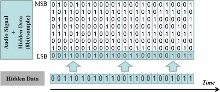
|  |
| --- |
| EPSI |
| Rendu stéganographie |
| Cours outil de chiffrement |

|  |
| --- |
| Saber FEKI JOAO MARTIN MATEUS FRANCK CAYZAK RAMLA BEN AMOR  08/04/2018 |

# Sujet :



On se propose de réaliser un site web permettant à deux personnes de s’échanger des informations (texte et image) de façon secrète en utilisant un principe de stéganographie. Le site web devra proposer les plusieurs services.

1. Création d’un fichier audio contenant un message texte caché La page propose à l’utilisateur de saisir son texte et de choisir un fichier audio servant de support. Lorsque l’utilisateur clique sur “Télécharger…”, le fichier audio de support est envoyé au site, le message y est dissimulé et l’utilisateur récupère son fichier audio contenant son texte.

2. Récupération d’un message dissimulé dans un fichier audio La page propose à l’utilisateur de choisir un fichier audio contenant un texte dissimulé. Lorsqu’il clique sur voir le texte, le fichier audio est envoyé au site et l’utilisateur voit le texte qui était dissimulé dans le fichier audio apparaître.

3. Création d’un fichier audio contenant une image cachée De la même manière qu’il est possible de cacher un texte, il est possible de cacher tout type d’information. Le site permettra également de dissimuler une image dans le fichier audio. On reprendra l’interface définie en 1 et on remplacera le champ texte par un autre bouton permettant le choix de l’image à dissimuler.

4. Récupération d’une image dissimulée dans un fichier audio Pour afficher l’image dissimulée, on procèdera de la même façon qu’en 2. Au lieu de “voir le texte” le bouton s’intitulera “Voir l’image”.

5. Remarques Pour des raisons de simplicité, on acceptera uniquement les fichiers audios au format WAV pour les fichiers audio support. Pour les images dissimulées tout format pourra être accepté. On veillera à ce que l’architecture permette une préservation la confidentialité des données échangées. Le nombre de bits de poids faible utilisé sur chaque sample devra être calculé automatiquement afin de minimiser la dégradation du fichier son support. Il se pourra par exemple qu’en fonction de la taille du message ou de l’image que l’on souhaite dissimuler l’opération soit impossible

# Stéganographie :

## Définition :

La stéganographie est l'art de la dissimulation. Elle consiste à cacher un message au sein d'un autre message anodin, de sorte que l'ignore l'existence même du secret.

Alors que la cryptographie repose sur le fait que le message ne soit pas compris, la stéganographie repose sur le fait que le message ne soit pas trouvé.

Nous allons étudier une technique de stéganographie appliquée à l'image, c'est-à-dire voire comment il est possible de cacher un message dans une image.

La stéganographie est l'art de la dissimulation : son objet est de faire passer inaperçu un message dans un autre message.

Elle se distingue de la [cryptographie](https://fr.wikipedia.org/wiki/Cryptographie), « art du secret », qui cherche à rendre un message inintelligible à autre que qui-de-droit.

Pour prendre une métaphore, la stéganographie consisterait à enterrer son argent dans son jardin là où la cryptographie consisterait à l'enfermer dans un coffre-fort — cela dit, rien n'empêche de combiner les deux techniques, de même que l'on peut enterrer un coffre dans son jardin.

C'est un mot issu du [grec ancien](https://fr.wikipedia.org/wiki/Grec_ancien) στεγανός / steganós (« étanche ») et γραφή / graphế (« écriture »).

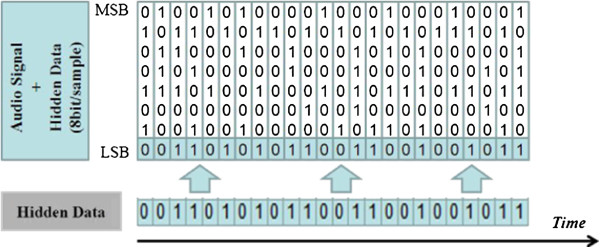
## La Méthode LSB (Least Significant Beat), ou méthode de bit de poids faible :

Cette méthode consiste à modifier le bit de poids faible des pixels codant l'image. Une image est un tableau constitué d'un ensemble de pixels.

Pour chaque pixel, on code la couleur avec trois octets : un pour le rouge, un pour le vert, un pour le bleu.

Chaque octet indique l'intensité de la couleur correspondante, sur un niveau allant de 0 à 255. 255 correspond à la couleur native.

Passer d'un niveau N à un niveau N – n, où n est suffisamment petit ne modifie que de peu la couleur, et c'est précisément sur cela que repose la méthode LSB.

Mise en pratique On prend un octet correspondant à l'une des trois couleurs d'un pixel, par exemple 01101011. Si on change les quatre derniers bits, cela ne change que de peu la couleur.

# Technologie choisie et utilisé :

Pour le choix de la technologie utilisé on est parti sur python est PHP car c’est assez facile de les mettre en place et parce que le groupe à trouver plus de facilité avec ces technologies et surtout que la documentation est plus facile à trouver et à comprendre

Python pour le cryptage la doc été super claire et il était très accessible

PHP html c’est la manière la plus facile pour faire les diffèrent interaction entre le code de cryptage et

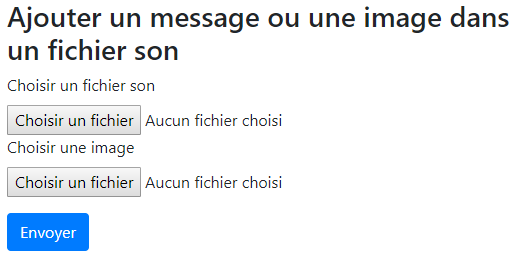
# Architecture de l’application développé :

L’architecture de l’application repose sur la simplicité le concept est le suivant on se base sur la méthode de bit de poids faible c’est-à-dire qu’on va prendre les derniers bits du fichier sur lequel ont crypté notre image ou texte et on le modifie pour y greffer le dit fichier en question.

Le travail est effectué en 2 étapes distincte :

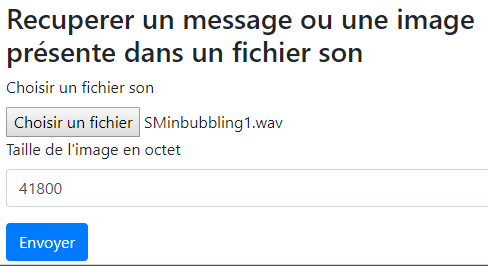
## 1ère étape : chiffrement

On a une page html qui dans laquelle on va mettre le fichier son et le texte ou l’image que l’on veut cacher à l’intérieur une fois sélectionné on va les uploader cette phase va faire appelle à la fonction écrite en python pour faire le chiffrement attendu et nous rendre le fichier crypter.



## 2 -ème étape : déchiffrement

On repart sur le même page mais cette fois pour la récupération on prend le fichier crypter et refait le même parcours mais cette fois pour le décryptage du fichier le Button uploade cette fois va faire appelle a la deuxième fonction dans notre fichier python qui est le décryptage qui cette fois nous donnera en output le fichier sons d’origine plus ce qui été crypter à l’intérieur.



# Mise en place de l’application :

La mise en place de l’application est assez simple pour faciliter l’utilisation a tout type d’utilisateur car il faut toucher un maximum de personne

Pour que l’application marche il faut installer un serveur apache qui lui va se charger de la création d’un Virtual host qui sera associé au dossier de l’application qu’il puisse faire appel aux différentes fonctionnalités de l’application de chiffrement en question