14085 NHAIRECH Oussama

La stéganographie digitale

Des attaques récentes ont révélé une nouvelle campagne des hackers qui utilisaient des fichiers audios pour cacher leurs logiciels malveillants. Pour cela, Ils se servent de la stéganographie digitale. Il est donc intéressant de découvrir ses techniques, ainsi ses possibilités et ses limites.
Des attaques récentes ont révélé une nouvelle campagne des hackers qui utilisaient des fichiers audios pour cacher leurs logiciels malveillants. Pour cela, Ils se servent de la stéganographie digitale. Il est donc intéressant de découvrir ses techniques, ainsi ses possibilités et ses limites.

Positionnement thématique (ETAPE 1)

INFORMATIQUE (Informatique pratique), MATHEMATIQUES (Mathématiques Appliquées).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
La Stéganographie digitale	*Digital steganography*
Le Bit de poids faible	*Least significant bit*
Pixel	*Pixel*
La Transformée en cosinus discrète	*Discrete cosine transform*
Image	*Image*

Bibliographie commentée

Le problème d'échange de données secrètes a toujours existé, et ce, depuis la naissance des grandes civilisations. Plusieurs méthodes ont été conçues pour ce propos. La stéganographie est parmi ces méthodes. Elle est plutôt un principe avant tout, qui consiste à camoufler le message secret et elle peut être transmise dans un environnement non sécurisé. On obtient le fichier Stego. Ainsi, l'existence du message est supprimée. Ce point est la carte maîtresse de la stéganographie et c'est pourquoi elle est largement utilisée dans différents domaines d'étude. Les principaux domaines d'application sont l'armée, la défense et les agences de renseignements pour la communication sécurisée de données secrètes [1] et les filigranes numériques [2].

Cette méthode n'est pas tout à fait nouvelle, elle date depuis l'antiquité [3], mais ces techniques sont bien développées avec la globalisation de l'internet. Les images digitales sont souvent utilisées comme objets de couverture dans la stéganographie numérique puisqu'ils présentent plus de redondance.

Les approches de la stéganographie digitale sont classées en deux catégories principales : le domaine spatial et le domaine fréquentiel [4] La première approche consiste à incorporer le message directement dans les pixels (l'unité de l'image) de l'image de couverture, c'est la stéganographie d'image à bit le moins significatif (LSB) [4], tandis que dans la deuxième approche, l'image de couverture est d'abord transformée dans le domaine des fréquences, puis le message secret est

incorporé. Les techniques du domaine de fréquentiel sont donc plus robustes. Les techniques envisageables de ce domaine sur la transformée de Fourier rapide, la transformée en cosinus discrète (TCD)[5], la transformée en ondelettes discrètes (DWT), etc. Je m'intéresse plutôt à la LSB et à la TCD. Afin de tester leur efficacité, il existe des critères qu'on liste :

- La robustesse : Les données incorporées ne doivent pas être corrompues lorsque les données Stego sont exposées à des attaques telles que comme le filtrage linéaire et non-linéaire, ou le flou, l'insertion de bruit aléatoire, la rotation et la mise à l'échelle, le recadrage ou le découpage, la compression, etc.

- L'imperceptibilité : les données Stego doivent être identiques à des données ordinaires. Aucun utilisateur ou logiciel ne doit pouvoir douter que le fichier Stego contienne d'autres données.

- la capacité de charge utile : elle représente la quantité d'informations confidentielles qui peuvent être stockées dans les données de couverture. La méthode stéganographie vise à transporter le maximum de données confidentielles en modifiant le moins possible les données de couverture.

Problématique retenue

Quel modèle retenir pour représenter l'image ? comment exploiter ce modèle pour cacher un message secret ?

Objectifs du TIPE

-Je crée un premier algorithme pour cacher un simple nombre binaire en changeant la valeur la moins significative de chaque pixel.
-Je cherche par la suite à cacher des données de poids significatifs comme un texte ou une image.
-L'image peut aussi être représentée dans le domaine fréquentiel , comme somme des images bases . La transformé en cosinus discrete est connu pour la compression de l'image,en supprimant les amplitudes de poids faibles. J'exploite cet algorithme autrement en cachant le message dans ces coefficients.(prototype)
-J'évalue les algorithmes en essayant d'optimiser l'imperceptibilité .

Références bibliographiques (ETAPE 1)

[1] NOAH SHACHTMAN : FBI: Spies Hid Secret Messages on Public Websites :
https://www.wired.com/2010/06/alleged-spies-hid-secret-messages-on-public-websites/
[2] INGEMAR J. COX, MATTHEW L. MILLER, JEFFREY A. BLOOM, JESSICA FRIDRICH, TON KALKER : Digital Watermarking and Steganography
[3] La stéganographie au cours des siècles :
http://www.bibmath.net/crypto/index.php?action=affiche&quoi=stegano/histstegano
[4] DR. MIKE POUND : Secrets Hidden in Images (Steganography) - Computerphile :
https://www.youtube.com/watch?v=TWEXCYQKyDc&t=642s
[5] Codage JPEG et transformation en cosinus discrète :
http://sorciersdesalem.math.cnrs.fr/Vulgarisation/JPEG/jpeg-DCT.html

DOT

[1] *- Explorer des applications qui cachent des messages dans des images, des audios et des textes pour assimiler le principe.*

[2] *- Recherche bibliographique sur les différents types de la stéganographie digitale et ses applications.*

[3] *- Se focaliser sur le media : l'image digitale et la recherche des différentes représentations (RGB, CMYK) .*

[4] *- Recherches bibliographiques précises sur les méthodes de la stéganographie.*

[5] *- Préparation de l'environnement (python – Jupyter notebook - les modules) et s'approprier avec elles.*

[6] *- Premiers tests : expérimenter avec la première méthode en cachant des citations et des images. Cela a donné un bon résultat, malgré le manque de la robustesse.*

[7] *- Etude de la deuxième méthode, qui représente une image dans le domaine fréquentiel, la proposition de la démarche,la rencontre des problèmes techniques,l'algorithme ne donne pas le résultat souhaité et conclusion.*