during our investigations is vital, especially as new and innovative methods continue to evolve.  Most dangerous among these are those that employ hiding methods along with cryptography, thus providing a way to both conceal the existence of hidden information while strongly protecting the information even if the channel is discovered.

Many vendors provide excellent technologies for protecting the privacy of information for the desktop. In addition, many of the latest smart mobile platforms (Android and iPhone) include built-in cryptographic capabilities. What is more dangerous and difficult to discover/decipher are data hiding methods that exploit multimedia and protocol weaknesses to both hide and communicate covertly. These new techniques provide hybrid solutions that combine the best of cryptography with the best of steganography. The interest, innovation, and advancement of these threats continue to go unchecked for the most part.

**REQUIREMENTS**

1. **Hardware:**

* Laptop

1. **Software:**

* Latest version of Python
* GUI