Qu'est-ce que le watermarking

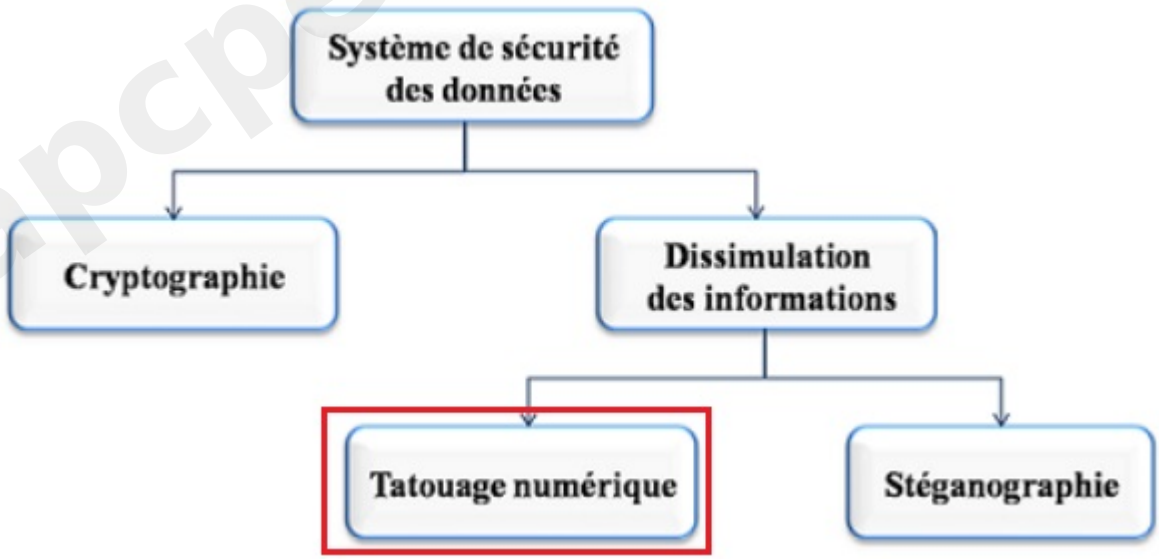
[sommaire]

1. **Objectifs**

- Connaitre le watermarking

- **Définitions**

- Le tatouage (appelé aussi filigrane en anglais `watermark`) est une technique qui trouve ces origines dans le marquage des documents papier et des billets.
- Le `watermarking`, aussi appelé tatouage numérique, est une empreinte, visible ou non visible, inscrite sur ou dans un support médiatique. Selon le format du support, l'empreinte est visuelle ou sonore. Elle permet d'identifier le contenu et son créateur à tout moment.
- Le tatouage numérique (en anglais digital `watermark`, "filigrane numérique") est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, vidéo, une image ou un autre document numérique.
- À ses débuts, le `watermarking` était une technique uniquement utilisée sur papier. Par exemple, sur des billets de banque ou des timbres. On marquait, tatouait, un papier en modifiant son épaisseur. Ainsi, la marque consistait en un jeu d'ombre et de lumière, visible sous un faisceau lumineux.

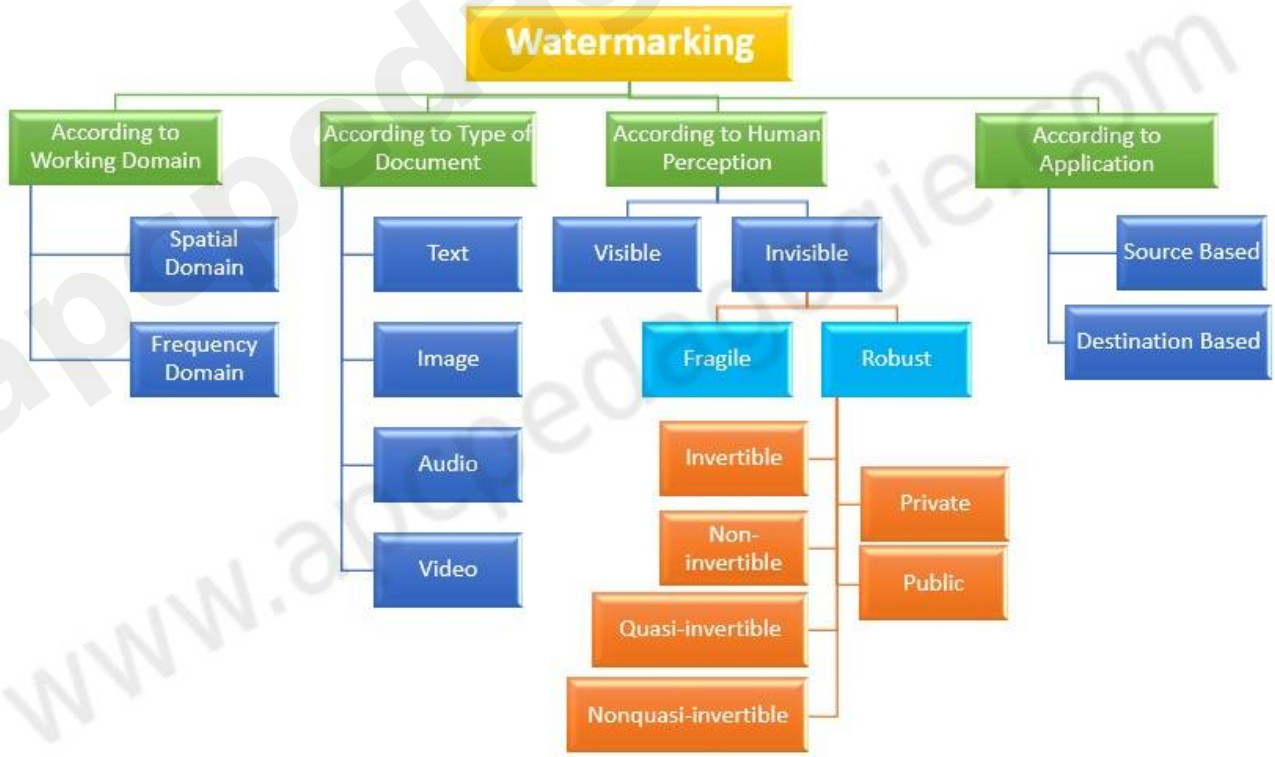


- **Historique de watermarking**

apcpedagogie.com

- Quoique la fabrication du papier ait été inventée en Chine plus de mille ans, le tatouage du papier n'est apparu qu'en 1282 en Italie. Il a été utilisé intensivement au 18 ème siècle en Amérique et en Europe comme marque et méthode contre la falsification des livres et d'argent
- Le terme digital watermark (tatouage numérique) fut pour la première fois employé en 1992 par Andrew Tirkel et Charles Osborne2. Le terme utilisé par Tirkel et Osborne est originaire du Japon : denshi sukashi (□□□□) qui se traduit en anglais par **electronic watermark**.
- Depuis 1995, l'explosion du nombre de publications et de brevets à ce sujet a fait du watermarking un domaine majeur surtout en traitement d'image. Très vite, de nombreux laboratoires et industriels se sont intéressés à ce domaine.
- Ce qui est concrétisé par la création de l'atelier IHW (Information Hiding Workshop) en 1996, d'une conférence spécifique au sein de SPIE en 1999 et de l'atelier IWDW (International Workshop on Digital Watermarking) en 2002.
- Quatre journaux dédiés aux problématiques de sécurité de l'information ont été crées :
- IEEE Trans. on **I**nformation Forensics and Security et IEE Proc. Information Security en 2005, LNCS Transactions on Data Hiding and Multimedia security et EURASIP Journal on Information Security en 2006.
- Cette dynamique a induit une prolifération d'entreprises dans le domaine du watermarking.

Les types de tatouage numérique



- **Visible**
  - Une image translucide visible superposée à l'image principale
  - Ce type de watermarking est un texte visible semi-transparent ou une image qui se superpose à l'image principale.
  - Ils permettent à l'image originale d'être évidente et visible, mais elle offre toujours une protection du droit d'auteur en servant de marque sur la propriété du propriétaire.
  - Les filigranes visibles sont une option préférable pour une protection fiable du droit d'auteur, en particulier lorsqu'il s'agit d'images.
- **Invisible**
  - Une image superposée qui ne peut pas être vue, mais qui peut être détectée de manière algorithmique
  - **Fragile**
    - Ces filigranes sont détruits par la manipulation des données. Il doit y avoir un système capable de détecter tous les changements dans les données si des filigranes fragiles doivent être utilisés.
  - **Fragile**
    - Ces filigranes sont détruits par la manipulation des données. Il doit y avoir un système capable de détecter tous les changements dans les données si des filigranes fragiles doivent être utilisés.

Les éléments d’un système de watermarking

- Selon un point de vue généralisé, un système de watermarking est un peu comme un système de communication composé de trois éléments principaux: un émetteur, un canal de communication, et un récepteur.
- Pour être plus précis, l'insertion de l'information à cacher dans le signal hôte joue le rôle de transmission de données; tout traitement appliqué au signal hôte après la dissimulation de l'information, ainsi que l'interaction entre les données de l’information cachée et ceux du signal hôte lui-même, représente la transmission à travers un canal de communication, la récupération de l'information cachée à partir des données de l'hôte joue le rôle de récepteur.

apcpedagogie.com

- Par analogie aux systèmes de communication, tout système de watermarking prend la forme donnée sur la figure suivante.

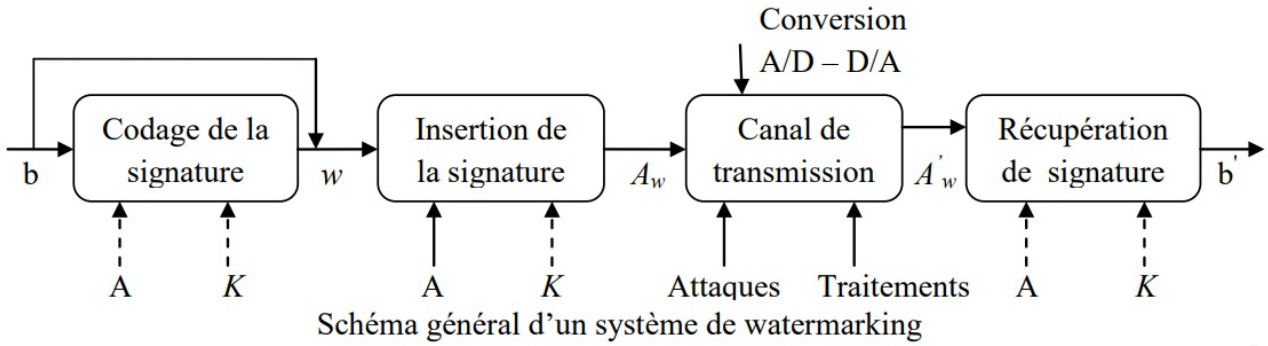


Schéma général d'un système de watermarking

- L'information de la signature à cacher au sein des données du signal hôte représente l'entrée même du système. Sans perdre de généralité, nous supposerons que cette information est donnée sous la forme d'une chaîne binaire: **b= (b_1,b_2 ,.....,b_k)**
- Avec bi ϵ {1,0}. Nous nous référerons à la chaîne b comme étant le code de watermark (à ne pas confondre avec le signal de watermark qui sera présenté plus tard).
- Du côté de l'émetteur, un module d'insertion incruste la chaîne b dans les données du signal hôte. Ce dernier peut être un fichier audio, une image fixe, une séquence vidéo, etc.....
- Il est généralement désigné par le symbole (A) sauf lorsque sa nature exacte ne peut être négligée. Dans ce cas, les images fixes et les vidéos sont désignés par le symbole (I) et l'audio par (S). Le module d'insertion peut accepter une clé secrète K, en tant qu'entrée supplémentaire.
- Une telle clé, dont l'objectif principal est d'introduire un certain secret pendant la phase d'insertion, est généralement utilisée pour paramétrer le processus d'intégration et rendre la reprise ou la détection du watermark impossible pour les utilisateurs non autorisés qui n'ont pas accès à K.
- Donc transmettre un message par le support d'un document comporte trois phases : l'insertion du message dans le support, la diffusion du document marqué et enfin l'extraction du message. Les briques de cet enchaînement résumé par la figure (I.1) seront détaillées dans les sections suivantes.

Stéganographie vs tatouage numérique

- La stéganographie et le tatouage sont deux approches de la dissimulation d'information mais n'ont pas les mêmes objectifs, ni les mêmes contraintes :
  - Dans le cas de la stéganographie, la quantité des données cachées peut aller jusqu'à la dissimulation d'une image entière dans une autre image ou un document dans un autre.

- Dans le cas du tatouage numérique, on cherche à dissimuler une quantité limitée d’information afin de vérifier l’intégrité du document par exemple ou de protéger les droits d'auteur.
- Dans la stéganographie, l'existence d'un message caché doit rester secrète, tandis que pour le tatouage numérique, l’existence du message peut être connue mais il doit rester caché.
- En stéganographie, l’attaquant va tenter de lire le message caché dans le document, alors que dans le cas du tatouage numérique, l’attaquant va essayer par exemple d’usurper l’identité de l’auteur en remplaçant la marque.
- La stéganographie est utilisée pour la communication secrète, tandis que le tatouage est utilisé pour la protection du contenu, la protection des droits d’auteur, l’authentification du contenu et la détection de modification.

Sommaire du cours Administration et sécurité des sites web

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

apcpedagogie.com