

# Are New Technologies an issue for society?

Clément CAUMES & Mehdi MTALSI-MERIMI

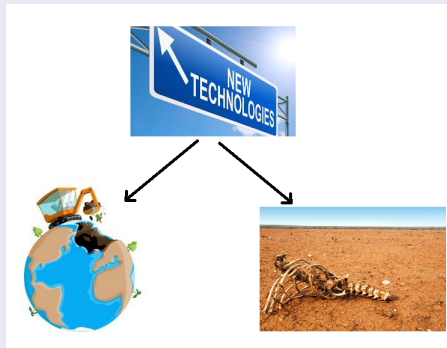
UFR des Sciences Versailles - M1 Informatique

Semestre 2

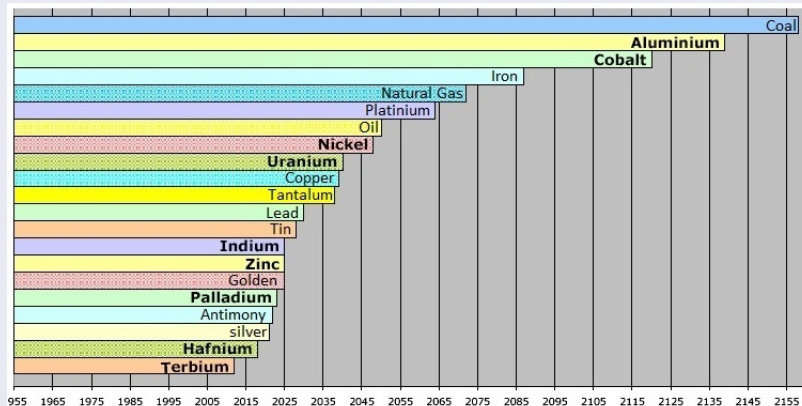
## Issues of resources

Increase of population, demands and productions induce :

- Resource overexploitation
- Extinction of rare animals and plant species



## Date of exhaustion of mineable resources



<http://terresacree.org/ressources.htm>

## Sustainable development = solution ?

- Development of the economy
- Development of the social aspect
- Preservation of the environment



Introduction

A curb for our planet

An impact for a social perspective

Conclusion

# PHONE ADDICTION

## THE NEW DRUG THAT IS KILLING AN ENTIRE GENERATION



Introduction

A curb for our planet

An impact for a social perspective

Conclusion

# PHONE ADDICTION

## THE NEW DRUG THAT IS KILLING AN ENTIRE GENERATION



## Demande du client

Réaliser un logiciel de stéganographie permettant à des personnes lambdas de communiquer sans que l'on soupçonne que leurs communications soient en réalité compromettantes.

- Cacher des données dans des fichiers de type image, audio et vidéo.
- Faire l'extraction automatique des données cachées du fichier à analyser.
- Gestion de plusieurs formats et diversité dans les algorithmes proposés.
- Proposition d'une bibliothèque partagée par deux interfaces différentes, une graphique et une en ligne de commande.











## Exemple

Alice choisit de cacher **message.txt** dans un fichier BMP  
**photo.bmp** et veut obtenir le fichier **piece\_jointe.bmp** après la

## Algorithmes de stéganographie

- Least Significant Bit (LSB)
- End Of File (EOF)
- Metadata
- End Of Chunk (EOC)
- Junk Chunk

## Besoin

Nécessité d'obtenir les informations de l'insertion pendant l'extraction impose une "signature".

## Signature StegX

- Identificateur de la méthode (1 octet).
- Identificateur de l'algorithme (1 octet).
- Taille du fichier caché (4 octets).
- Taille du nom du fichier caché (1 octet).
- Nom du fichier caché (entre 1 et 255 octets).
- Mot de passe (64 octets).



## Least Significant Bit

- Modification des bits de poids faible des octets de données de l'hôte.

## Avantage

L'utilisation de cet algorithme n'augmente pas la taille du fichier résultat en fonction de la taille du fichier caché.

## Inconvénient

Le fichier à cacher doit être assez petit pour pouvoir le cacher intégralement dans le fichier hôte.



## End Of File

- Écriture des données à cacher après la fin officielle du fichier hôte.

## Avantage

Il n'y a pas de limite de taille pour cacher le fichier.

## Inconvénient

L'utilisation de cet algorithme augmente considérablement la taille du fichier résultat par rapport au fichier hôte.



## Metadata

- Écriture des données à cacher dans des blocs de données spécifiques qui ne modifieront pas les données originales.

## Avantage

Il n'y a pas de limite de taille pour cacher le fichier.

## Inconvénient

L'utilisation de cet algorithme augmente considérablement la taille du fichier résultat par rapport au fichier hôte.





## End Of Chunk

- Écriture des données à cacher après les différents chunks interprétables du fichier hôte. Ces données seront non reconnus et donc ignorés.

## Avantage

Il n'y a pas de limite de taille pour cacher le fichier.

## Inconvénient

L'utilisation de cet algorithme augmente considérablement la taille du fichier résultat par rapport au fichier hôte.



## Junk Chunk

- Écriture des données à cacher dans un chunk appelé "junk" : les données ne seront pas interprétées

## Avantage

Il n'y a pas de limite de taille pour cacher le fichier.

## Inconvénient

L'utilisation de cet algorithme augmente considérablement la taille du fichier résultat par rapport au fichier hôte.



## Description des modules

- Vérification de la compatibilité des fichiers.
- Proposition des algorithmes de stéganographie.
- Insertion des données.
- Détection de l'algorithme de stéganographie.
- Extraction des données.

## Exemple

Avec la vérification de la compatibilité des fichiers, il s'agit d'un format **BMP non compressé**.

## Description des modules

- Vérification de la compatibilité des fichiers.
- **Proposition des algorithmes de stéganographie.**
- Insertion des données.
- Détection de l'algorithme de stéganographie.
- Extraction des données.

## Exemple

- Grâce au module Proposition des algorithmes de stéganographie, les spécificités du format de `piece_jointe.bmp` ont été déduites.
- Les algorithmes **EOF**, **LSB** et **Metadata** sont proposés.
- Alice choisit l'algorithme **EOF**.

## Description des modules

- Vérification de la compatibilité des fichiers.
- Proposition des algorithmes de stéganographie.
- **Insertion des données.**
- Détection de l'algorithme de stéganographie.
- Extraction des données.

## Exemple

Lors de l'insertion de Alice, l'algorithme EOF sera utilisé où les données de l'hôte, la signature StegX suivies des données du fichier à cacher seront écrites dans `piece_jointe.bmp`.

## Description des modules

- Vérification de la compatibilité des fichiers.
- Proposition des algorithmes de stéganographie.
- Insertion des données.
- Détection de l'algorithme de stéganographie.
- Extraction des données.

## Exemple

Après que Alice ait fini la dissimulation, Bob va déduire les spécificités du fichier `piece_jointe.bmp` et déduire les informations sur le fichier caché `message.txt`.

## Description des modules

- Vérification de la compatibilité des fichiers.
- Proposition des algorithmes de stéganographie.
- Insertion des données.
- Détection de l'algorithme de stéganographie.
- **Extraction des données.**

## Exemple

L'algorithme EOF sera utilisé pour extraire les données du fichier caché de message.txt.

## Problème

Si Oscar connaît la stéganographie, il peut utiliser un éditeur hexadécimal en voir en clair les données cachées.

## Solution

L'utilisation d'une méthode de protection des données est ajoutée :

- Données à cacher XORées avec une suite pseudo-aléatoire générée à partir du mot de passe (chiffrement par substitution polyalphabétique).
- Données à cacher mélangées (chiffrement par transposition).



## Lecture et écriture de fichiers : endianness en fonction des formats

- Little endian et big endian selon les formats.
- Travail de recherche poussé pour chaque format et pour chaque algorithme de stéganographie.

## Format MP3

- Format compressé utilisant des algorithmes de compression complexes.
- Étude des versions des formats (MPEG 1 Layer III, MPEG 2 Layer III).
- Étude des versions de formats de métadonnée (ID3 version 1, ID3 version 2).

## Bilan logiciel

- Faire de la stéganographie sur des fichiers image, audio et vidéo (insertion et extraction). ✓
- Plusieurs formats sont gérés et une diversité dans les algorithmes sont proposés. ✓
- Réaliser deux interfaces : ligne de commande et graphique. ✓
- ▶ Futures améliorations : nouveaux formats et algorithmes.

## Bilan humain

- L'équipe s'est efforcée à travailler de façon professionnelle et ordonnée.
- Projet de grande envergure qui a nécessité de diviser la conception selon les trois types de formats étudiés.