SSGMCE	SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGG.	LABORATORY MANUAL
	PRACTICAL EXPERIMENT INSTRUCTION SHEET	
	EXPERIMENT TITLE : To demonstrate how attackers can hide sensitive data inside image files using steganography tools	
EXPERIMENT NO.: **SSGMCE/WI/IT/01/5IT08/6**	ISSUE NO. : 00	ISSUE DATE : 08.07.2025
REV. DATE :	REV. NO. :	DEPTT. : INFORMATION TECHNOLOGY
LABORATORY : Information Security System (5IT08)	SEMESTER : V	PAGE: 1 OF 5

1.0) AIM: To demonstrate how attackers can hide sensitive data inside innocent-looking files (images) using steganography tools

2.0) SCOPE:

- To understand the concept of **steganography** and how it differs from encryption.
- To learn how attackers can use steganography to secretly transfer information.
- To realize the importance of **forensics and detection techniques** in cyber law.

3.0) FACILITIES/ APPARATUS:

- **Windows PC**
- **OpenStego** (Free and open-source steganography tool)Download OpenStego

4.0) THEORY:

- **Encryption:**Converts a readable message (plaintext) into an unreadable format (ciphertext) using algorithms and keys.

Example: If you encrypt `HELLO` using a key, it may look like `X9a#1z`.

Anyone can see that an encrypted message exists, but they cannot read it without the key.

- **Steganography:**

Goes one step further by hiding the **existence** of the secret message.

A text file, for example, can be hidden inside an image, audio, or video file.

The cover file (e.g., a `.jpg` photo) looks normal to the human eye, but secretly contains

another message inside.

- **Comparison – Encryption vs. Steganography:**

Feature	Encryption	Steganography
Visibility	Encrypted text is visibly scrambled	Hidden message not visible
Detection	Easy to detect but hard to read	Hard to detect without special tools
Example Use	Secure emails, banking transactions	Covert communication, hiding malware

- **Use Cases in Real Life:**

Attackers may hide malicious code or stolen data in harmless-looking files.

Hackers may secretly pass instructions inside images on social media.

Security experts also use steganography for watermarking digital images to prevent piracy

5. Steps / Procedure

Step A: Prepare Secret Message

Create a text file named secret.txt.

Write a message inside, e.g., “Meeting at 10 PM. Don’t share.”

Save and close the file.

Step B: Hide Data using OpenStego

Open OpenStego.

Select Data Hiding option.

Input:

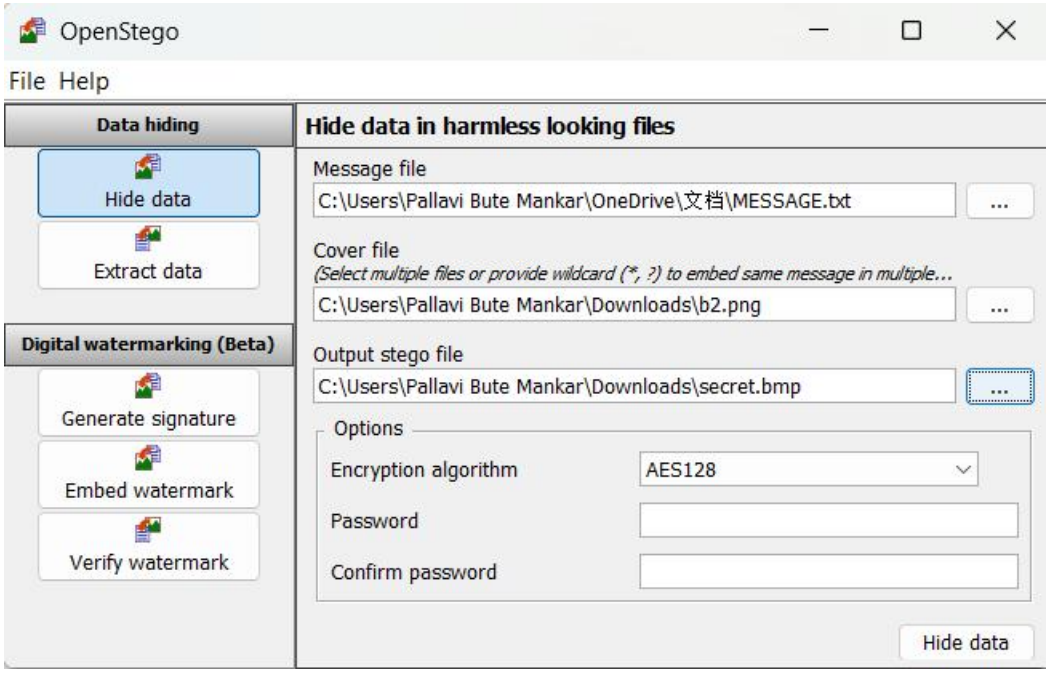
Message File → secret.txt

Cover File → Choose an image (e.g., photo.jpg)

Output File → stego.jpg

Click Hide Data.

A new file stego.jpg is created, which looks like a normal photo.



Step C: Verify Stego Image

Open stego.jpg in Windows Photo Viewer.

It should display like a normal picture, with no visible difference.

Step D: Extract Hidden Message

In OpenStego → Choose Extract Data.

Input File → stego.jpg.

Select Output Path

The hidden message (from secret.txt) will be recovered.

Image with hidden message

6. Observation / Output

In this practical we will observe that the image appears unchanged.

However, the secret message can be extracted only using the steganography tool.

7. Result

We understood the working of steganography.

8.0) CONCLUSION:.

In this practical we realized how attackers may misuse such techniques for illegal activities.