Stéganalyse

Compte rendu cryptologie INFO002

LOMBARDI Alexis - CARRILLO Killian

Sommaire

Définitions

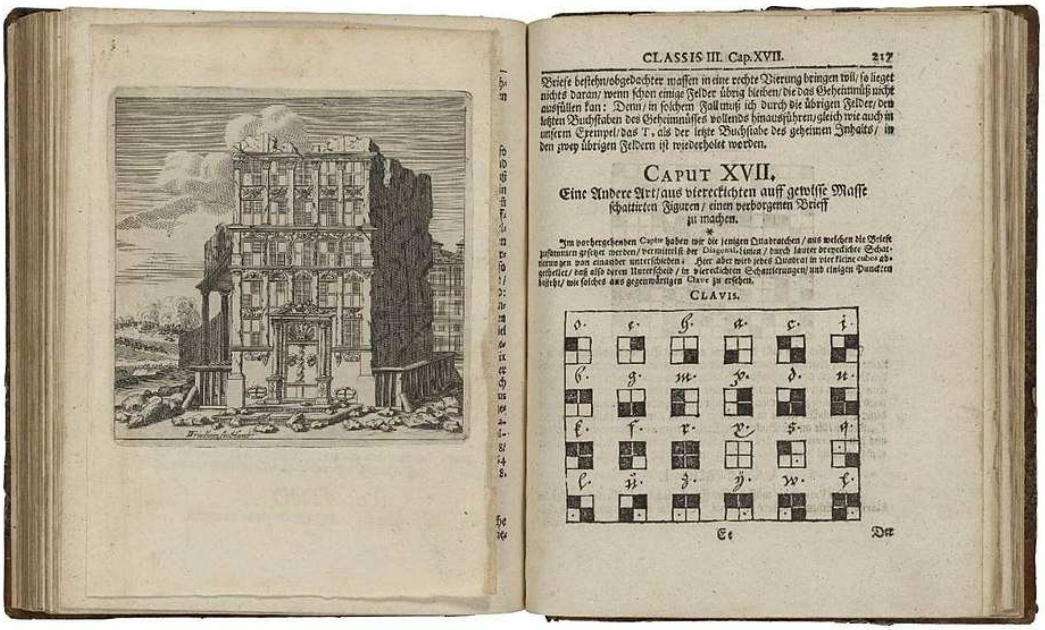
La Stéganographie

Pour savoir ce qu’est la stéganographie, il faut commencer par définir la stéganographie.

“ La **stéganographie** est un domaine où l'on cherche à dissimuler discrètement de l'information dans un média de couverture (typiquement un signal de type texte, son, image, vidéo, etc.). Elle se distingue de la cryptographie qui cherche à rendre un contenu inintelligible à autre que qui-de-droit. Lorsqu'un acteur extérieur regarde un contenu cryptographié il peut deviner la nature sensible de l'information qui lui est cachée. L'intérêt de la stéganographie réside précisément dans la possibilité de communiquer en échangeant des contenus d'apparence anodines de telle sorte à ne pas éveiller de soupçons.”

- Wikipédia

La stéganographie existe depuis de nombreuses années, ainsi il existe différentes manières pour cacher un message. Par exemple:



CLASSIS III. Cap. XVII. 217

Briefe bestehn/obgedachter massen in eine rechte Vierung bringen will/ so lieget nichts daran/ wenn schon einige Felder übrig bleiben/ die das Geheimnüß nicht ausfüllen kan: Denn/ in solchem Fall muß ich durch die übrigen Felder/ den letzten Buchstaben des Geheimnüsses vollends hinausführen/ gleich wie auch in unserm Exempel/ das T, als der letzte Buchstabe des geheimen Inhalts/ in den zwey übrigen Feldern ist wiederholet worden.

CAPUT XVII.

Eine Andere Art/ aus viereckichten auff gewisse Masse schattirten Figuren/ einen verborgenen Brieff zu machen.

Im vorhergehenden Capite haben wir die jenigen Quadraten/ aus welchen die Briefe zusammen gesetzet werden/ vermittelst der Diagonal-linien/ durch lauter dreyeckichte Schattierungen von einander unterschieden. Hier aber wird jedes Quadrat in vier kleine oder abgetheilet/ deß also deren Unterscheid/ in viereckichten Schattierungen/ und einigen Punckten besteht/ wie solches aus gegenwärtigen Clave zu ersehen.

CLAVIS.

Et Der

En 1684, Johannes Balthasar Friderici a réalisé un moyen de cacher du texte dans une image. Ce message est codé grâce aux fenêtres de l’immeuble. Le message est “WIR HABEN KEIN PULVER MEHR” (nous n'avons plus de poudre).

L’image de gauche possède une image cachée, l’image de droite. Celle-ci est obtenu en ne gardant que les 2 bits les moins significatifs de chaque composante de couleur.

La Stéganalyse

La stéganalyse est un peu l’opposé de la stéganographie, car au lieu de cacher un message, il va plutôt le rechercher.

“La stéganalyse est l'ensemble des techniques destinées à découvrir un message caché dans un média (image, vidéo, son, texte...).”

- Wikipedia

“La stéganalyse est le procédé de détection de la stéganographie en regardant la variation entre les patterns non naturels et/ou avec un volume élevé.”

- TutorialsPoint

On peut ainsi se demander quels sont les objectifs de la stéganalyse.

Les objectifs

L’objectif de la stéganalyse est le même que celui de la cryptanalyse envers la cryptologie mais pour la stéganographie.

C’est-à-dire de déceler la présence d’un message qui est caché dans un média comme une image,un son ou encore une vidéo, il est possible alors après la détection de modifier l’image avec la même méthode de stéganographie pour changer des informations importantes ou encore de tout simplement les détruire ou bien tout simplement récupérer les informations cachées pour les exploiter si celles-ci sont sensibles.

Depuis 2021 jusqu'à 2024, l'europe réalise un projet nommé "UnCover". Son but est de lutter contre la criminalité qui utilise de plus en plus les méthodes de stéganographie. Ainsi pendant une enquête criminelle, cet outil pourra être utilisé.

Des pirates peuvent aussi utiliser la stéganalyse pour détruire un tatouage caché d'un film, d'une image ou autre pour ne pas pouvoir faire le lien entre un utilisateur qui a les droits.

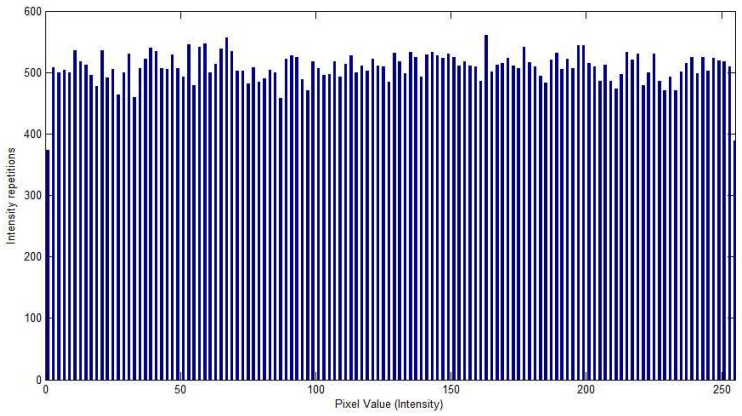
Les différentes méthodes

La méthode par statistiques

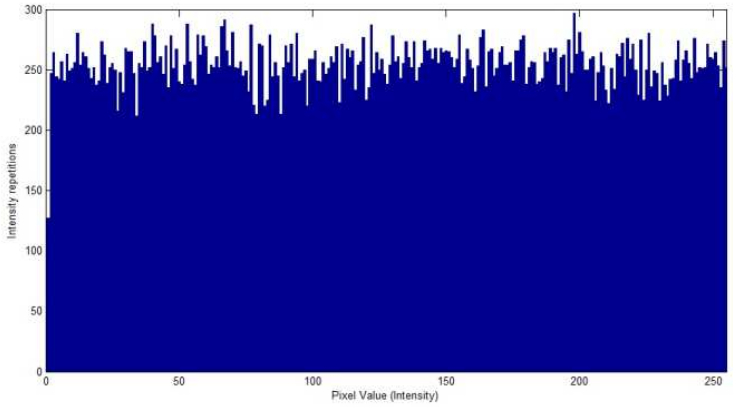
Cette méthode nécessite de connaître d'avance certaines propriétés statistiques, puis à partir de ces données il sera possible de retrouver des "paternes". Ces propriétés sont récupérées à partir de données déjà traitées (on part du message caché avec le média utilisé).

Pour comprendre et expliquer les propriétés, il faut de solides compétences en mathématiques, nous ne pourrons donc pas vous l'expliquer (si vous êtes courageux voici un document assez complet https://hal-utt.archives-ouvertes.fr/hal-02470070/document).

On peut maintenant déceler des anomalies dans un média comme un pixel d'une couleur trop différentes. Pour le détecter on peut, par exemple, comparer les histogrammes de deux images.



Histogramme d'une image sans message caché (avec certains taux de compression)



Histogramme d'une image avec un message caché

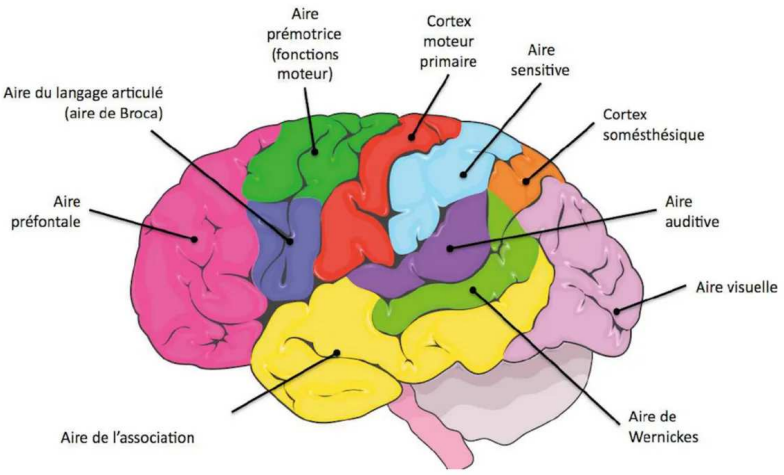
Les deux histogrammes ont été créés à partir du nombre de pixel d'une certaine couleur. Ainsi dans la première image, on peut remarquer que certaines couleurs n'apparaissent jamais. Cela est dû au taux de compression. Cependant si on ajoute un message caché sur la même image, on peut obtenir l'histogramme de l'image 2.

Par exemple, pour vérifier qu'il n'y est pas de message caché dans une vidéo, on peut regarder image par image que l'histogramme ne varie pas d'un seul coup…

La méthode par machine learning

La méthode par machine learning utilise la méthode par statistique, car l'IA est adaptée à la détection de paternes. Ainsi depuis 2015, la stéganalyse utilise le deep learning.

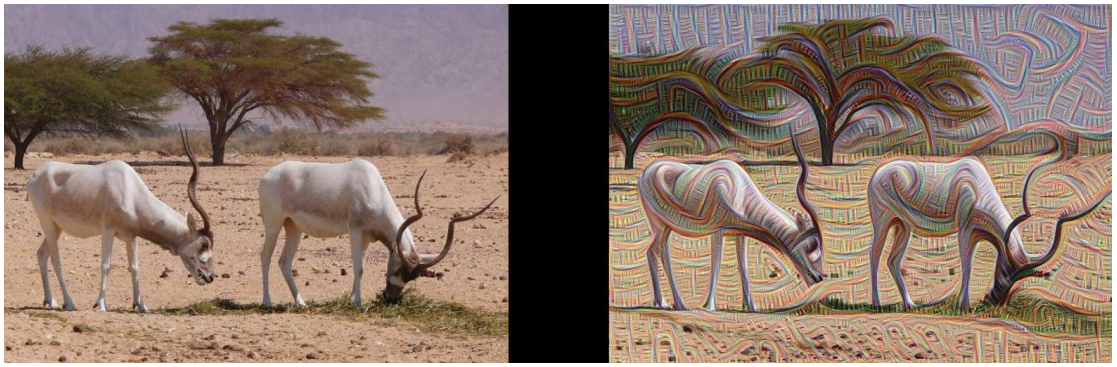
Le type de réseau neuronal utilisé est appelé convolutif ou CNN pour "Convolutional Neural Networks". Sa particularité est que l'on va créer un motif de connexion inspiré du cortex visuel des animaux (dans le cerveau). C'est la partie la plus à droite de l'image ci-dessous (appelée aire visuelle).



Représentation des différentes parties du cerveau

Dans cette partie du cerveau, les neurones vont se chevaucher en fonction de notre champ visuel. Ces neurones sont séparés en deux types: ceux qui traitent une petite partie de l'image et ceux qui mettent en commun. C'est comme cela que nous percevons une image.

Google à développé un programme de vision par ordinateur appelé DeepDream. Le but de cette IA est de générer une image à partir d'objet appris.
A partir de l'image de gauche, l'IA va "découper" l'image en petit morceau, puis les relier pour former l'image de droite. Voici comment "voit" une intelligence artificielle.



Exemple d'image et de son traitement par DeepDream

Maintenant il suffit d'entraîner une IA dont le but est de détecter des presets sur différents supports: image, vidéo, son, texte pour détecter si un message est caché.

La méthode par signature

Le but de cette méthode est de chercher une trace ou une signature dans le média en question. Ces traces sont laissées par les outils de stéganographie ce qui

représente une faille dans l'outil. Le but de ces outils est de laisser aucune trace possible car chaque trace est une faille exploitable.
Par exemple, le logiciel hide and seek dans une ancienne version, croppait ou faisait du padding d'une image qui n'avait pas la bonne taille en ajoutant des pixels noirs supplémentaires :

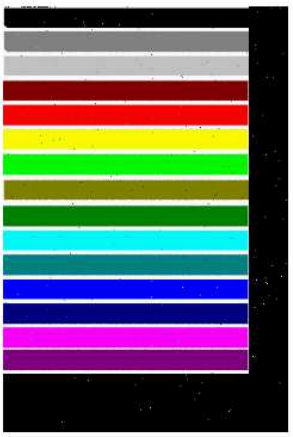


Fig. 3. Example of padding method Created using *Hide and Seek v4.1*

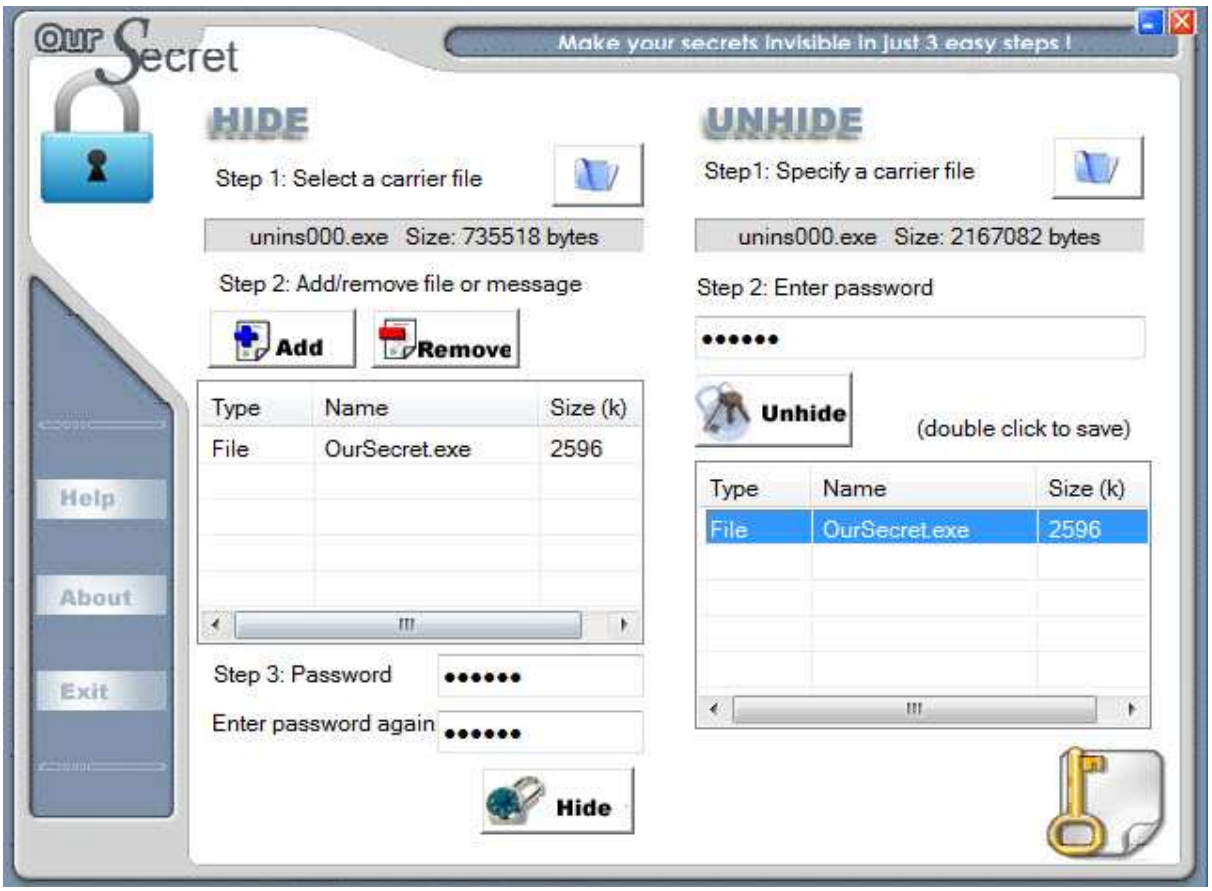
Ceci permettait donc à des personnes faisant de la stéganalyse de voir un nombre anormal de pixel noirs ce qui laisse entendre la possibilité d'un message caché par le logiciel Hide and Seek et donc en ayant le logiciel on a la méthode de stéganographie utiliser ce qui permet potentiellement de découvrir le message ou alors il est possible de tout simplement le détruire.
Il existe d'autre histoire de faille importante d'un logiciel comme des messages laissés après l'EOF d'une image ou encore des données aberrantes comme ceci :

Couleurs obtenues après un message dissimulé révélant une suite de données aberrantes

Toutefois cette méthode est très chronophage, en effet il faut tester et chercher jusqu'à la plus petite faille pour des fois seulement savoir qu'il y a un message crypter et rien de plus. Néanmoins, la méthode est fiable, car si on a la signature d'un logiciel alors on est sûr de la présence d'un message dissimulé.

Outils

Il existe un nombre important d'outils de stéganalyse, néanmoins, ils sont dans la majorité des cas inutiles seuls et ont besoin d'être complété par d'autres.
En effet, il existe une multitude d'outils de stéganographie, chacun ayant leur propre faille et méthode pour dissimuler un message. C'est pour cela qu'il y a besoin d'une multitude d'outils de stéganalyse pour tester toutes les failles possibles.
Certains logiciels comme StegSeek sont spécialement conçus pour voir les messages de StegHide.
Voici par exemple un outil permettant la stéganographie : OurSecret:



Imaginons que celui-ci soit utilisés à des fins criminelles alors comment décrypter les messages.

Le projet Uncover qui est un projet européen pour la lutte contre la criminalité sur internet. Il a pour but de faire avancer la stéganalyse pour détecter et corrompre les réseaux criminels utilisant la méthode de la stéganographie pour cacher leurs messages codés.

Le but d'Uncover est d'aider la police et d'autres personnes combattant la criminalité en fournissant les outils nécessaires au décryptage des messages dissimulés.

Conclusion

La stéganalyse est déjà fonctionnelle depuis plusieurs années.
Il est ainsi possible de détecter des messages cachés (si les techniques sont déjà connues). Cependant il reste beaucoup de choses à améliorer, car la stéganographie est de plus en plus utilisée par les criminels, et s'ils utilisent de nouvelles techniques, alors il faudra apprendre à détecter des presets.
Les études menées sur la stéganalyse ont surtout été utilisés pour des images en noir et blanc, ainsi l'analyse d'image en couleur est à explorer.
Enfin il est plus simple de détecter un message que de le récupérer, ce point est donc à être amélioré.