Cahier Des Charges

AYOUB Pierre - BASKEVITCH Claire - BESSAC Tristan -
CAUMES Clément - DELAUNAY Damien - DOUDOUH Yassin

Stéganographie & Stéganalyse

Mercredi 14 Mars 2018

1 Préambule

1.1 Définition des termes du sujet

La stéganographie est l'art de la dissimulation, appliquée en informatique en cachant des données dans d'autres données. Cette dissimulation se fait généralement au sein de fichiers multimédias. La stéganographie se différencie de la cryptographie, qui correspond à chiffrer un message afin qu'il soit illisible par une personne différente de l'émetteur et du destinataire. En effet, un message chiffré en cryptographie sera visible par tous mais illisible, tandis qu'un message caché dans un fichier f en stéganographie ne sera vu que si un inconnu sait que f contient un message et connaît l'algorithme pour l'interpréter.

La stéganalyse, quant à elle, est la recherche de données cachées dans des fichiers suspects. Si ces données sont identifiées, il faut ensuite réussir à les extraire pour les lire.

1.2 Historique

La stéganographie est une méthode très ancienne dont la première référence à cette utilisation date du premier siècle avant Jésus-Christ. Elle apparaît dans un récit écrit par Hérodote qui raconte comment deux citoyens communiquaient secrètement : le premier citoyen rasait la tête de son esclave et lui écrivait un message sur son crâne. Ensuite, il fallait attendre que les cheveux de l'esclave repousse puis envoyer ce dernier chez le deuxième citoyen. Ce dernier devait de nouveau raser la tête de l'esclave pour découvrir le message qui lui était destiné. Une autre utilisation de la stéganographie consistait à utiliser de l'encre ,invisible à l'oeil nu, mais qui était révélée à la chaleur.

Avec l'émergence de l'Informatique, les techniques de Stéganographie se sont renouvelées. En effet, il est désormais possible de cacher des données dans d'autres données. Cette multiplicité de techniques stéganographiques grâce à l'Informatique montre l'étendue de cette application dans tous les domaines. Par exemple, la stéganographie moderne a été utilisée dans des communications terroristes (transmission de messages) ou dans les signatures de fichiers multimedia (tatouage numérique) afin de protéger les droits d'auteurs.

2 Conducteurs du projet

2.1 But du projet

Le but du projet est de réaliser un logiciel de Stéganographie. Les utilisateurs ciblés sont des personnes lambdas qui veulent communiquer sans que l'on soupçonne que leurs communications sont en réalité compromettantes.

Le but de l'application est de permettre à un utilisateur U_1 d'envoyer des données cachées à un autre utilisateur U_2. Ce deuxième utiliseur devra pouvoir interpréter ces données en utilisant la même application que U_1.

2.2 Motivation du projet

La motivation du projet est venue par notre envie de la majorité des membres de ce groupe de projet d'obtenir le master Secrets. En effet, nous voulions tous réaliser un projet en rapport à la cryptographie et c'est donc pour cela que nous nous sommes réunis afin de réaliser ce type de projet.

3 Explications des algorithmes de stéganographie

L'application devra pouvoir cacher des données dans des fichiers de différents formats (texte, image, son, video). Chaque format nécessite un algorithme différent.

3.1 Algorithme LSB (Least Significant Bit)

Pour le format image, nous allons utilisé l'algorithme LSB : cela permet de cacher des bits dans des octets tel qu'ils seront invisibles pour l'Homme. Chaque pixel d'une image correspond à un triplet de nombres : R,G,B qui correspondent aux composantes de couleurs Rouge-Vert-Bleu de 0 à 255. Le but de cet algorithme est donc de cacher des bits dans cette image. Pour se faire, nous allons remplacer les 2 bits de poids faibles de chaque composante des pixels de l'image. En effet, à l'oeil nu, l'homme ne discernera jamais le changement minime de composante. Nous allons faire un exemple : Prenons un exemple de couleur C_1 dont le triplet est $(219, 27, 91)$

R : $219_{10} = 11011011_2$ G : $27_{10} = 11011_2$ B : $91_{10} = 1011011_2$

Imaginons que la donnée à cacher dans le fichier composé de cet unique pixel de couleur C_1 correspond à la suite de bits $B = 000000_2$ et Ce qui donne une toute autre couleur C_2 en changeant les 2 bits de poids faibles de chaque composantes du pixel :

R : $216_{10} = 11011011_2$ G : $24_{10} = 11000_2$ B : $88_{10} = 1011000_2$

Voici ici les deux couleurs C_1 et C_2, montrant ainsi qu'un humain ne pourra jamais détecter un changement de bit :

FIGURE 1 – Couleur C_1

FIGURE 2 – Couleur C_2

Pour la partie réception du fichier, il faut savoir si ce fichier a été utilisé pour un message caché et connaître combien de bits sont cachés. Il faudra donc calculer la taille maximale du message à cacher qui sera une puissance de 2. En effet, en fonction de la taille du fichier, un certain nombre de bits sera réservé pour connaître la taille des données à cacher. En fonction de ces informations, la suite de bits cachée sera donc formée.

4 Contraintes du projet

4.1 Calendrier

Le Cahier des Charges doit être remis le 14 mars. Le Cahier des Spécifications est à remettre le 18 avril. La remise du produit au client est le 25 mai. La présentation du produit au client sera le 1 juin 2018.

4.2 Contraintes imposées

5 Exigences fonctionnelles

5.1 Portée du produit

5.2 Exigences du client

L'application doit respectée deux exigences pour le client : elle doit permettre à un utilisateur ne connaissant pas la stéganographie de pouvoir facilement utiliser toutes les fonctionnalités de l'application grâce à une interface graphique. De plus, une interface au terminal doit être également proposée pour les utilisateurs savant manipuler le terminal. En effet, ces utilisateurs pourront réaliser les mêmes fonctionnalités qu'avec l'interface graphique.

6 Exigences non fonctionnelles

6.1 Apparence et Perception : Ergonomie

6.2 Facilités d'utilisation

6.3 Performance

6.4 Exigences culturelles, politiques et légales

7 Autres aspects du projet

7.1 Solutions sur étagère déjà existantes

7.2 Tâches à réaliser pour le développement de l'application

7.3 Estimations des coûts du projet

7.4 Améliorations pour les versions futures du projet

7.5 Choix du langage et de l'interface

8 Conclusion