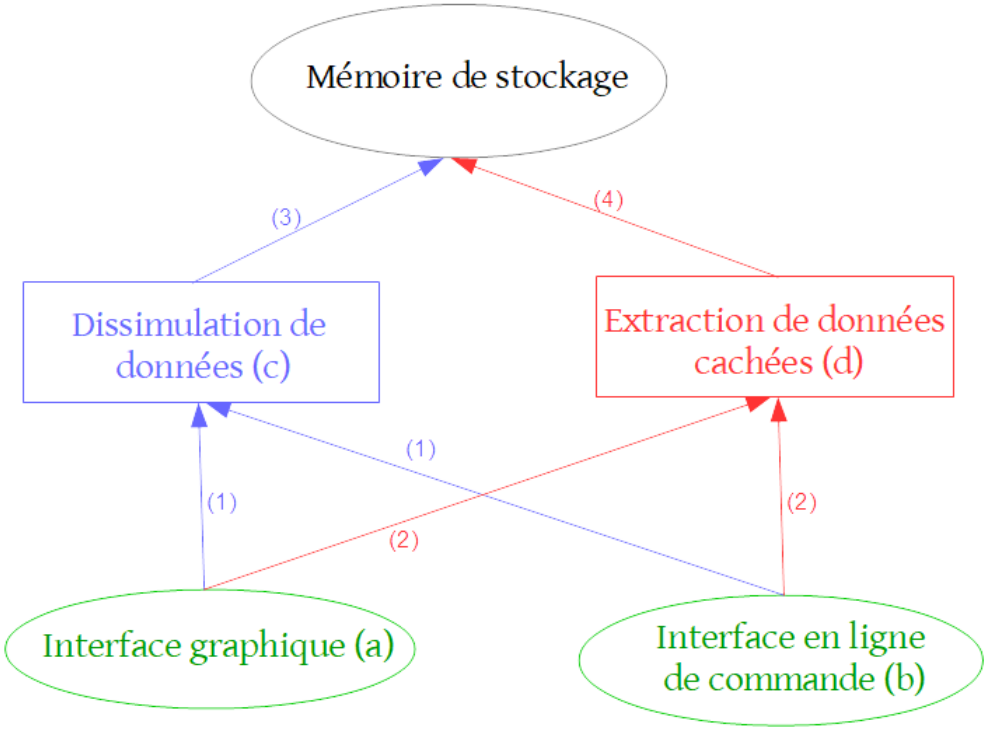

Liste des modules et de leurs fonctionnalités

a) **Interface graphique** : interface permettant à l'utilisateur de choisir avec la souris parmi les deux fonctionnalités possibles de l'application. Il peut dissimuler des données dans un fichier (dont le type et le format sont pris en charge par l'application). Ou bien, il peut extraire les données cachées dans un fichier (s'il en dissimule).

b) **Interface en ligne de commande** : interface ressemblante à celle graphique mais qui permet à l'utilisateur de manipuler l'application avec le terminal.

c) **Dissimulation des données** : ce premier module implémente plusieurs fonctionnalités :
- Compatibilité : le format du fichier "hôte" choisi par l'utilisateur est vérifié, pour savoir s'il est bien pris en charge par l'application.
- Proposition des algorithmes de stéganographie : en fonction du type et du format du fichier "hôte" ainsi que de la taille des données à cacher, un ou plusieurs algorithmes seront proposés.
- Insertion des données cachées dans l'hôte : écriture du fichier hôte dans lequel les données du fichier à cacher ont été insérées selon l'algorithme choisi par l'utilisateur.

d) **Extraction des données** : ce deuxième module implémente aussi plusieurs fonctionnalités :
- Compatibilité : le format du fichier "suspect" choisi par l'utilisateur doit être examiné afin de vérifier sa compatibilité avec l'application.
- Déterminisation : on recherche si le fichier suspect contient effectivement des données cachées. Cette déterminisation permet de savoir si un fichier a été utilisé par notre application dans le module *Dissimulation des données (c)*. Si le fichier suspect contient des données cachées, l'utilisateur choisira le chemin des données à extraire.
- Extraction : écriture des données cachées présentes dans le fichier analysé (si le fichier suspect en contenait véritablement).

Liste des informations qui circulent entre les modules

1) — fichier hôte

— fichier à cacher
— chemin et nom du fichier à créer, qui dissimulera les données à cacher et ayant l'apparence de l'hôte.

2) — fichier suspect à analyser

3) — fichier hôte contenant les données cachées

4) — fichier résultant, représentant les données cachées