14408 AYOUBA Anrezki

Analyse des invariants de dissimulation : détection de la stéganographie dans les images JPG

Depuis mes années au lycée, la stéganographie a toujours suscité ma curiosité. J'avais alors conçu un site permettant de cacher des informations dans des images ou des textes grâce à différentes méthodes de dissimulation, que j'implémentais progressivement. Avec une amie, nous nous amusions à échanger des messages cachés, mais cette pratique a rapidement soulevé un défi : comment détecter si un message dissimulait ou non une information, sans devoir tester manuellement chaque méthode ? Pour y répondre, j'ai développé un bot capable de tester toutes les méthodes disponibles dans ma base de données et de décoder en fonction de chacune.

Cependant, à mesure que le nombre de méthodes de dissimulation augmentait, ce bot devenait de plus en plus inefficace, la complexité de ses tests ralentissant considérablement le processus. Ce constat a fait émerger une question plus fondamentale, qui constitue aujourd'hui la problématique de mon TIPE : existe-t-il un invariant spécifique aux données dissimulées dans les fichiers image JPG, permettant ainsi de détecter la présence d'informations cachées, indépendamment de la méthode de dissimulation utilisée ?

Positionnement thématique (phase 2)

INFORMATIQUE (Informatique pratique), INFORMATIQUE (Informatique théorique), INFORMATIQUE (Apprentissage Automatique et Statistiques), MATHÉMATIQUES (Théorie de l'Information), MATHÉMATIQUES (Analyse et Traitement des Signaux), MATHÉMATIQUES (Algèbre Linéaire et Tenseur)

Mots-clés (phase 2)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Stéganographie	Steganography
Stéganalyse	Steganalysis
Invariant de dissimulation	Hiding invariant
Image JPG	JPG image
Méthodes de dissimulation	Embedding methods
Apprentissage automatique	Machine learning

Bibliographie commentée

La stéganographie est une technique ancienne et moderne permettant de dissimuler des informations au sein de supports numériques. Elle repose sur des concepts fondamentaux de la théorie de l'information et s'appuie sur des méthodes variées et sophistiquées. Le sujet de mon étude se concentre sur les invariants potentiels permettant d'identifier des informations dissimulées dans des images JPG, indépendamment de la méthode de dissimulation utilisée. Cette recherche implique une compréhension approfondie des principes théoriques, des algorithmes, ainsi que des attaques possibles contre ces méthodes.

La théorie de l'information, développée par Claude Shannon, offre une base essentielle pour comprendre comment l'information peut être cachée dans un signal tout en minimisant la

perturbation. L'article fondateur [**1**] de Claude Shannon expose les bases de la quantification de l'information, qui s'applique également à la stéganographie. Cette référence est incontournable pour établir les concepts fondamentaux liés à la capacité et à la sécurité des canaux de communication. De manière plus spécifique, Christian Cachin [**2**] propose une modélisation mathématique pour évaluer la sécurité des systèmes de stéganographie, en introduisant des notions comme l'entropie conditionnelle et la divergence de Kullback-Leibler. Ces mesures permettent de quantifier l'efficacité des algorithmes et de déterminer si une dissimulation est détectable.

Christian Cachin [**3**] fournit une description exhaustive des techniques modernes de stéganographie, en particulier celles qui opèrent sur des images numériques. Les principes des méthodes par substitution des bits de moindre poids (LSB) sont détaillés, ainsi que leurs limites en termes de robustesse face à la stéganalyse. Fridrich introduit également des stratégies visant à réduire les artefacts détectables dans les données modifiées, une problématique directement liée à l'étude des invariants. Dans un contexte plus large, Wayner Peter [**4**] explore les liens entre la stéganographie et la cryptographie. Dans son livre, il met en lumière l'utilisation conjointe de ces deux domaines pour sécuriser l'information, tout en présentant des algorithmes pratiques comme ceux basés sur la manipulation des pixels ou des fréquences. Ces informations sont essentielles pour comprendre les techniques existantes et les défis qu'elles posent à la détection.

La détection des informations dissimulées dans les images JPG est un domaine de recherche intensif. Le développement d'outils d'analyse comme StegExpose [**5**] permet d'automatiser cette détection en analysant les anomalies statistiques générées par la dissimulation. Ces outils peuvent constituer un point de départ pour identifier des invariants spécifiques aux fichiers JPG.

Des approches telles que celle de l'apprentissage supervisé [**7**][**8**] peuvent aussi être utilisées pour l'analyse des invariants, mais aussi pour l'identification d'invariants pertinents, notamment grâce à des modèles comme les CNN (Convolutional Neural Networks). Ces techniques permettent de détecter des motifs complexes et d'affiner les méthodes de stéganalyse, ouvrant la voie à des outils de plus en plus performants pour l'identification des informations dissimulées.

Problématique retenue

Est-il possible d'identifier un invariant de dissimulation dans des fichiers JPG, c'est-à-dire une caractéristique commune à toutes les données issues d'un processus de stéganographie, indépendamment de l'algorithme utilisé ou du type de données, permettant ainsi de détecter la présence d'information cachée dans ces fichiers ?

Objectifs du TIPE du condidat

1. Définir formellement la notion d'information dans le cadre de la dissimulation dans les images JPG.
2. Sélectionner un ensemble représentatif de méthodes de stéganographie appliquées aux fichiers JPG.
3. Étudier en détail le fonctionnement des méthodes de dissimulation sélectionnées.
4. Analyser les données issues de la dissimulation dans des fichiers JPG à l'aide de techniques statistiques.
5. Créer une base de données combinant des images JPG "clean" et des images "stego".

6. Implémenter un modèle d'apprentissage supervisé, ici le CNN (convolutional neural network) pour identifier des caractéristiques communes aux images dissimulées.
7. Développer un algorithme de reconnaissance (déterministe et non déterministe) pour détecter des informations dissimulées dans les images.
8. Évaluer la performance du modèle de d'apprentissage supervisé dans la détection de la stéganographie.
9. Comparer l'efficacité de l'algorithme développé avec d'autres techniques existantes.
10. Élargir le model d'aprentissage de de nouvelles methodes de dissimulations et a d'autres types de couvertures.

Abstract

Steganography, the art of hiding information within digital media, plays a crucial role in secure communication. This study focuses on identifying invariants specific to JPG images that persist across various steganographic techniques, enabling robust detection of hidden data. By leveraging theoretical principles from information theory and practical tools for steganalysis, we aim to characterize unique statistical signatures left by different methods of data embedding. This approach seeks to bridge the gap between the diversity of concealment methods and their detection, contributing to the development of more effective analytical frameworks for digital security.

Référence bibliographiques (phase 2)

[**1**] Shannon, Claude. A Mathematical Theory of Communication, Bell System Technical Journal, 1948.

[**2**] Cachin, Christian. An Information-Theoretic Model for Steganography, Information Hiding Workshop, 1998.

[**3**] Fridrich, Jessica. Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2009.

[**4**] Wayner, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking, Morgan Kaufmann, 2009.

[**5**] StegExpose, outil de stéganalyse open source, disponible sur GitHub.

[**6**] OpenStego, framework de stéganographie open source, disponible sur opestego.sourceforge.net.

[**7**] Vincent, Barra et Antoine Cornuéjols Laurent Miclet. Apprentissage artificiel

[**8**] Rémi Cogranne, Patrick Bas, Marc Chaumont. Stéganalyse : détection d'information cachée dans des contenus multimédias.

DOT

[**1**] *Février 2024 : définition d'une problématique et début de la recherche documentaire*

[**2**] *Février 2024 : choix de trois méthodes de dissimulation (LSB, DCT, Masquage psychoacoustique dans l'audio)*

[**3**] *Mars 2024 : implémentation des méthodes de dissimulation choisies*

[**4**] *Mars 2024 : Mise en place d'une base de données d'étude*

[5] *Mars 2024 : implémentation en Python d'une méthode de détection de la méthode LSB en utilisant le test du khi carré et l'apprentissage supervisé*

[6] *Mars 2024 : implémentation en Python des algorithmes pour le traitement et la récolte des données*

[7] *Avril 2024 / septembre 2024 : implémentation d'un algorithme de deep learning pour l'analyse des données*

[8] *Septembre 2024 / décembre 2024 : Étude des résultats pour la mise en évidence d'un invariant de dissimulation*

[9] *Restriction à l'étude des images au format JPG, pour plus de précisions et faciliter la prise en main du problème*

[10] *Janvier 2025 : définition de la problématique et protocole expérimental*

[11] *Janvier 2025 : sélection des méthodes de dissimulation pour les images JPG*

[12] *Janvier 2025 : collecte d'images et constitution des catégories (stégo et clean)*

[13] *Janvier 2025 : analyse des images stégo pour identifier les caractéristiques communes*

[14] *Janvier 2025 : implémentation des algorithmes pour récolter les caractéristiques*

[15] *Janvier 2025 : clustering des données et identification des invariants et rencontre*

[16] *Janvier 2025 : Rencontre avec un doctorant du LAAS-CNRS, Abdel Kader CHABI SIKA BONI. Il travaille sur l'application des techniques d'intelligence artificielle aux systèmes IoT autonomes*

[17] *Février 2025 : amélioration du modèle avec de nouvelles données et de nouvelles caractéristiques issues du modèle CNN*

[18] *Mars 2025 : développement de l'algorithme de détection et tests sur les images*

[19] *Avril 2025 : évaluation et comparaisons des résultats*

[20] *Juin 2025 : conclusion et perspectives*