PRODUCT FUNCTIONS

The main purpose of the StegSleuth tool is to assist students of the Polytechnic University of Puerto Rico who participate in Capture the Flag (CTF) competitions.

StegSleuth will be a tool for steganography that will offer the following functions:

* Find hidden payloads in a carrier.

The payload is extracted from the carrier using the algorithms provided.

* Hide payloads in a carrier.

The payload is embedded in the carrier using the algorithm provided.

* Encrypt payloads to hide in a carrier.

Encrypt payloads that are going to be embedded in a carrier.

* Decrypt hidden payloads in a carrier.

Decrypt payloads that are extracted from a carrier.

* Compare carriers to see if there are changes.

Compare carriers to verify if there is any hidden hash.

In Figure ??, the relationship between the system requirements can be observed. Also, Figure ?? shows the use case diagram that models the functionalities of the system in different use cases.

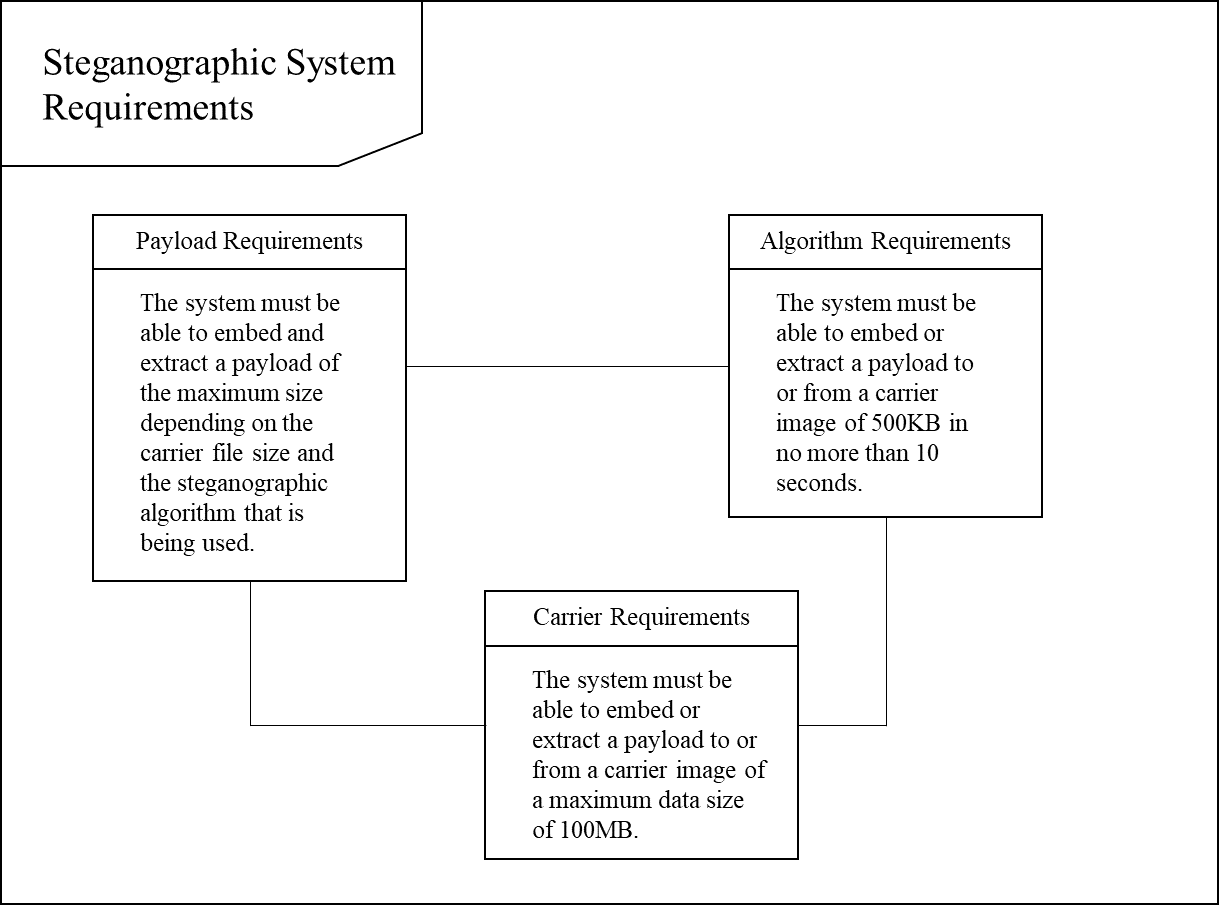


Figure ?? Requirements Diagram

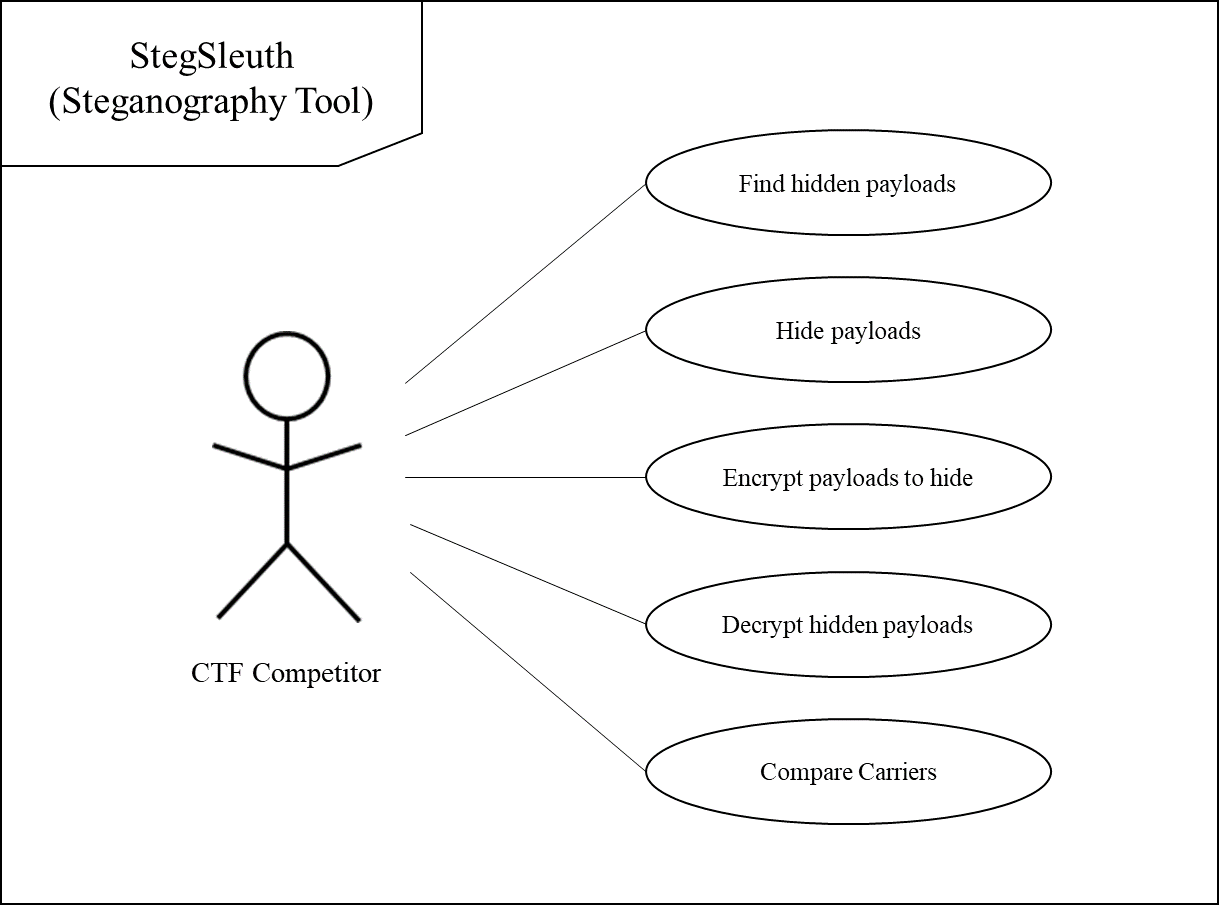


Figure ?? Use Case Diagram

USER CHARACTERISTICS

This tool’s target demographic will be cybersecurity Capture the Flag competitors. The users should be able to utilize all of the functions of the system at their convenience. Said users should have knowledge in the field of steganography and cryptography and may be of any age or academic preparation. With this preparation they should be able to decide which cryptographic and steganographic algorithms they will be using to solve their problem. In addition, they must know how to operate the Linux operating system (OS).

\* In steganography the **payload** is the data covertly communicated and the **carrier** is the signal, stream, or data file that hides the payload.

\* Operating System (OS)

https://www.pabloyglesias.com/mundohacker-esteganografia/

https://hackernoon.com/simple-image-steganography-in-python-18c7b534854f