Transmission dissimulée d'information grâce à la stéganographie

Victor Halbitte MPI

TIPE Session 2025

La stéganographie consiste à transformer subtilement un support numérique pour y dissimuler des données sans en altérer son apparence. Elle repose sur des techniques permettant de convertir des données visibles en données cachées, assurant ainsi une transmission discrète et donc sécurisée de l'information.

Elle se distingue de la cryptographie en rendant l'information invisible plutôt que chiffrée. J'ai donc trouvé intéressant d'explorer cette technique méconnue, qui offre une approche camouflée de la transmission d'informations, et qui pourrait s'allier à la cryptographie pour sécuriser encore davantage une transmission de données.

Professeur encadrant du candidat : Joshua Peignier

Positionnements thématiques et mots-clés :

INFORMATIQUE (Informatique pratique), MATHEMATIQUES (Analyse)

Mots-clés (Français)	Mots-clés (Anglais)
Stéganographie	Steganography
Image numérique	Digital image
Nombre binaire	Binary number
Bit de poids faible	Least significant bit

Bibliographie commentée :

La stéganographie est une technique qui consiste à dissimuler un message à l'intérieur d'un support, de manière à ce que sa présence passe inaperçue. Elle se distingue de la cryptographie qui, elle, vise à rendre les données indéchiffrables sans se soucier de leur discrétion.

La stéganographie est utilisée depuis l'Antiquité, notamment pour la transmission secrète de messages durant les périodes de guerre. Aujourd'hui, elle trouve des applications dans des domaines variés, tels que la sécurité informatique ou encore la communication discrète entre deux entités. Le principal défi actuel auquel doit faire face la stéganographie réside dans sa capacité à dissimuler les informations de manière suffisamment subtile pour échapper à la détection, notamment par l'intelligence artificielle, tout en garantissant l'intégrité et la confidentialité des données transmises.

Notre étude de la stéganographie se fera en prenant les images numériques comme support de transmission d'information. Pour débuter, il faut pouvoir extraire un par un les pixels de l'image avant de les modifier comme souhaité. Cette étape peut se réaliser à l'aide de la bibliothèque Pillow de Python qui offre de grandes libertés sur la manipulation d'image.

L'approche choisie ici est d'utiliser les bits de poids faibles de l'image qui vont permettre de stocker les données sans pour autant changer considérablement l'aspect visuel de l'image de départ [1][2]. Il est donc nécessaire de parcourir l'image pixel par pixel et de modifier chacun d'entre eux pour y dissimuler les données, préalablement converties en binaire.

La question se pose alors sur les répercussions sur l'aspect visuel de l'image qu'une telle transformation peut provoquer. L'image de départ et celle modifiée par l'algorithme peuvent alors être comparées pour déterminer le degré de différence. On choisira ici la mesure de distorsion PSNR (Peak Signal to Noise Ratio) pour quantifier cette modification de l'image [3].

La stéganographie permet de cacher des données dans un support, mais cette technique se révèle très peu efficace, voire inutile, si une personne tierce a connaissance de cette dissimulation. En effet, les données n'étant pas chiffrées, il est très facile de reconstituer le message de départ une fois les données extraites. Le chiffrement [5] des données avant la dissimulation peut alors être une solution efficace pour garantir encore plus la sécurité lors du transfert des données par stéganographie.

Un autre problème majeur de la stéganographie apparaît lorsque l'on souhaite compresser l'image. Par exemple, la compression JPEG avec perte vise à supprimer les détails fins de l'image pour obtenir un fichier entre 3 et 100 fois plus petit que l'initial. Cette transformation se fait en rendant l'image moins détaillée et cela peut donc, en partie voire totalement, corrompre ou effacer les informations cachées. L'ajout de codes correcteurs tel que le code de Hamming (7,4) [3] peut alors être une solution pour protéger davantage les données et ainsi les reconstituer si elles ont été modifiées.

Problématique :

Comment transformer puis dissimuler des données à l'aide de la stéganographie pour les transmettre en toute discrétion ? Quelles améliorations peut-on apporter pour rendre la stéganographie encore plus performante ?

Objectifs du TIPE :

- Implémenter deux algorithmes simples permettant de dissimuler dans une image un texte ou bien une autre image
- Analyser les changements visuels causés par une telle insertion de données
- Proposer un chiffrement permettant de sécuriser les données en plus de les rendre invisibles
- Etudier les résultats de l'ajout d'un code correcteur pour protéger les données notamment lors d'une compression de l'image

Références bibliographiques :

N°	Auteur(s)	Thème / Titre	Source
[1]	T.Morkel - J.H.P.Eloff - M.S.Olivier	An overview of image steganography	https://shorturl.at/MAYg9
[2]	Sarra Kouider	Insertion adaptative en stéganographie	https://theses.hal.science/tel-01020745v1
[3]	François Dubois	Code de Hamming	https://www.imo.universite-paris-saclay.fr/~francois.dubois/cours/codes-automates/codauto-cours-04-04mars2020.pdf
[4]	National Instrument Corp.	Peak Signal-to-Noise Ratio	https://www.ni.com/en/shop/data-acquisition-and-contro add-ons-for-data-acquisitio what-is-vision-development- peak-signal-to-noise-ratio- html?srsltid= AfmBOordNanP3kqeVwdtUdrQXUG
[5]	Cryptage XOR	Renaud Lifchitz	http://www.primenumbers.net/Renaud/fr/crypto/XOR.htm