Malavasi Adrien
Ferreira Yvain

Stéganographie et Tatouage

Définitions :

La cryptographie sert à rendre un contenu indéchiffrable en le cryptant notamment.

La stéganographie et le tatouage servent à rendre un contenu indistinguable à l'aide d'un support (message sonore, un texte, des images , de la vidéo, des programmes informatiques, des partitions musicales, etc...).

La stéganographie permet de cacher l'existence même d'un message.

La cryptographie et la stéganographie / tatouage peuvent être utilisés complémentairement.

Comparaison :

Le tatouage se rapproche plus de la stéganographie que de la cryptographie, à quelque différences près :

-En stéganographie, l'existence du message doit être cachée, on recherche une indiscernabilité statistique, alors pour le tatouage on peut savoir qu'il y a une information cachée, le but recherché étant une indiscernabilité perceptuelle (on parlera alors de masquage psycho-perceptif).

-En stéganographie, le message de couverture n'est pas important, alors qu'en tatouage, il est primordial et ne doit pas être dénaturé. On va moduler la couverture par le message de tatouage, mais on veut que ce dernier reste utilisable par un humain. La plupart du temps, on se donne un budget de distorsion, une quantité de distorsion que l'on s'autorise à infliger à la couverture, qui reste dans les limites de l'imperceptible. Le lien entre le message caché et le support est donc beaucoup plus fort.

Contraintes :

Le tatouage possède trois contraintes principales : la capacité, la robustesse et la sécurité.

-Capacité : quantité d'information que le tatouage véhicule, exprimée généralement en nombre de bits.
Plus on cache de bits, plus la distorsion augmente ; et au contraire, à distorsion fixée (ce qui est généralement le cas en pratique), on cachera seulement un certain nombre de bits. Le tatouage est pour une bonne part une affaire de compromis.

-Robustesse : puissance des attaques/manipulations pouvant être infligées à la couverture sans que le tatouage soit affecté. S'il faut dégrader le support jusqu'à la rendre inutilisable pour rendre le tatouage inopérant, alors le tatouage est efficace. Toutefois, la variété des manipulations que peut subir la couverture rends la conception d'un tatouage robuste si compliqué que l'on a pas encore résolu aujourd'hui à en produire pour tous les types de couvertures.

-Sécurité : en approximation, on peut dire qu'elle consiste à cacher aussi la clef secrète. Autrement dit, si un pirate observe plusieurs contenus tatoués, il ne faudrait pas qu'il puisse deviner la clef secrète, c'est ici qu'interviennent plusieurs principes de la cryptographie afin de cacher la clé.

Réalisation :

L'information adjacente est une des caractéristiques qui fondent les domaines de la stéganographie et du tatouage.
C'est un ensemble de formules mathématiques que l'on applique pour tatouer un message sur un support. (voir le pdf ci dessous page 18 à 20)
http://laris.univ-angers.fr/_resources/logo/DEAHeraultRomain.pdf
Par exemple, sur une image, on se sert des trois pixels supérieurs et inférieur à celui que l'on veut modifier pour camoufler la donnée, ce qui crée un flou, c'est là que la contrainte de capacité entre en jeu.

Pour la stéganographie comme pour le tatouage, la clef secrète servira à mettre en évidence le message caché.

Exemples d'application :

-Authentification :

L'authentification de l'origine d'un document est primordiale dans les applications de reconnaissance militaire par exemple.
De même, une chaîne de télévision ou une agence de presse souhaite pouvoir authentifier les images reçues d'un reporter : c'est la notion de « caméra-vérité » (true camera), qui permet de certifier la provenance de l'information.
L'insertion d'un tatouage permet alors d'authentifier la provenance d'un document.
Pour être réellement crédible, il faut que l'insertion de la marque soit réalisée au plus près de l'acquisition.

-Preuve de propriété :

La preuve de propriété appartient à la classe des applications de protection du droit d'auteur.
Ici, le tatouage est utilisé comme une signature permettant de prouver qu'une œuvre donnée a bien été créée par un certain utilisateur.
Le tatouage doit donc ici avoir une valeur juridique, ce qui implique certaines contraintes particulières.

-Traçage de contenu (fingerprint) :

Il consiste à insérer dans l'œuvre un identifiant caractéristique de l'acquéreur ou distributeur, ce qui permet de déterminer l'auteur d'une diffusion illégale lorsque l'on retrouve un document piraté.
Cet outil de traçage a pour but de dissuader le piratage.

Sources :

http://laris.univ-angers.fr/_resources/logo/DEAHeraultRomain.pdf

https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-135.htm#

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

http://laris.univ-angers.fr/_resources/logo/DEASimonAntoine.pdf