Université de Montpellier
Master 2 - Imagine
TP Image, Sécurité et Deep Learning (HAI918I)

Enseignante : Pauline Puteaux
pauline.puteaux@lirmm.fr
A rendre le 24 octobre 2021 (23h59)

TP Sécurité Multimédia

Le but de ce TP est de manipuler différents algorithmes et outils utilisés en sécurité multimédia. Vous utiliserez des images en niveaux de gris (format `.pgm`*). Vous noterez que l'ensemble des méthodes vues dans le TP peuvent aisément être étendues aux images couleur (format* `.ppm`*).*

Vous devrez rendre le compte-rendu de ce TP et vos sources. Le compte-rendu doit être constitué de vos réponses aux questions et éventuellement de remarques sur vos choix d'implémentation. Le code doit être commenté.

Ci-dessous, vous trouverez les conventions de nommage (à respecter pour être évalué...) :
Sujet du mail : `[M2-IMAGINE] TP Sécurité multimédia - Nom Prénom`
Compte-rendu : `CR_TP_SecuriteMultimedia_NomPrenom`
Archive des sources : `Code_TP_SecuriteMultimedia_NomPrenom`

(1) Chiffrement d'images

(a) Implémentation de la méthode de chiffrement

On rappelle le fonctionnement du chiffrement XOR :

Définition Le chiffrement XOR est une méthode de chiffrement symétrique. Soit une image de taille $m \times n$ pixels $p(i)$ avec $0 \leq i < m \times n$. L'image chiffrée associée est obtenue en effectuant un ou-exclusif entre les pixels de l'image en clair et une séquence binaire générée pseudo-alétoirement.

i) Implémentez une fonction qui prend en entrée un nombre entier considéré comme clé de chiffrement pour initialiser un générateur pseudo-aléatoire. Ce générateur sera utilisé pour obtenir une séquence pseudo-aléatoire de la même taille que l'image.

ii) A l'aide de la fonction précédente, implémentez la fonction de chiffrement. Chiffrez l'image de votre choix et présentez le résultat obtenu dans votre rapport. Vous indiquerez aussi la clé de chiffrement utilisée.

iii) L'opération XOR étant symétrique, la fonction de déchiffrement est identique. Vérifiez que vous réussissez à reconstruire l'image originale en ré-appliquant votre fonction.

iv) Utilisez une nouvelle clé de chiffrement pour chiffrer l'image choisie en question ii). Les images chiffrées obtenues sont-elles identiques ? Montrez-le à l'aide de la méthode de votre choix.

(b) Analyse statistique

i) Calculez le PSNR entre l'image originale et l'image chiffrée.

ii) Calculez l'entropie de l'image en clair, puis celle de l'image chiffrée.

iii) Tracez l'histogramme de l'image originale, puis celui de l'image chiffrée.

iv) Discutez le niveau de sécurité de la méthode de chiffrement implémentée à l'aide des résultats obtenus aux questions précédentes.

(2) Insertion de données cachées

(a) Plans binaires

On rappelle la définition d'un plan binaire :

Définition Un plan binaire d'un signal numérique discret est un ensemble de bits correspondant à une position binaire donnée dans chacun des nombres binaires représentant le signal. En particulier, pour une image en niveaux de gris au format `.pgm`, on dénombre 8 plans binaires (du plus significatif – appelé MSB (*Most Significant Bit*), au moins significatif – appelé LSB (*Least Significant Bit*)).

i) Implémentez une fonction permettant, à partir d'une image, de récupérer le plan binaire à la position k, avec $0 \leq k < 8$. Vous devrez utiliser les opérateurs binaires.

ii) Dans votre rapport, illustrez les plans binaires MSB et LSB d'une image en clair et d'une image chiffrée. Discutez les résultats obtenus : en particulier, quelle(s) remarque(s) pouvez-vous faire sur la corrélation entre les bits voisins ?

(b) Implémentation de la méthode d'insertion

i) Générez une séquence aléatoire de bits de la même taille que l'image de votre choix. Cette séquence sera considérée comme le message à insérer dans l'image.

Remarque Dans un scénario applicatif, tout message inséré est d'abord chiffré avant son insertion dans une image et a donc les mêmes propriétés statistiques qu'une séquence aléatoire de bits.

ii) Implémentez une fonction permettant d'insérer un message binaire dans une image par substitution du bit à la position k, avec $0 \leq k < 8$, de chaque pixel. Vous devrez utiliser les opérateurs binaires.

iii) Dans votre rapport, illustrez l'image obtenue après substitution des MSB de l'image en clair de votre choix. Calculez le PSNR entre l'image originale et l'image marquée. Quelle remarque pouvez-vous faire quant à la qualité de l'image obtenue ? Pourquoi ?

iv) Dans votre rapport, illustrez l'image obtenue après substitution des LSB de l'image en clair de votre choix. Calculez le PSNR entre l'image originale et l'image marquée. Quelle remarque pouvez-vous faire quant à la qualité de l'image obtenue ? Pourquoi ?

(c) Un peu de stéganalyse...

i) Tracez l'histogramme de l'image marquée, après substitution des LSB.

ii) Comparez l'histogramme obtenu avec celui de l'image originale. Expliquez les différences obtenues.

iii) Si l'image marquée est visuellement similaire à l'image originale, un attaquant peut-il y détecter la présence d'un message caché ?

(3) Insertion de données cachées... dans des images chiffrées

(a) Implémentation naïve

i) Encodage : Réalisez le chiffrement XOR d'une image en clair. Adaptez la méthode d'insertion implémentée précédemment pour insérer un message secret dans les MSB de tous les pixels sauf ceux de la première ligne et ceux de la première colonne. Présentez l'image chiffrée marquée obtenue dans votre rapport.

ii) Décodage : Déchiffrez l'image chiffrée marquée. Présentez l'image obtenue dans votre rapport. Vous devrez constater que seuls les MSB de l'image déchiffrée sont potentiellement mal reconstruits.

(b) Prédiction des valeurs des MSB

i) Implémentez une fonction permettant de calculer le prédicteur d'un pixel à un indice donné. Ce prédicteur devra être calculé à partir des pixels voisins précédents.

Remarque Pour prédire $p(i)$, il est conseillé, dans le cadre de ce TP, de considérer la moyenne entre le pixel de gauche, le pixel du haut et le pixel en diagonale en haut à gauche :

$$pred(i) = \frac{p(i-1) + p(i - nb\_colonnes) + p(i - 1 - nb\_colonnes)}{3}.$$

ii) Implémentez une fonction permettant de calculer la valeur d'un pixel dont le MSB aurait été inversé.

Exemple Si $p(i) = 200$, $inv(i) = 72$, et si $p(i) = 50$, $inv(i) = 178$.

iii) Dans une image naturelle en clair, il existe une forte corrélation entre les pixels voisins. A l'aide des deux questions précédentes, reconstruire l'image originale en prédisant la valeur du MSB de chaque pixel. Présentez l'image obtenue dans votre rapport. Calculez son PSNR avec l'image originale. Vous remarquerez des artefacts sur l'image reconstruite. Comment expliquez-vous cela ?

Remarque 1 Lors de l'insertion de données cachées, les pixels de la première ligne et de la première colonne n'ont pas été marqués par le message.

Remarque 2 $p(i)$ et $inv(i)$ sont les deux valeurs possibles des pixels de l'image en clair. Il convient de calculer leur distance avec la valeur du prédicteur $pred(i)$.

iv) Pour éviter le problème survenu à la question précédente, une solution est de pré-traiter l'image originale avant son chiffrement. Implémentez la fonction de pré-traitement à l'aide du pseudo-code ci-dessous. En quoi consiste ce pré-traitement ?

Algorithme 1 : Pré-traitement de l'image originale.

```
Entrées : Image originale I de m × n pixels p(i)
Sorties : Image pré-traitée I' de m × n pixels p'(i)
pour 0 ≤ i < m × n faire
    si |pred(i) − p(i)| ≥ |pred(i) − inv(i)| alors
        si p(i) < 128 alors
            p'(i) = pred(i) − 63;
        sinon
            p'(i) = pred(i) + 63;
        fin
    sinon
        p'(i) = p(i);
    fin
fin
```

v) Réalisez le pré-traitement de l'image originale, le chiffrement de l'image pré-traitée, l'insertion de données cachées, puis la reconstruction par prédiction. Présentez l'image obtenue dans votre rapport. Calculez son PSNR avec l'image originale. Vous remarquerez qu'il n'y a plus d'artefacts et que l'image reconstruite est fortement similaire à l'image originale.

(4) Bonus

— Implémentez la fonction d'extraction d'un message secret inséré dans une image (en clair ou chiffrée) par substitution des LSB ou des MSB. Vérifiez que le message extrait est bien identique au message inséré.

— Adaptez votre code pour prendre en entrée un fichier texte, le convertir en binaire, le chiffrer, et réaliser son insertion dans une image. De plus, lors de l'extraction du message (au format binaire), implémentez la fonction de conversion inverse pour récupérer les données textuelles.