Remerciements

Nous tenons tout d'abord à remercier Dieu Le Tout Puissant et Miséricordieux, qui nous a donné la force et la patience d'accomplir ce Modeste travail.

En second lieu, la première personne que nous tenons à remercier du fond du cœur est notre cher Professeur encadrant M. Abdelaziz Doukkali, pour l'orientation, la confiance et la patience qui ont constitué un apport considérable pour mener ce travail à bon port. Qu'il puisse trouver par-delà même un vibrant hommage à sa haute personnalité, son professionnalisme et son sens charismatique, combien inébranlables.

Nous voudrions également saluer ses efforts colossaux pour nous mettre dans le bain et nous amorcer afin de démarrer cette esquisse. Nos remerciements s'adressent à juste titre à toutes les personnes auprès desquelles nous avons demandé conseil et aussi à tous ceux qui ont contribué de près ou de loin pour donner une ossature à ce travail par leurs propositions et recommandations. Nous espérons pouvoir un jour leur témoigner notre profonde reconnaissance.

Dédicace

A nos chers parents

A nos chers frères

A nos chères sœurs

A toute notre famille

A nos professeurs

A tous nos amis

A tous ceux qu'on aime

A tous ceux qui nous aiment

On dédie ce travail, à titre de reconnaissance.

Introduction

Nous vivons aujourd'hui l'avènement foudroyant d'une ère marquée par l'essor époustouflant des technologies de pointe. Parallèlement, les besoins interminables des utilisateurs ont également explosé via des moyens de communication tout azimuts. Ce constat est d'autant plus préoccupant que le nombre d'informations mises en circulation est devenu pléthorique, faisant ainsi naitre le besoin de sécurisation de ces échanges. La clé de voute portant remède pour préserver nos données s'avère être la cryptographie. Cependant, quiconque voit la circulation de data cryptée soupçonnera le contenu et se dira que ce n'est pas pour rien que ce message a été crypté et conclura que cela revêtirait une importance majeure, le poussant à tout pour en décortiquer le contenu.

C'est à ce juste titre que la stéganographie gagne du terrain. Méconnue du grand public, elle a toujours été confondue avec la cryptographie. Toutefois, chacune est une science à part entière et peuvent se mettre à disposition l'une de l'autre. La force de la stéganographie réside dans le fait que un curieux, avant même d'essayer de trouver du texte dans une image ou un support informatique, encore faut-il savoir qu'elle en contient.

Le présent projet se propose de mettre en exergue une implémentation de la stéganogrphie par camouflage de data dans une image, amalgamé à une cryptographie à clé partagée.

Pour étayer le bien fondé de nos propos, ce mémoire se propose donc de donner un aperçu général sur la stéganographie, avant d'enchainer avec les techniques et formes possibles, pour clore avec l'implémentation de notre idée de manœuvre.

I- État de l'art

1- Définition

La stéganographie est l'art de communication secrète. L'objectif étant de dissimuler un message secret dans un médium anodin (une image, une vidéo, un son..) de manière imperceptible.

Ce mot est issu du grec « Stéganô », qui signifie Je couvre et « Graphô » qui veut dire J'écris. Ainsi, on dissimule les informations que l'on souhaite transmettre secrètement dans un ensemble de données d'apparence anodine, ce que l'on appelle le cover ou le médium de couverture, afin que leur présence reste imperceptible. La science "oposée" porte le nom de stéganalise.

Le socle de sa force doit principalement sa robustesse à deux constats:

- nos sens (vue, ouïe) ne sont pas capables de détecter du changement infinitésimal dans une image ou un son,
- et de prime abord, nous ne savons pas à l'avance que tel support renferme de l'information cachée.

2- Historique

2.1- Stéganographie classique

L'avènement de la stéganographie remonte à l'Antiquité, tout comme la cryptographie. D'origine grecque, le mot stéganographie est apparu pour la première fois dans l'histoire vers 445 av J.-C, à travers les récits d'Hérodote.

Dans son œuvre l'Enquête1, Hérodote rapporta l'histoire de Histiée, conseiller du roi de Perse, qui incita son gendre Aristagoras, le roi de Milet, à se rebeller contre les Perses vers 500 av J.-C. Pour ce faire, il fit raser la tête de son esclave, lui tatoua le message sur le crâne, puis attendit la repousse de ses cheveux avant de l'envoyer à Milet. Une fois l'esclave arrivé à destination, il n'eut qu'à se faire raser la tête une deuxième fois, pour transmettre le message secret.

Plus loin encore, dans ce même ouvrage, on retrouve aussi l'histoire de Démarate en 480 av J.-C, qui réussit à déjouer le plan de Xerxès, roi du perse, visant à envahir la Grèce. Démarate, ancien roi de Sparte, fut au courant du plan d'invasion de Xerxès. Il décida alors de prévenir les Grecques, ceci en leur envoyant un message gravé sur le bois d'une tablette d'écriture recouverte de cire, et donc d'apparence

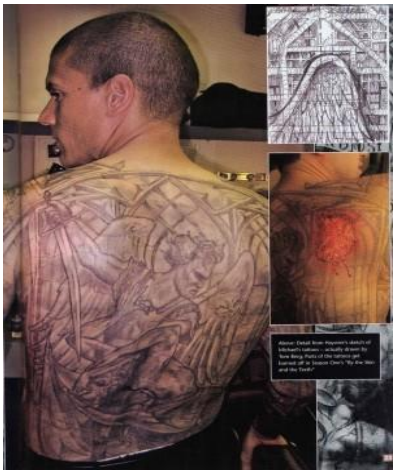
extérieure vierge. Au fil des siècles qui se sont écoulés depuis Hérodote, différentes formes de stégano-graphie, de plus en plus évoluées, ont été utilisées dans le monde:

- En Chine antique, on écrivait les messages secrets sur de très fins rubans de soie, qu'on enrobait ensuite dans des petites boules de cire. Ces boules, ensuite avalées par le messager, pouvaient voyager jusqu'au destinataire, d'une manière totalement discrète.
- Plus subtile encore, l'invention de l'encre sympathique fut l'un des procédés stéganographiques le plus utilisé. L'encre sympathique, ou l'encre invisible, est un procédé chimique qui consiste à utiliser du jus de citron, du lait, ou même du chlorate de soude, pour écrire le message secret qui sera invisible à l'œil nu. Un simple passage sous une source chaude (flamme de bougie, fer à repasser chaud...) révèle le message. Cette technique reste encore présente, puisqu'on trouve aujourd'hui sur les billets de banque des encres ultraviolette, qui créent une réaction, en cas de photocopie, en inscrivant un message permettant de lutter contre la contrefaçon.
- Une autre forme de dissimulation de messages est la stéganographie linguistique. Pour cacher un message secret dans un texte, on peut utiliser le langage, l'espace entre les mots, la ponctuation, l'orthographe, ou encore des repères au niveau des caractères.
- Durant la Seconde Guerre mondiale, on nota l'apparition de la technique du micropoint de Zapp. Très appréciée par les agents allemands, cette technique consiste à réduire une photo, d'une page en un point d'un millimètre ou moins, qui est ensuite placé discrètement dans du texte anodin.

Ces exemples de stéganographie classique montrent que les méthodes pour dissimuler l'information se basaient sur la notion de canal secret pour envoyer l'information.

2.2- Stéganographie contemporaine

S'appuyant sur les technologies de pointe, la stéganographie moderne est potentiellement applicable à différents supports numériques : fichiers audio, vidéos, textes, ...etc. Parmi les fichiers qui sont très adaptés pour la dissimulation d'information, on retrouve également les **images numériques**.



Le fameux feuilleton "prison break" et l’affaire de Snowden illustrent deux procédés distincts de la stéganographie contemporaine.

II- Etude technique

1- Schéma stéganographique

La définition du problème peut s'expliquer par le scénario des prisonniers, posé par G.J. Simmon en 1983. Soit Alice et Bob deux prisonniers enfermés dans deux cellules différentes, et souhaitant communiquer un message d'évasion. Comme dans toute prison, Alice et Bob ne sont autorisés à communiquer qu'à travers un intermédiaire. Eve est la gardienne chargée de la surveillance des échanges de message entre Alice et Bob.

Si Eve suspecte le moindre signe de conspiration entre les deux détenus, elle s'autorisera à mettre fin à leur échange. Alice et Bob sont conscients de cette situation, et savent très bien que l'utilisation de messages chiffrés éveillerait les soupçons de Eve. Ils doivent donc utiliser une technique de dissimulation pour cacher leur plan dans des messages innocents. Ils pourront ainsi planifier leur évasion, sans attirer la suspicion de Eve.

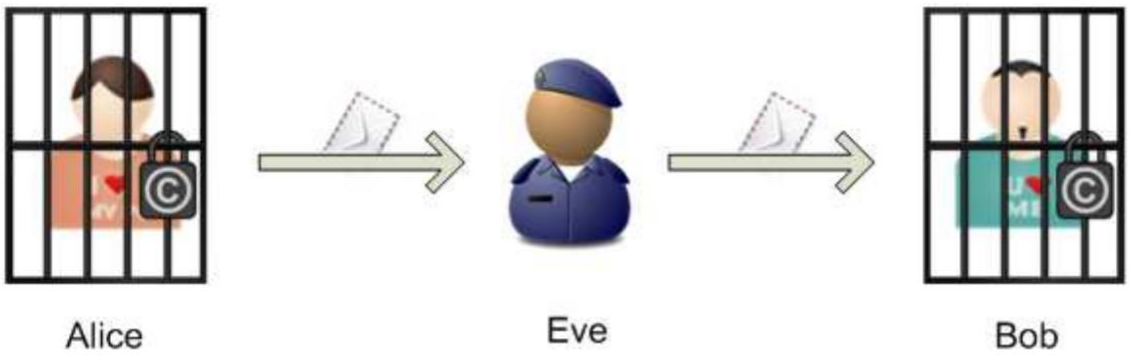
Dans ce scénario, on distingue deux parties : les stéganographes représentés par les deux prisonniers Alice et Bob, et la stéganalyste modélisée par la gardienne Eve. Du côté stéganographie, Alice et Bob ont pour but de se communiquer discrètement des informations secrètes de manière totalement indétectable. Du côté stéganalyse, Eve la gardienne est libre d'examiner le médium intercepté. Lorsque Eve conclut qu'il y a présence d'un message caché, elle coupe la communication. Si non, elle laisse passer la communication.

D'après cette histoire, on peut définir un schéma stéganographique, en utilisant les notations suivantes : soit M l'ensemble des messages possibles à insérer et C l'ensemble de tous les supports possibles. Un schéma stéganographique est défini par deux fonctions :

$$Emb : C \times M \rightarrow C$$

qui est la fonction d'insertion (embedding), elle prend en paramètre un support ou médium de couverture et un message qu'on veut dissimuler, puis retourne un nouveau médium de couverture appelé Stego-médium ou Stegoobjet. Le stego-médium peut être intercepté par quelqu'un qui peut faire une modification ou non. Finalement, le stego-objet est traité par une fonction d'extraction (fonction inverse à la fonction d'insertion) :

$$Ext : C \rightarrow M \text{ qui retourne le message original.}$$



Les utilisations de la stéganographie sont devenues aussi multiples que variées, avec emploi de manière légale ou carrément illicite.

Le tableau suivant illustre les domaines d'application de la stéganographie contemporaine :

Utilisations légales	Utilisations malveillantes
Libertés d'expression	Les réseaux terroristes
Les armées	Pédophilie
Secrets intimes	Espionnage industriel

2- Catégories de stéganographie

Les deux grandes branches de la stéganogrphie sont en fait les suivantes : **linguistique et technique.**

- **Stéganographie linguistique** : comprend toutes les formes de styles possibles, jeux de langue ou utilisation de repères au niveau des caractères.

  Les différentes formes de la stéganographie linguistique sont :

- Sémagramme : De cette manière, le système stéganographique échappe totalement à l'observateur. Alfred de Musset est l'utilisateur le plus connu de ce procédé. Il a entretenu, entre 1833 et 1834, une relation secrète avec Georges Sand au travers de poèmes qu'il lui envoyait.
- Acrostiche : Ce procédé permet de transmettre des données au travers de lettres initiales dans chaque vers de poème et qui, lus de haut en bas, forment un mot ou une expression.
- Ponctuation : L'utilisation de points, hauteur de lettres et virgules par les prisonniers de guerre a également permis de transmettre des messages à leur famille.
- Nulles : Ces codes camouflés consistent à marquer d'un signe particulier certaines lettres d'un texte (par des piqûres d'aiguilles sur ou sous les lettres). Il suffit alors de rassembler les lettres marquées pour former un mot.
- Insertion d'erreurs : Mise en valeur de l'information au travers d'erreurs ou de formes de style dans un texte.
- Le processus de mise en œuvre de ces différents procédés demeure trop complexe. C'est ainsi qu'on leur préfère les procédés plutôt techniques.

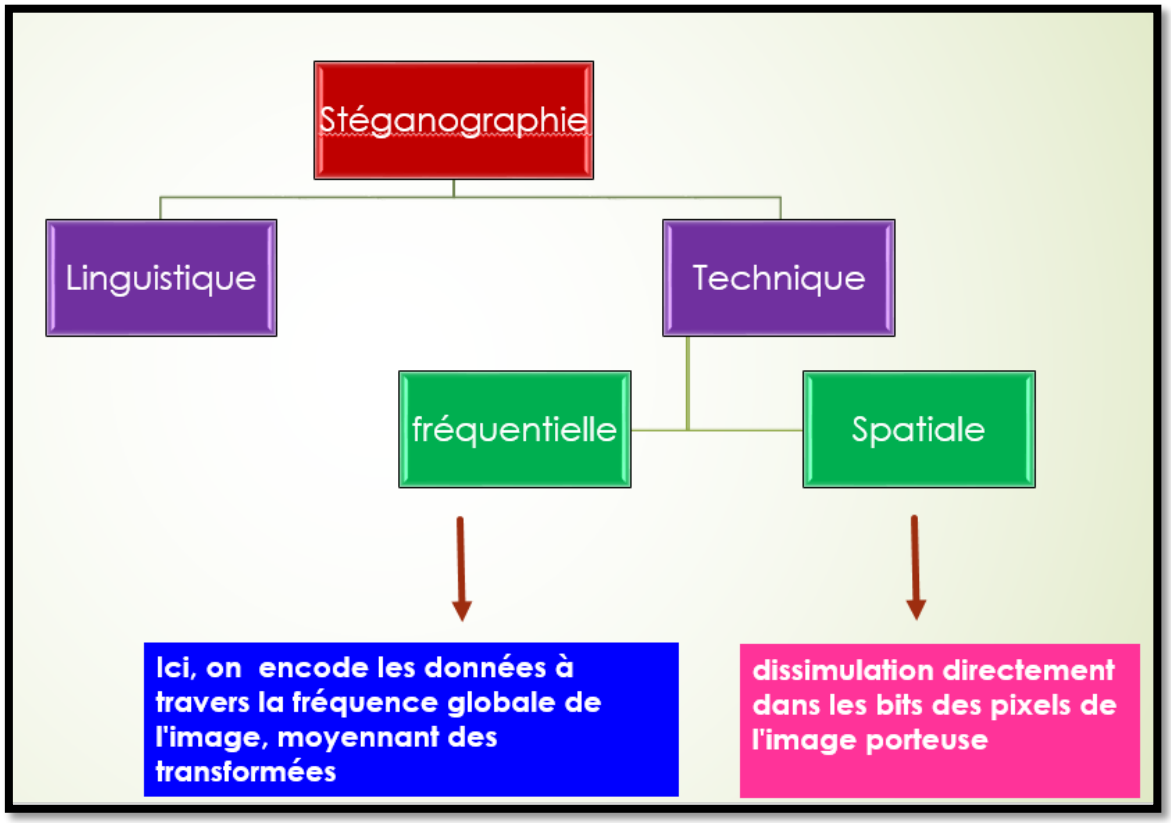
- **Stéganographie technique**. Celle-ci regroupe les moyens de transmissions purement physiques. Elle se subdivise à son tour en deux variantes :
  - ✓ Stéganographie spatiale : son principe consiste en la **dissimulation directement dans les bits des pixels de l'image porteuse.**
  - ✓ Stéganographie fréquentielle : consiste en un **codage des données à travers la fréquence globale de l'image, moyennant des transformées (fourrier, cosinus discret,…).**

  Bref, elle a recours à la dissimulation de données dans plusieurs types de médias :

  - ❖ Audio : Afin de transmettre de l'information de manière cachée dans du son, différentes techniques existent et se basent sur le fait qu'un son affecte la perception d'un autre : un son plus fort peut en cacher un autre, un son peut être caché temporairement lorsqu'il est moins fort et qu'il est placé avant ou après un son plus fort.

- ❖ Images, vidéo : une image ou une vidéo peuvent également contenir un message. Une image est constituée de pixels. Il est possible d'insérer des bits du message secret à l'intérieur sans que ces modifications soient perceptibles à l'œil humain.

Le schéma ci-après illustre cette subdivision.



3- Types de schéma stéganographique :

Il existe 3 façons pour l'insertion d'un message secret :

- la stéganographie par sélection du médium de couverture :
- la stéganographie par synthèse du médium hôte
- et enfin lastéganographie par modification d'un médium de couverture

a- stéganographie par sélection du médium de couverture :

En stéganographie par sélection du médium de couverture, Alice, l'émetteur, dispose au préalable d'une base fixe d'images. Pour communiquer secrètement avec Bob, Elle sélectionne, à partir de sa base, l'image qui communique au mieux le message désiré. Par exemple, Alice peut transmettre à Bob un bit d'information, simplement en jouant sur l'orientation de l'image envoyée (portrait

ou paysage). De même, la présence d'un animal ou d'un objet particulier, dans l'image envoyée, peut avoir un sens caché, partagé uniquement entre l'émetteur et le récepteur. Par ailleurs, Alice peut également utiliser une fonction de hachage, avec une clé secrète commune entre elle et Bob, pour transmettre son message. Dans un tel cas de figure, Alice parcourt sa base d'images, jusqu'à ce qu'elle tombe sur une image, dont l'empreinte digitale coïncide avec le message désiré. Une fois trouvée, elle envoie cette image à Bob, qui pourra facilement lire le message secret en réappliquant la fonction de hachage avec sa clé secrète. Bien évidemment, cette dernière méthode de dissimulation devient très vite impraticable dans la réalité. En effet, plus le message est long, plus le nombre d'images à parcourir est important. L'avantage de ce genre d'approches est qu'elles sont quasiment indétectables. En effet, le médium de couverture n'ayant subi aucune modification, il est impossible de deviner qu'il y a un message caché. Le problème majeur de ces méthodes reste cependant celui de la capacité d'insertion très limitée.

b- la stéganographie par synthèse du médium hôte

Elle consiste à créer le support hôte qui embarque au mieux le message secret. En théorie, si Alice est capable de créer un médium de couverture, avec une distribution connue entre elle et Bob, elle devrait pouvoir cacher son message de manière parfaitement sûre. En d'autres termes, Alice pourra dissimuler son message secret tout en préservant parfaitement la distribution originale. Alice peut par exemple prendre plusieurs images de la même scène. Pour envoyer un message secret, Alice crée une nouvelle stégo image en échantillonnant simplement les différentes images acquises. En stéganographie linguistique, on retrouve également ce concept de dissimulation au travers de l'acrostiche. Par ailleurs, elles sont également très limitées en capacité d'insertion.

c- la stéganographie par modification du médium

Le stéganographie par modification du médium de couverture est la méthode d'insertion la plus pratique et la plus utilisée dans la littérature. Le principe de cette méthode consiste à altérer un médium de couverture, pour dissimuler un message, de sorte que celui-ci soit indétectable visuellement et statistiquement. Autrement dit, le message est inséré en modifiant le support, de manière à préserver "le plus possible" lastatistique originale de ce support. Soit K l'ensemble des clés possibles, le schéma stéganographique par modification du médium de couverture est caractérisé par deux fonctions :

- la fonction d'insertion, notée Emb, prend en entrée une clé privée k ∈ K et de vient comme suit :

$$Emb : C \times M \times \mathbf{K} \rightarrow C.$$

- la fonction d'extraction, notée Ext, utilisée par le récepteur, Bob, et qui prend en paramètre une clé stéganographique, et le stégomédium reçu, et qui retourne lemessage secret en sortie :

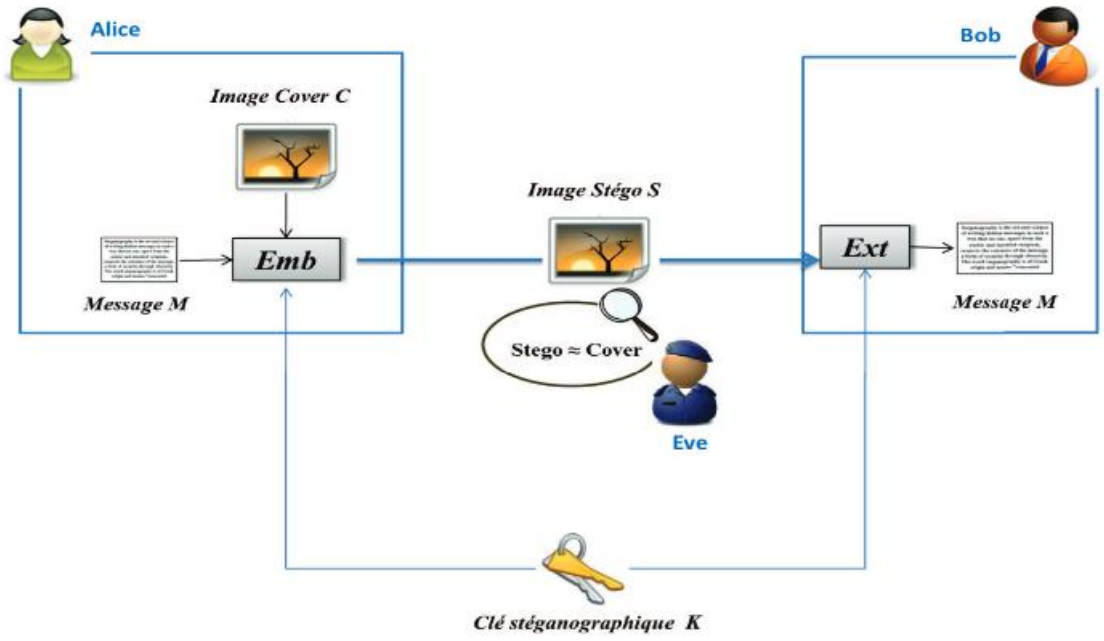
$$Ext : C \times \mathbf{K} \rightarrow M.$$

- L'objectif d'un schéma stéganographique est qu'après qu'Alice ait inséré le message, Bob puisse l'extraire.

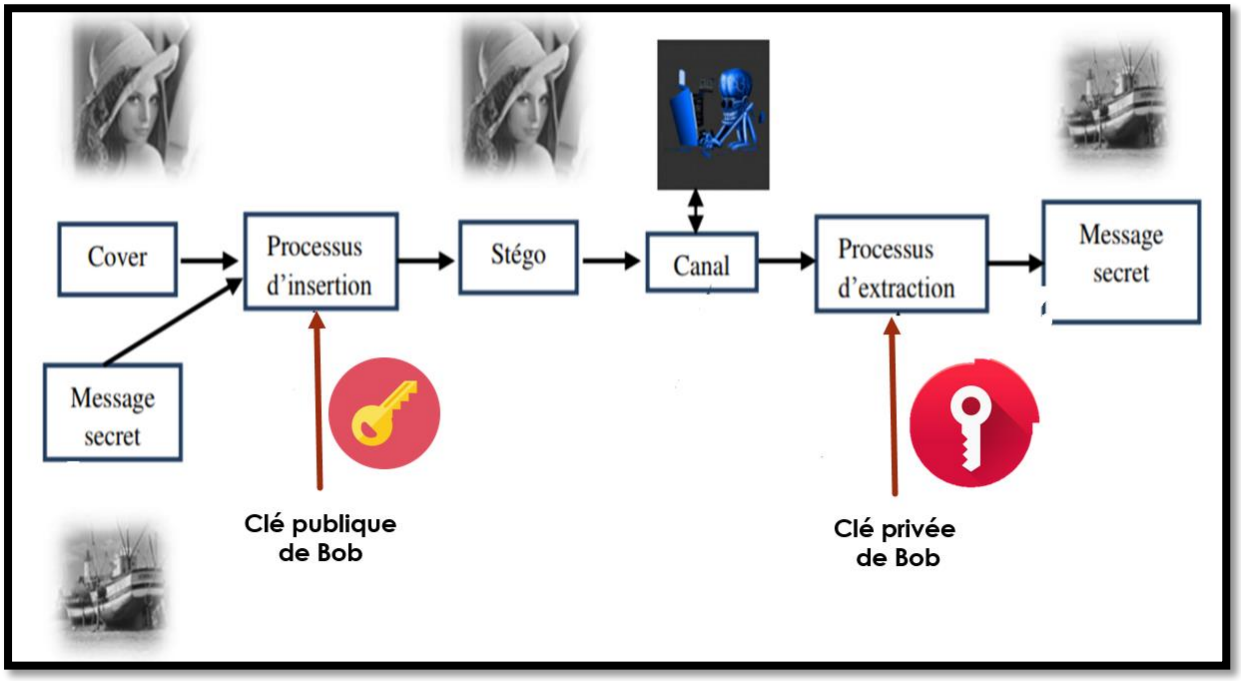
De manière similaire à la cryptographie, il existe trois types d'algorithmes stéganographiques par modification : pure, à clé symétrique et à paire de clés.

a- Pure : sans aucun ajout de clés, simple à implémenter mais au détriment de l'aspect sécuritaire

b- Dans le cas d'un schéma de stéganographie à clé privée, l'émetteur et le récepteur (Alice et Bob), doivent partager au préalable une clé secrète commune. Cette clé est alors utilisée par la suite pour l'insertion et l'extraction du message secret.



c- Par ailleurs, dans le cas d'un schéma de stéganographie à clé publique, Alice utilisera la clé publique de Bob pour l'insertion du message secret, que seul Bob pourra le déchiffrer par la suite avec sa clé privée.



4- Propriétés des systèmes de stéganographie :

a- **Capacité** : La capacité d'insertion d'un système de stéganographie reste tributaire de la taille en bits du message secret à intégrer dans un média de taille donnée. La capacité d'insertion relative est le rapport entre la taille du message secret à dissimuler et la taille du médium utilisé.

b- **Sécurité** : tout ce dont jouit la cryptographie en matière d'exigences de sécurité peut de même être à la faveur de la stéganographie. Ce qu'il ne faut pas perdre de vue, c'est que l'on ne doit jamais être en mesure de faire la distinction entre l'image d'origine et l'image stégo. De plus, il faut prendre en considération cette phrase : "modifier sans abimer, modifier sans altérer" : c'est ce qu'on appelle la distorsion.

c- **Robustesse** : Elle est relative à la résistance du message dissimulé aux diverses attaques (transformations) apportées au médium stégo.

5- Disciplines connexes

Les branches scientifiques, qui peuvent être confondues avec la stéganographie sont le tatouage et la cryptogrpahie.

- **Le duo stégano / crypto :**

  La cryptographie consiste en une écriture secrète (au sens d'indéchiffrable), tandis que la stéganographie consiste en une écriture discrète (au sens d'indiscernable). Si la notion de « clef secrète » est commune à la cryptographie et à la stéganographie, leur différence essentielle réside dans le fait que, pour la cryptographie, la clef secrète empêchera celui qui n'en a pas la connaissance de déchiffrer le message, alors que la stéganographie empêchera de suspecter son existence même.

  Sans doute convient-il d'appuyer dès maintenant sur une implication majeure de cette différence : la cryptographie est une écriture secrète mais nue, alors que la stéganographie est une écriture discrète : elle nécessite une couverture, un contenu dans lequel vivre, tel un espion qui n'est pas vraiment celui qu'on croit. En d'autres termes, un message crypté est immédiatement perçu comme incompréhensible, alors qu'un message stéganographié n'est pas même immédiatement perçu comme existant. Le lecteur conviendra aisément que l'important pour un assiégé est bien qu'on ne puisse pas soupçonner ses communications plutôt qu'on ne puisse les déchiffrer. Ainsi donc, nous distinguons l'écriture secrète de l'écriture indiscernable, qui nous intéresse ici. De fait, rien n'interdit de cacher un message préalablement crypté. Les deux disciplines n'ont jamais été concurrentes, mais sont plutôt complémentaires.

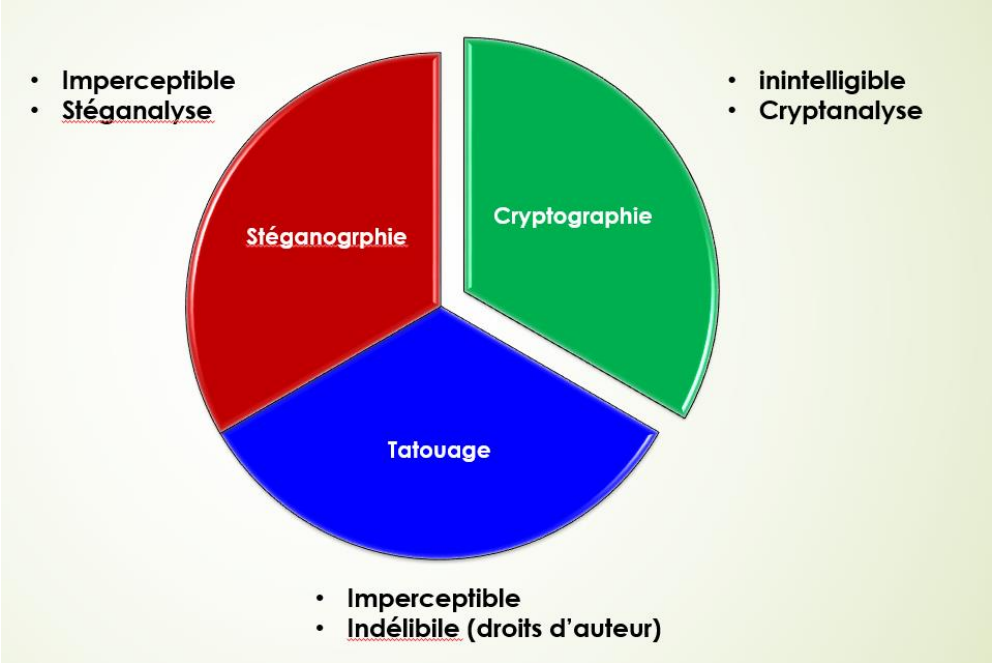
  Par ailleurs, si le dual de la crypto est la cryptanalyse, le dual de la stégano est la stéganalyse. Celle-ci consiste à attaquer les méthodes de stéganographie. Elle peut être appliquée par deux types de personnes. L'attaquant actif, qui connait la présence de l'information et tente de la modifier ou de l'extraire et l'attaquant passif, c'est-à-dire la personne qui arrive à déceler la présence du message et qui ne fait que constater sa présence.

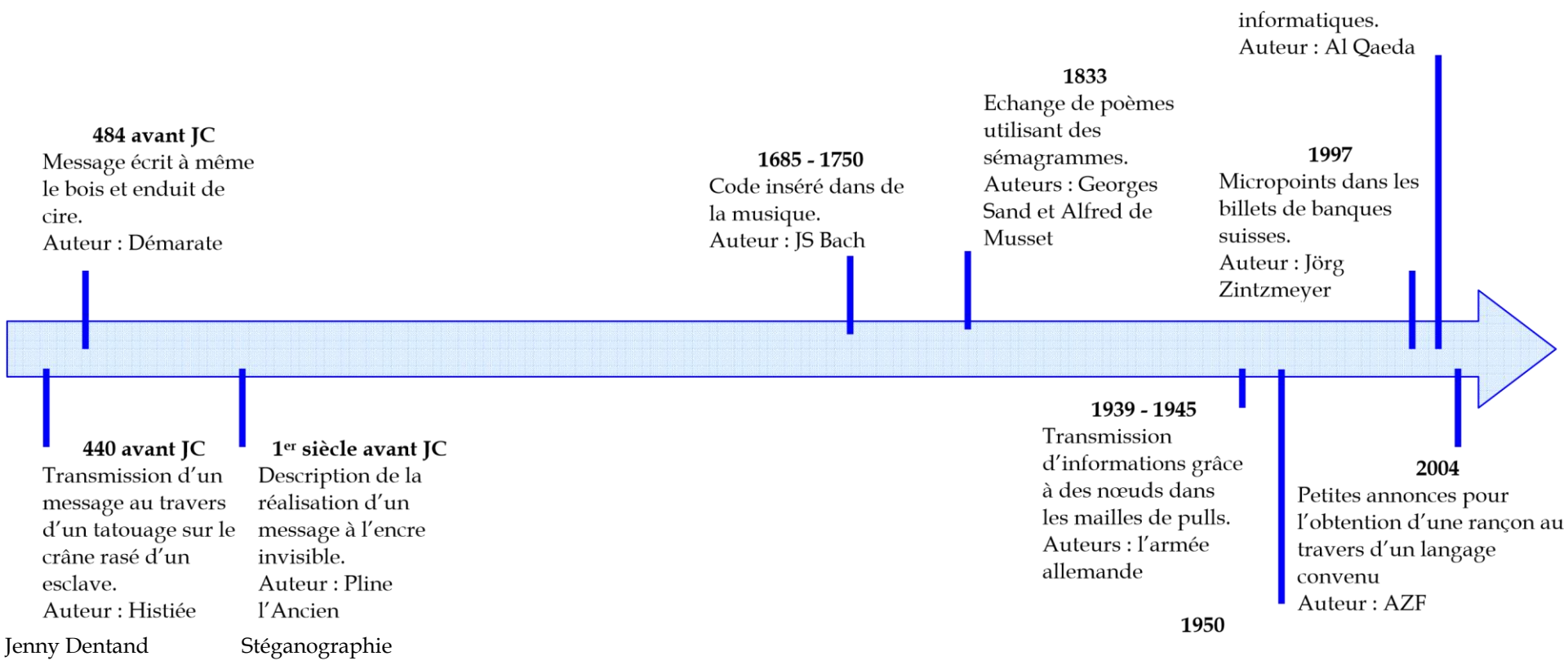
- **Le duo stégano/tatouage :**

  Ces deux domaines de recherche peuvent paraître semblables car ils ont la même exigence d'indiscernabilité (de l'existence du message) ; pourtant, leur

différence est fondamentale : la stéganographie recherche une indiscernabilité statistique, alors que le tatouage recherche une indiscernabilité perceptuelle.
Soulignons encore deux autres points communs entre la stéganographie et le tatouage. D'abord, ces deux disciplines recouvrent un procédé numérique.
Mais surtout, ces deux disciplines vont devoir s'adapter à la couverture particulière à laquelle on les applique. C'est ce que l'on appelle tirer parti de l'information adjacente. Ainsi, en tatouage comme en stéganographie, on tirera beaucoup d'avantages à se servir de la couverture particulière dans laquelle on va cacher notre message.

La relation entre le trio est schématisée sur la figure qui suit :




informatiques.
Auteur : Al Qaeda
1833
Echange de poèmes utilisant des sémagrammes.
Auteurs : Georges Sand et Alfred de Musset
484 avant JC
Message écrit à même le bois et enduit de cire.
Auteur : Démarate
1685 - 1750
Code inséré dans de la musique.
Auteur : JS Bach
1997
Micropoints dans les billets de banques suisses.
Auteur : Jörg Zintzmeyer
1939 - 1945
Transmission d'informations grâce à des nœuds dans les mailles de pulls.
Auteurs : l'armée allemande
440 avant JC
Transmission d'un message au travers d'un tatouage sur le crâne rasé d'un esclave.
Auteur : Histiée
1er siècle avant JC
Description de la réalisation d'un message à l'encre invisible.
Auteur : Pline l'Ancien
1950
2004
Petites annonces pour l'obtention d'une rançon au travers d'un langage convenu
Auteur : AZF
Jenny Dentand
Stéganographie

III- Idée de manœuvre : La Méthode LSB par clé secrète

1- Explication du LSB

L'idée est de prendre un message et de le modifier de manière aussi discrète que possible afin d'y dissimuler l'information à transmettre. Le message original est le plus souvent une image. La technique de base, dite LSB pour Least Significant Bit, consiste à modifier le bit de poids faible des pixels codant l'image : une image numérique est une suite de points, que l'on appelle pixels, et dont on code la couleur à l'aide d'un triplet d'octets. Par exemple, pour une couleur RGB sur 24 bits, chaque octet indique l'intensité de la couleur correspondante --- rouge, vert ou bleu (Red Green Blue) --- par un niveau parmi 256. Passer d'un niveau n au niveau immédiatement supérieur (n+1) ou inférieur (n-1) ne modifie que peu la teinte du pixel, or c'est ce que l'on fait en modifiant le bit de poids faible de l'octet.

Voyons l'exemple suivant.

00000000 10101000 11100101	00000000 00100000 11001101
00100100 00011111 00101000	11111111 11100000 10110010

Chaque entrée de ce tableau représente un pixel couleur, nous avons donc une toute petite image 2×2. Chaque triplet de bits (0 ou 1) code la quantité de l'une des trois couleurs primaires du pixel.

Le bit le plus à droite de chaque triplet est le fameux bit de poids faible : LSB. Si on souhaite cacher le message **111 111 001 111**, l'image est modifiée de la façon suivante : le bit de poids faible du i^{ème} octet est mis à la valeur du i^{ème} bit du message ; ici on obtient :

0000000**1** 1010100**1** 1110010**1**	0000000**1** 0010000**1** 1100110**1**
0010010**0** 0001111**0** 0010100**1**	1111111**1** 1110000**1** 1011001**1**

Le LSB peut même être couplé à un générateur aléatoire lors de l'insertion, ce qui rend la tâche compliquée en cas d'interception par des personnes malveillantes. Il ne

saurrait reconstituer le fichier d'origine étant donné l'aspect aléatoire de distribution des bits du message d'origine dans le cover.

Une autre technique repose sur le LSB avec permutation.

2- Principe du projet

En réalité, ce système se prête tout particulièrement aux images. Dans une image numérique ordinaire, on obtient une image en 16,7 millions de couleurs (256^3).

Modifier les bits de poids faible des composantes ne change que très peu la couleur (deux valeurs proches entre 0 et 255 correspondent à des intensités proches).

En revanche, ne connaître que les bits de poids fort permet de reconstituer l'image assez fidèlement.

Notre idée est donc de stocker les bits de poids fort d'une image (l'image secrète) à l'emplacement des bits de poids faible d'une autre (l'image anodine) qui se trouvera peu affectée.

Pour rechercher une image cachée dans une autre par ce biais, il faut donc sélectionner par exemple les 4 bits de poids faible de chaque composant de chaque pixel (nombre entre 0 et 15) et les multiplier par 16 (décalage de 4 positions binaires).

Image 1	R=01001110	G=01101111	B=11111111
Image 2	R=01110011	G=01110110	B=10101010
Image fabriquée	R=01000111	G=01100111	B=11111010

L'émetteur de l'image secrète ou du fichier secret avant de se projeter sur l'image cover, il passe inéluctablement par une encryption moyennant AES. Cela renforce la sécurité de la transmission du data caché.

IV- Réalisation

Nous avons mis sur pied un programme python, débouchant sur une interface graphique pour faciliter la procédure stéganographique. **Le code a été tapé en dur, sans aucune utilisation de bibliothèque.**

Le programme est fort de 5 fonctions principales :

- **encrypt_AES ()** : prend en paramètre le data secret pour le crypter à l'aide de AES, avec une clé à 32 bits.

```
def encrypt_AES(data):
    key='1234567890abcdef'
    obj = AES.new(key, AES.MODE_ECB)
    #texte=padd(data)
    return obj.encrypt(data[:(len(data)//16)*16])
```

- **encode_in_pixel ()** : permet de remplacer les bits de la data cryptée respectivement dans les 3 bits LSB du rouge puis les 3 bits du vert et enfin les 2 bits LSB du bleu.
  Il sied de signaler ici que le cover est en format **pixel**, alors que le data est en format **modèle** (c'est-à-dire en format **Octet**).

```
def encode_in_pixel(byte, pixel):
    """Encodes a byte in the three least significant bits of each channel.
    """
    x=bin(byte)[2:]
    byte=bin(byte)[2:]
    byte=padding(byte)
    r = int(byte[:3],2)
    g = int(byte[3:6],2)
    b = int(byte[6:],2)

    color = (r+(pixel[0]&248),\
             g+(pixel[1]&248),\
             b+(pixel[2]&252))
    return color
```

- **decode_in_pixel ()** : permet de récupérer, depuis l'image stégo reçue, respectivement les 3 bits LSB du rouge puis les 3 bits du vert et enfin les 2 bits LSB du bleu. La suite des 8 bits forment octet par octet notre image secrète que l'on récupère fidèlement.

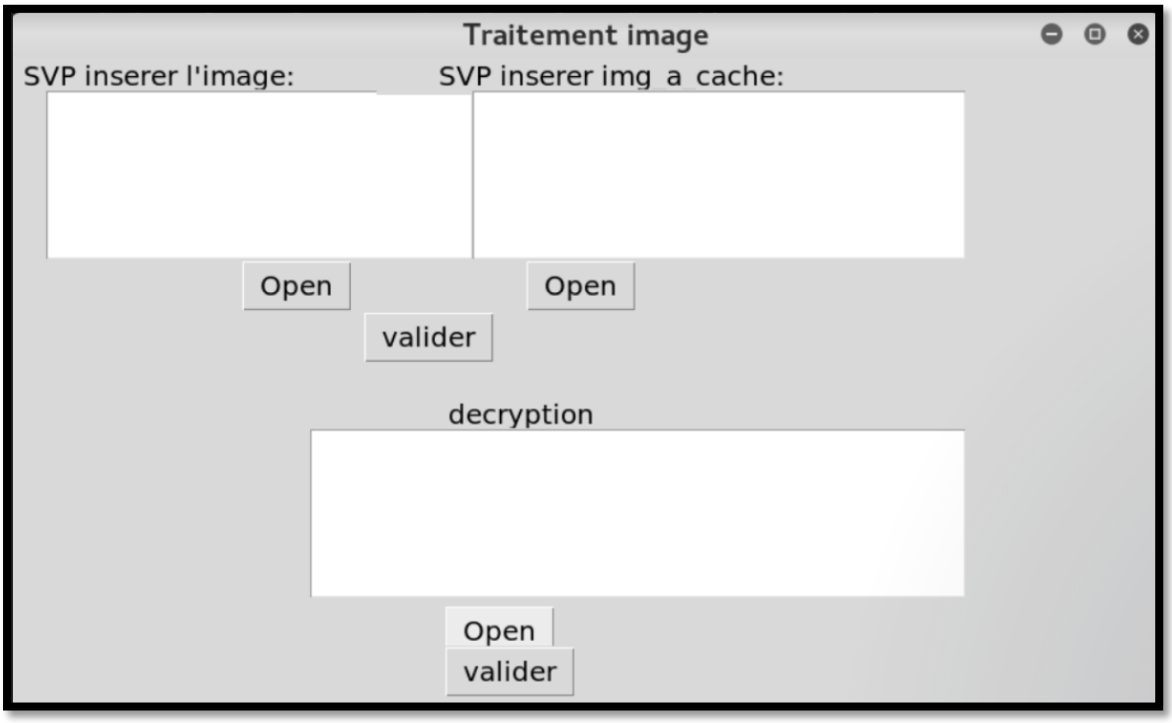
```
def decode_in_pixel(pixel):
    a=padding(bin(pixel[0])[2:])
    b=padding(bin(pixel[1])[2:])
    c=padding(bin(pixel[2])[2:])
    r=a[5:]+b[5:]+c[6:]

    return chr(int(r,2))
```

- **decrypt_AES () :** fait l'opposé de la fonction encrypt_AES (), nous permettant ainsi de récupérer notre data en clair.

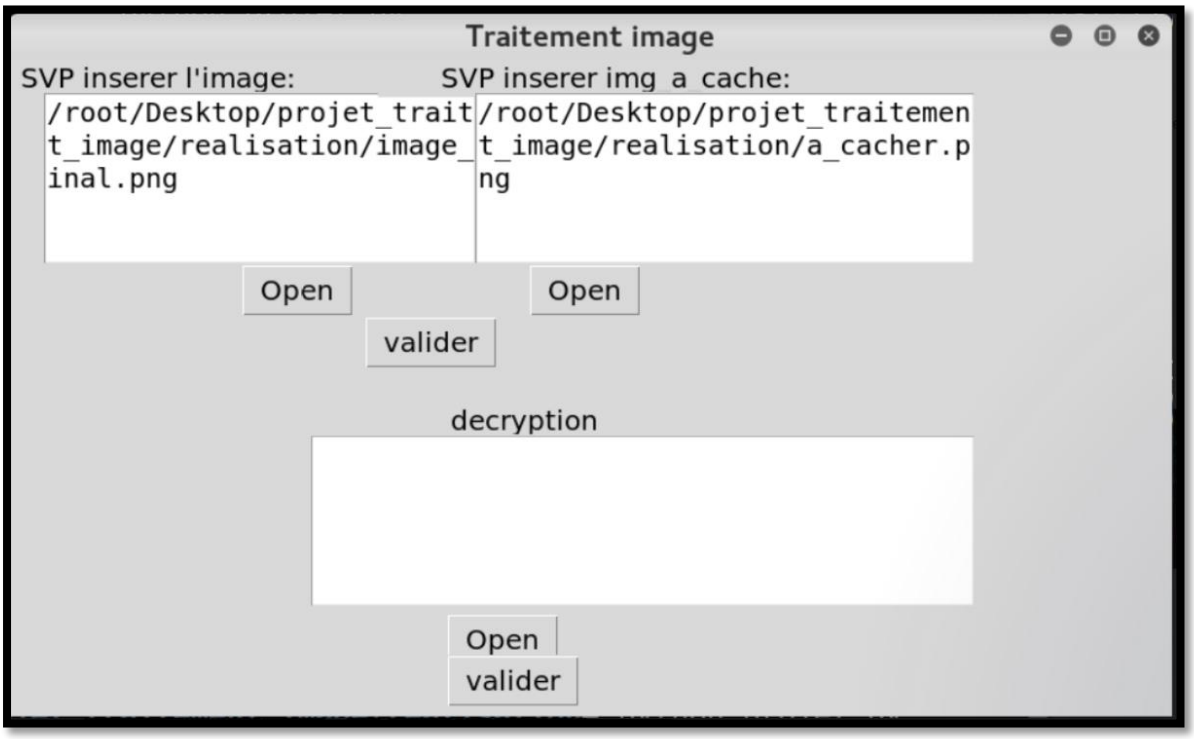
```
def decrypt_AES(data):
    key='1234567890abcdef'
    obj = AES.new(key, AES.MODE_ECB)
    return obj.decrypt(data)
```

- **Démonstration de l'implémentation :**

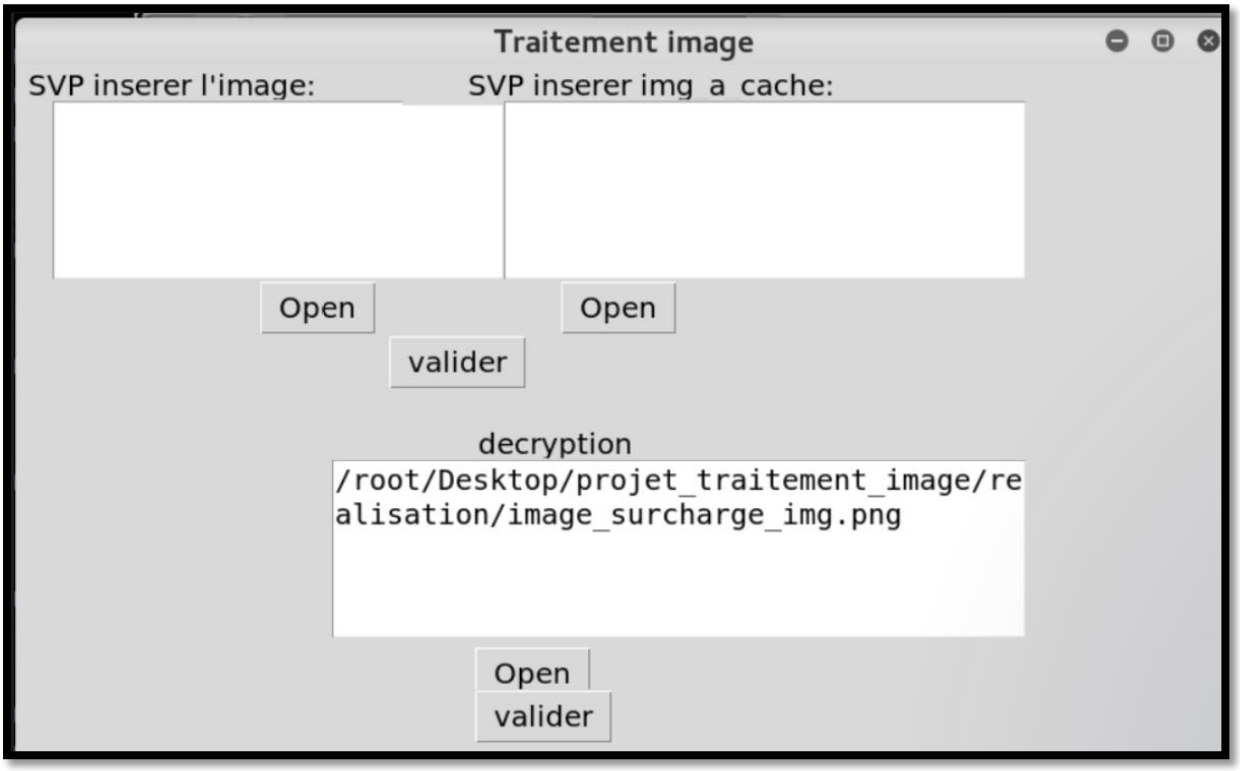
L'interface d'accueil de notre application se présente comme suit :



Il suffit de remplir les champs de l'image cover et l'image secrète par le billais de leurs chemins respectif.



La validation de l'utilisateur permet d'extraire l'image secrète, comme indiqué ci-après :



Conclusion

Il va sans dire alors que la stéganographie demeure une solution incontournable à l'ère des technologies de pointe où l'échange d'informations bat son plein. Contrairement à la cryptographie, les informations sont cachées mais encore faut-il savoir que information y est.

En effet, la stéganographie repose sur bel et bien sur son caractère **imperceptible.** Elle est parfois confondue à la cryptographie et au tatouage. Pourtant, chacune de ce cette trilogie est une discipline à part, complémentaire parfois.

La stéganographie se subdivise en spatiale (objet de notre travail) et fréquentielle. Nous avons démontré à travers notre mémoire qu'il était possible de cacher des data à l'intérieure d'une image en distribuant les bits de notre data sur les bits du cover, le tout implémenté par un programme informatique, débouchant sur la possibilité de récupérer fidèlement les data d'origine, moyennant au passage AES.

En guise de perspective, ce travail gagnerait encore en performance si l'interface créée incorporait également un autre champ pour la stéganographie fréquentielle, donnant ainsi à l'utilisateur la possibilité de choisir entre la procédure spatiale ou fréquentielle.

Wébographie

https://tel.archives-ouvertes.fr/tel-01275346/document#page=18&zoom=100,0,348

https://tel.archives-ouvertes.fr/tel-01020745/document

http://hugo.alatristasalas.free.fr/files/Rapport-Steganographie.pdf

http://bts2.epsi.free.fr/COURS/St%E9ganographie.pdf

http://lig-membres.imag.fr/donsez/ujf/easrr0203/tatouagestegano/tatouagestegano.pdf

https://www.researchgate.net/profile/Teddy_Furon2/publication/50875195_La_steganographie_moderne/links/00b49529af4caec310000000.pdf

https://interstices.info/cryptographie-steganographie-et-tatouage-des-secrets-partages/