Steganography Tool-2

OpenStego:

OpenStego is an open-source software application designed for steganography(the practice of hiding data within image files). This technique is especially useful for secure communication, where the goal is not just to encrypt the data but to conceal its very existence.

**Key Features**

1. **Data Hiding**  
   OpenStego allows users to embed data within image files, typically in formats like PNG or BMP. These formats are preferred because they are lossless, ensuring that the hidden data remains intact without any degradation.
2. **Digital Watermarking**  
   In addition to hiding data, OpenStego offers digital watermarking capabilities. This feature enables users to protect their intellectual property by embedding a watermark within an image. The watermark is subtle and doesn’t noticeably alter the image, yet it can be critical in proving ownership.
3. **Encryption**  
   OpenStego enhances security by offering encryption for the hidden data. Users can set a password, which is required to retrieve the embedded content. This ensures that even if someone knows data is hidden within an image, they cannot access it without the correct password.
4. **Open-Source**  
   As an open-source tool, OpenStego is freely available for anyone to use, modify, and distribute. Its source code is accessible, allowing users to verify the security measures or customize the tool to meet their specific needs.

**How to Use OpenStego**

* **Hiding Data**  
  To hide data, simply select an image file and the data file you wish to embed. Optionally, you can set a password to encrypt the hidden content. OpenStego will then generate a new image file that contains the hidden data, with no obvious changes to the image’s appearance.
* **Extracting Data**  
  To extract hidden data from an image, load the image file into OpenStego and enter the password if encryption was used. The software will then reveal the embedded file, ready for use.