Assignment 2 Design work

Dimitry Rakhlei

Summary

The goal of this assignment was to become familiar with Steganography and to design a simple LSB stego application. I spent a good portion of my time developing a DCT based application based on a few papers I ended up reading. I had to stop working on that portion of the project because I was going down a rabbit hole where for every solution to a problem I had to solve two more.

I will keep working on the DCT application but here is the design for a simpler LSB based approach to stego with AES-256 encryption provided by the `pycrypto` library. Works with most file formats.

Installation & Usage

```
sudo pip install -r requirements.txt
```

The program only requires pycrypto, numpy, hashlib and Pillow to work. These libraries may already be present with a standard Linux installation.

After that the application can be used by calling the lsbit.py file from the command line via the python3 executable.

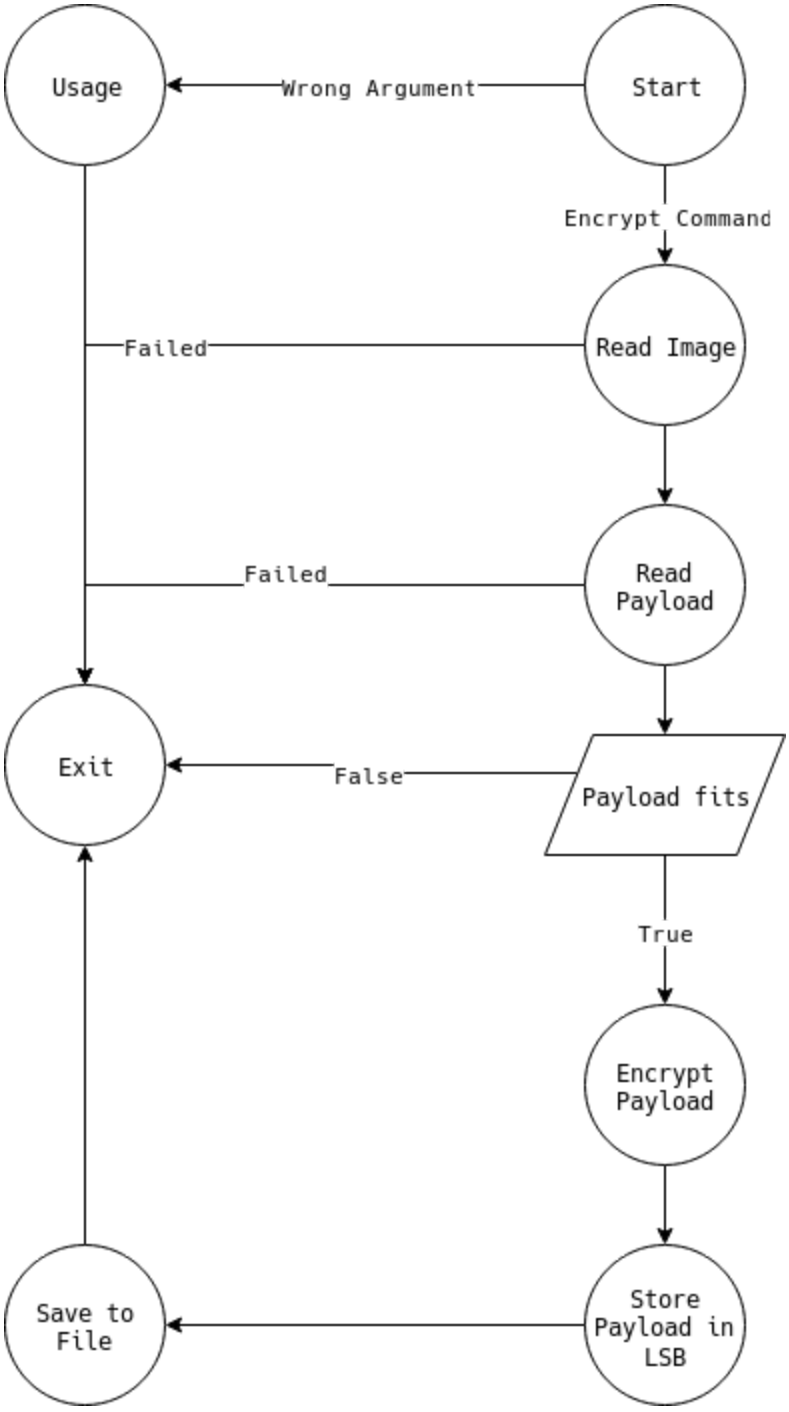
Example of typical usage:
python3 lsbit.py hide img/Colorchecker.bmp util.py mypassword

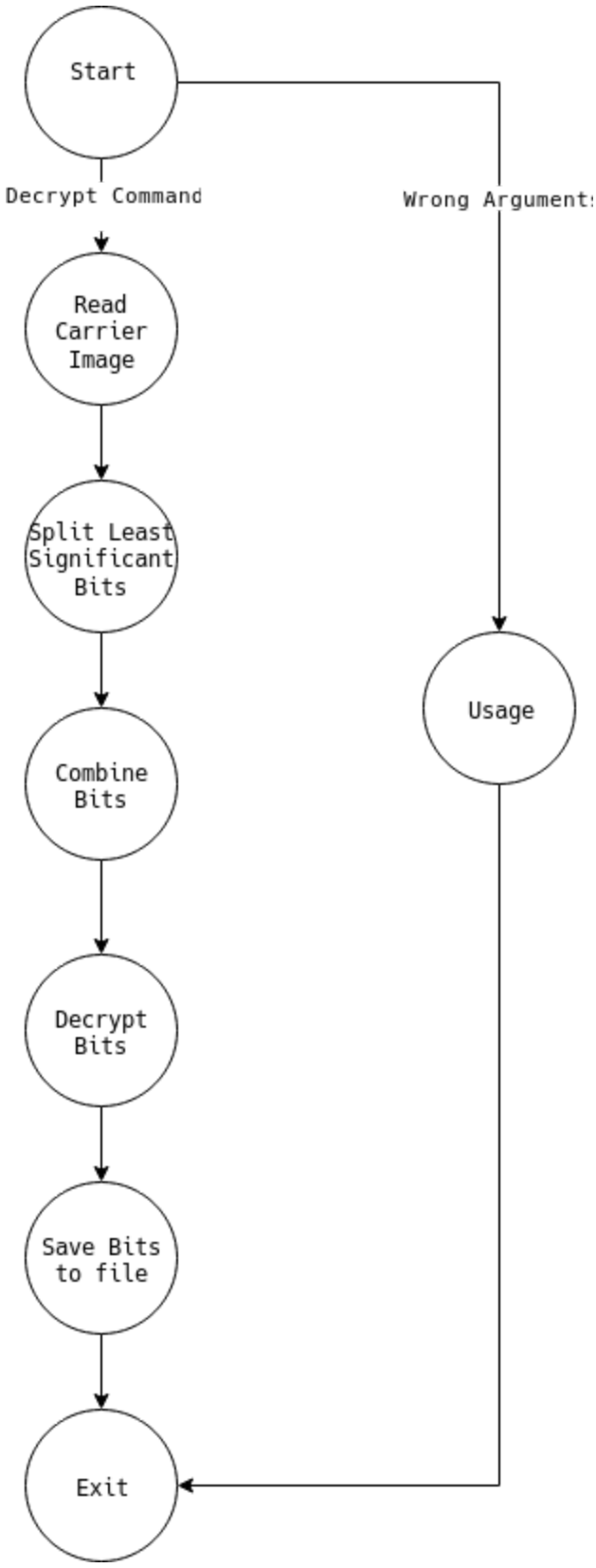
Pseudocode

```
Parse command line arguments
If command == "hide" Then do
      Read payload file
      Encrypt payload file with password
      Open carrier image specified
      Copy carrier image for output
      Foreach row of image Do
            Foreach column of image Do
                  Set the output image pixel LSB at [row, col] to payload
data
            Done
      Done
      Save output image.
Else If command == "reveal" Then do
      Open carrier image
      Store all LSBs
      Combine the LSB data
      Decrypt using password
      Write Data to file
EndIF

Done!
```

Design


Usage
Wrong Argument
Start
Encrypt Command
Failed
Read Image
Failed
Read Payload
Exit
False
Payload fits
True
Encrypt Payload
Save to File
Store Payload in LSB


Start
Decrypt Command
Wrong Arguments
Read Carrier Image
Split Least Significant Bits
Combine Bits
Decrypt Bits
Save Bits to file
Exit
Usage