Steganography Tool-1

Steghide:  
  
Steghide is a steganography tool that allows you to embed or extract hidden data within various file types, such as images, audio files, or text documents. Steghide uses strong cryptography and compression techniques to hide data securely. The hidden data can be encrypted using a passphrase, adding an extra layer of protection.  
  
**Key Features of Steghide**

* **File Types Supported**: Steghide supports JPEG, BMP, WAV, and AU file formats for hiding data.
* **Compression**: The data is compressed before being embedded, reducing the file size and making detection harder.
* **Encryption**: The hidden data can be encrypted using the Rijndael algorithm (AES) with a key size of 128 bits.
* **Embedding Options**: You can adjust various parameters like the embedding rate, which controls how much of the carrier file is used to hide the data.
* **No File Size Increase**: After embedding, the size of the cover file does not increase, which helps maintain its integrity and avoid suspicion.
* **CRC32 Checksum**: Steghide provides error detection through a CRC32 checksum to ensure the hidden data's integrity.

**Steghide Example  
1) Embedding a Secret File:**eg: steghide embed -cf cover.jpg -ef secret.txt -sf steganography.jpg -p "password"  
  
-cf cover.jpg: Specifies the cover file (the image in which data is hidden).

-ef secret.txt: Specifies the secret file (the data to be hidden).

-sf steganography.jpg: Specifies the output file with the embedded data.

-p "password": (Optional) Specifies the passphrase for encryption.  
  
**2) Extracting a Hidden File:**  
eg: steghide extract -sf stego.jpg -p "password"  
  
-sf stego.jpg: Specifies the stego file (the file containing hidden data).

-p "password": Specifies the passphrase if the hidden data was encrypted.