Qu'est-ce que la Stéganographie

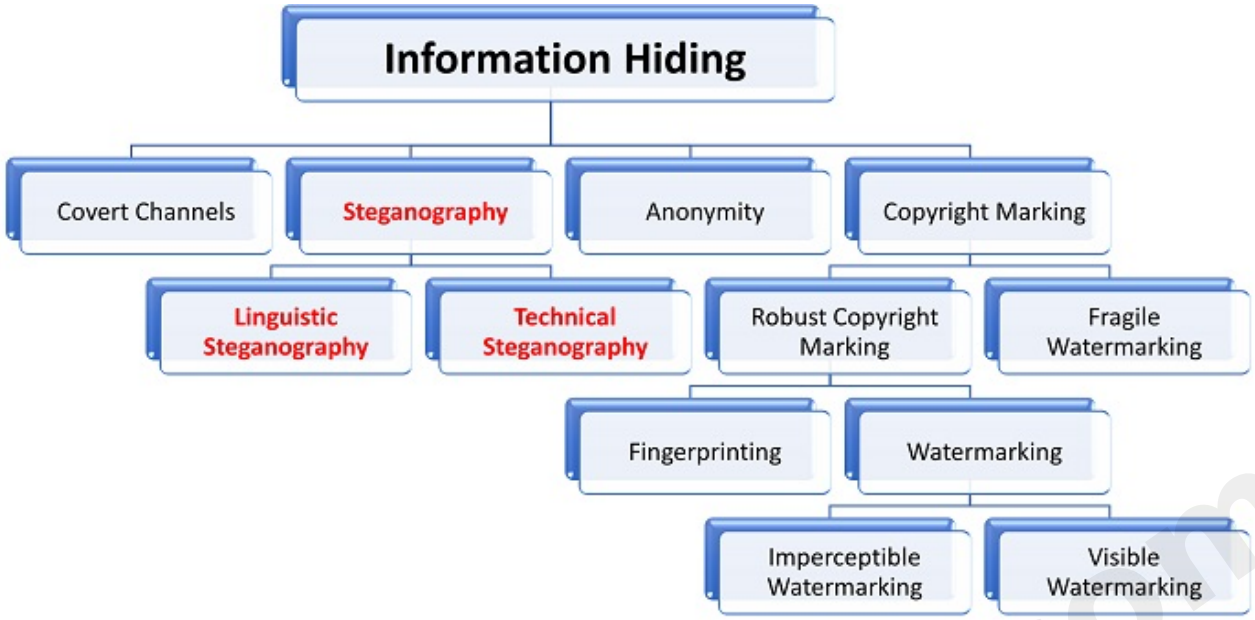
[sommaire]

1. **Objectifs**

- Connaitre la Stéganographie

- **La dissimulation d'informations**
  - La dissimulation d'informations est une branche de l'informatique qui traite de la dissimulation de l'existence d'un message
  - Il est lié à la **cryptographie** dont l'intention est de rendre les messages illisibles sauf par les destinataires prévus
  - Il utilise des technologies issues de nombreuses disciplines scientifiques :
    - Traitement numérique du signal (images, audio, vidéo)
    - Cryptographie
    - Théorie de l'information\Théorie du codage
    - Compression des données
    - Perception visuelle/auditive humaine
  - Il existe quatre sous-disciplines principales de la dissimulation d'informations
    - Steganography (Stéganographie)
    - Watermarking (Filigrane)
    - Covert Channels (Canaux secrets)
    - Anonymity (Anonymat)
  - Stéganographie, Sécurité réseau, Université d'Okara

apcpedagogie.com



- ## Définitions et Terminologies de Stéganographie

  - Le mot `stéganographie` (en anglais : steganography ou data hiding) tire son origine d'une étymologie grecque : steganos signifiant caché, couvert et graphos signifiant écriture, dessin. Ainsi nous pouvons en déduire que la stéganographie est l'art de cacher des messages secrets au sein de messages plus anodins.
  - La `stéganographie` est la technique consistant à insérer un fichier dans un second fichier, sans que l'aspect extérieur de ce dernier ne soit modifié (hormis sa taille).
  - La `stéganographie` est la technique consistant à cacher des données secrètes dans un fichier ou un message ordinaire, non secret, afin d'éviter toute détection. les données secrètes sont ensuite extraites à leur destination. L'utilisation de la stéganographie peut être combinée avec le cryptage comme étape supplémentaire pour cacher ou protéger les données.
  - Le mot `stéganographie` est dérivé des mots grecs **steganos** (signifiant caché ou couvert) et de la racine grecque **graph** (signifiant écrire).
  - Le mot `stéganographie` vient du grec "steganos" (caché ou secret) et "graphy" (écriture ou dessin) et signifie littéralement "écriture cachée".
  - Si la cryptographie est l'art de secret, la `stéganographie` est l'art de dissimulation : son objet est de faire passer inaperçu un message secondaire dans un message primaire. Le message primaire reste lisible à tous, tandis que le message secondaire n'est lisible que par une ou plusieurs personnes propriétaires d'une information secrète.
  - Le plus souvent, la `stéganographie` est appliquée aux images, mais de nombreux autres types de données ou de fichiers sont possibles: l'audio, Vidéo, Texte, Programmes exécutables, Liens

- ## Histoire de Stéganographie

  - L'apparition de la stéganographie est très ancienne et elle est à peu près contemporaine de celle de la cryptographie.
  - La première trace écrite se trouve dans les histoires de l'historien grec Hérodote, parues vers 445 av J.-C, à travers deux récits. Le premier relate l'histoire d'Histiée, ancien tyran de Milet, qui incite son gendre d'Aristagoras, le nouveau tyran de Milet, à se révolter contre son roi Darius. Pour transmettre son message à Aristagoras, il eut l'idée de raser la tête de son esclave le plus fidèle, de lui tatouer son message sur le crâne et d'attendre que les cheveux repoussent avant d'envoyer l'esclave pour Milet, avec pour consigne de se faire raser les cheveux. Un autre passage des histoires relate l'histoire de Demarate, ancien roi de Sparte réfugié auprès du roi des Perses, Xerxès Ier, qui a succédé à Darius. Demarate fut mis au courant d'un projet d'invasion de la Grèce. Il décida alors de prévenir Sparte en toute discrétion en utilisant le stratagème suivant : « il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis » Les tablettes étant arrivées à Sparte, la reine Gorgô fit gratter la cire et découvrit ainsi le message de Démarate.
  - La **stéganographie** (sous forme d'encre invisible) a été utilisée par Washington pendant la guerre d'indépendance. Avant la guerre civile, les courtepointes étaient cousues avec des motifs spéciaux pour indiquer aux esclaves en fuite dans quelle direction aller et quoi faire

    > *Le concept de dissimulation de messages n'est pas nouveau – il existe depuis des siècles. Un Grec a rasé la tête d'un esclave, a écrit un message, puis a attendu que les cheveux repoussent avant d'envoyer l'esclave à sa destination.*

  - Dans les années 1980, certains des documents du cabinet de Margaret Thatcher ont été divulgués à la presse. Elle a ordonné que les traitements de texte utilisés par les employés du gouvernement encodent leur identité dans l'espacement des mots des documents

- ## méthodes de stéganographie

  - Les histoires racontées par Hérodote illustrent déjà les deux principales méthodes de stéganographie utilisées au cours des siècles.
  - On pourra essayer de **cacher physiquement l'existence d'un message**, comme sur le crâne d'un esclave. Ou alors on **dissimulera le message sur un support qui transmet déjà de l'information**, comme les tablettes de cire.
  - Ces deux méthodes ont toujours cohabité, même si la seconde fut sans doute plus populaire.

apcpedagogie.com

- Une autre technique de stéganographie est l'**utilisation d'encres sympathiques** ou invisibles. Cette technique était très utilisée au moyen âge pour envoyer des messages secrets.
- On écrit, au milieu des textes écrits à l'encre, un message à l'aide de jus de citron, de lait, de certains produits chimiques. Il est invisible à l'œil, mais une simple flamme, ou un bain dans un réactif chimique, révèle le message.
- Durant la seconde guerre mondiale, en plus des techniques de l'encre invisible, des méthodes plus sophistiquées furent utilisées à l'aide de moyens modernes, comme les microfilms cachés sous des timbres postes ou sur des couvertures de magazine. Les microfilms sont de toutes petites photographies (de la taille d'un caractère), mais qui peuvent contenir l'équivalent d'une page de livre. Cette technique était très appréciée par les Allemands

Domaines de stéganographie

- La stéganographie est divisée en deux domaines, **spatial** et **fréquentiel**. Dans le domaine spatial, le message secret est inséré dans les pixels de l'image porteuse, tandis que dans le domaine fréquentiel, les pixels sont transformés en coefficients, et le message secret est inséré dans ces coefficients.

- **Domaine spatial**
  - La stéganographie spatiale consiste à faire changer des bits de pixels de l'image pour insérer les bits du message secret. La technique LSB est l'une des techniques la plus simple et la plus répandue.
  - Elle consiste à cacher un message secret dans les bits de poids faible des pixels de l'image, de sorte que les distorsions apportées par le processus d'insertion restent non perceptibles.
  - La raison est que pour l'œil humain, les variations de la valeur du LSB sont quasiment imperceptibles. L'insertion de bits de message secret peut être faite séquentiellement ou de façon pseudo aléatoire.
  - La stéganographie par substitution de LSB et la stéganographie par correspondance de LSB sont des exemples de techniques de stéganographie dans le domaine spatial.

- **Domaine fréquentiel**
  - Le message est inséré dans les coefficients transformés de l'image, ce qui a pour effet d'apporter plus de robustesse contre les attaques. La stéganographie fréquentielle est une technique essentielle de dissimulation de l'information secrète : de nos jours, la plupart des systèmes de stéganographie opèrent dans le domaine fréquentiel.

apcpedagogie.com

    - La stéganographie fréquentielle va ainsi permettre de cacher l'information dans des zones de l'image moins sensibles à la compression, au recadrage et aux divers traitements de l'image, [Raja et al.,2004].
    - Dans la suite nous rappelons les principes des différentes techniques de transformation dans le domaine fréquentiel.

Cryptographie vs stéganographie

- La cryptographie et la stéganographie sont deux techniques différentes de protections des données numériques :
    - La cryptographie permet d'échanger des messages illisibles afin que seules les personnes autorisées puissent les lire. Dans ce cas, la sécurité repose sur l'incompréhensibilité de message transmis, par contre, la sécurité de la stéganographie dépend de la question de l'existence du message secret.
    - La cryptographie protège un document numérique durant sa transmission. Après la réception et le décryptage, ce document devient clair et non protégé. Donc il peut être facilement copié et distribué. À la stéganographie le message secret resté protégé même après la réception.
    - Une autre différence au niveau des attaques, en cryptographie, le pirate va essayer de décrypter le message, tandis qu'en stéganographie l'attaquant va essayer de détecter l'objet de couverture.

Logiciel de stéganographie

- Le logiciel de stéganographie est utilisé pour exécuter diverses fonctions afin de masquer les données, y compris le codage des données afin de les préparer à être masquées dans un autre fichier, le suivi des éléments du fichier texte de couverture contenant des données masquées, le cryptage des données pour être caché et extraire les données cachées par son destinataire.
- Il existe des programmes propriétaires ainsi que des programmes open source et d'autres programmes gratuits disponibles pour faire de la stéganographie. OpenStego est un programme de stéganographie open source ; d'autres programmes peuvent être caractérisés par les types de données pouvant être masquées ainsi que par les types de fichiers dans lesquels les données peuvent être masquées.
- **Stéganographie d'image** : cette application est un outil JavaScript utilisé pour masquer des images dans d'autres fichiers image.
    - **OpenStego** : Ce programme est un outil de stéganographie open-source
    - **Xiao Steganography** : Xiao cache des fichiers secrets dans des fichiers WAV ou BMP

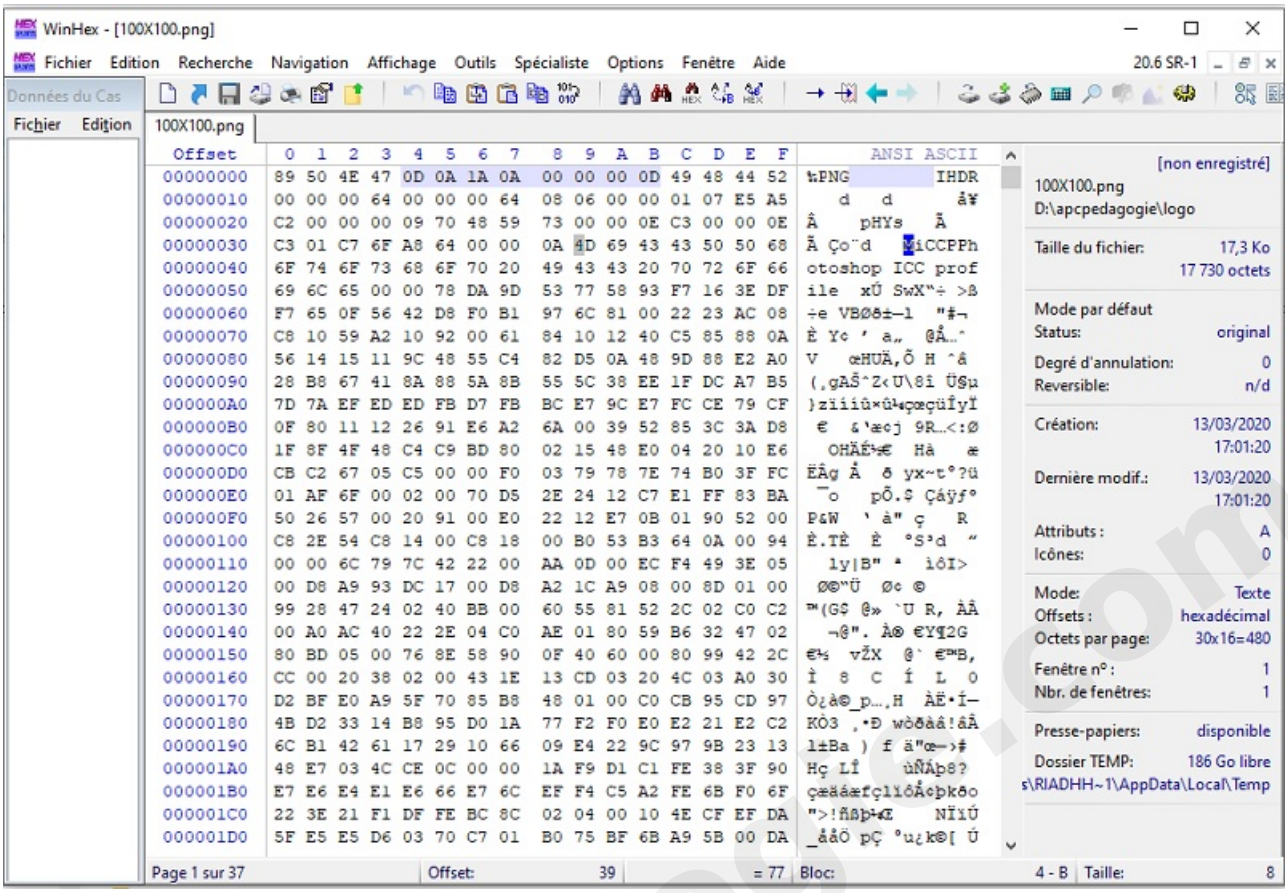
apcpedagogie.com

- **Crypture** : cette application est un outil en ligne de commande utilisé pour effectuer une stéganographie
- **NoClue** : cette application est un outil open source qui masque les informations textuelles dans les fichiers de support vidéo et image.
- **Steganography Master** : Cette application est un outil open source basé sur Android qui peut masquer du texte dans une image et vous donne un outil de décodage pour extraire des messages texte cachés à partir de fichiers image. Il prend en charge plusieurs formats d'image (BMP, JPG, ICO, PNG)
- **Steghide** : Steghide est une application qui cache des données dans différents fichiers audio et image, y compris JPEG, BMP, AU et WAV

Passer des informations numériques

- Faire passer des informations numériques est tout aussi simple. Cacher sa signature dans une image afin que personne ne puisse se l'approprier et en revendiquer la possession est un jeu d'enfant.
- Munissez-vous tout d'abord d'un logiciel adéquat: un éditeur hexadecimal. Pour notre exemple, nous choisirons **WinHEX**, téléchargeable sur http://www.winhex.com.
- Trouvez une image pour effectuer vos tests. Ici, nous prendrons l'image "logo.png", qui représente le logo de **apcpedagogie.com**.
- **1.** Ouvrez **Hex.edit** et faites Ouvrir
- **2.** Ouvrez votre image (ou n'importe quel autre type de fichier tant qu'il ne s'agit pas d'une application)
- **3.** Vous devriez avoir ce type de fenêtre

apcpedagogie.com



- **4.** A gauche se trouve la translation HexaDécimale des données qui s'affichent à droite (et qui sont incompréhensibles)
- **5.** Peu nous importent les données HexaDécimales. Repérez en haut, dans la colonne de droite, les espaces vides (caractérisés par des points qui s'ensuivent sur plusieurs lignes)
- **6.** C'est dans cette zone que devront se porter nos travaux. A la place de ces points, écrivez un petit mot. Ici nous écrirons : stegano, et, très important, ne laissez jamais d'espaces dans vos messages, mettez-y des points. Notez que cela aurait tout aussi bien pu être le nom d'une société ou d'une personne, propriétaire des droits de l'image.
- **7.** Sauvegardez l'image sous un autre nom (dans le menu: File puis Save as). Il est très important de prendre cette précaution car une mauvaise manipulation peut avoir des résultats désastreux. sur ce type de fichiers.
- **8.**Ouvrez de nouveau l'image afin de voir si les modifications n'ont pas posé de problèmes.

- ## Application: Cryptographie ou stéganographie ?

  Pour chacun des exemples historiques ci-dessous, préciser s'il s'agit de **stéganographie** ou de **cryptographie**.

  - **Question1:** En-480, **Démarate** informe Sparte d'une attaque imminente, en gravant cette information sur une plaquette de bois ensuite recouverte de cire vierge, afin de ne

pas faire prendre de risque à l'esclave qui transportera la tablette.

- **Question 2:** Au V^{e} siècle avant notre ère, les Hébreux remplacent chaque lettre du texte en clair par une autre lettre de l'alphabet choisie de la manière suivante :A devient Z,B devient Y, etc.
- **Question 3:**En 1518, Jean Trithème remplace chaque lettre du texte en clair par un group e de mots, le texte chiffré ressemblant alors à un poème.
- **Question 4:** En 1623, Francis Bacon représente chaque lettre du texte en clair par un group e de 5lettres A ou B. Le texte codé résultant est ainsi constitué d'une succession de ces deux lettres.
- **Question 5:** Pendant la Seconde Guerre mondiale, les Allemands réduisent la photo d'une page entière en un p oint de moins d'un millimètre apposé sur une autre page au contenu sans importance.
- **Question 6:** Toujours pendant la Seconde Guerre mondiale, les Allemands ont utilisé la machine Enigma : chaque lettre est remplacée par une autre, l'astuce est que la substitution change d'une lettre à l'autre.

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/quest-ce-que-la-steganographie · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com