Détection et suivi de personnes dans des séquences d'images par CNN pour la protection de la vie privée.

CR #7 - Chiffrement sélectif et autres perspectives

CANHOTO Mickaël,
FONTAINE Emmanuel
Master 2 Imagine

I - Introduction

Cette semaine, nous nous sommes concentrés sur le chiffrement sélectif, ainsi que d'autres perspectives afin de mieux traiter le déchiffrement AES. En effet, nous allons voir les différents problèmes liés au déchiffrement ainsi que les solutions que nous avons trouvé et choisi.

II - Chiffrement sélectif

Le chiffrement sélectif est un chiffrement dans lequel on affecte uniquement certains bits de chaque octet. Cela permet d'anonymiser les personnes tout en gardant la silhouette et les informations autour. Contrairement au chiffrement AES classique qui fait bruité l'entièreté de la boîte englobante.

Dans notre cas, nous allons utiliser le même chiffrement CBC que l'AES en y affectant les 6 premiers bits de poids faible. Le nombre de bits à choisir est un compromis important entre sécurité et quantité d'informations.

Chiffrement sélectif des 6 LSBs

Dans des vidéos ou les passants ne sont pas proche de la caméra, l'anonymisation est très efficace. Une amélioration possible serait la possibilité de choisir le nombre de bits à chiffrer.

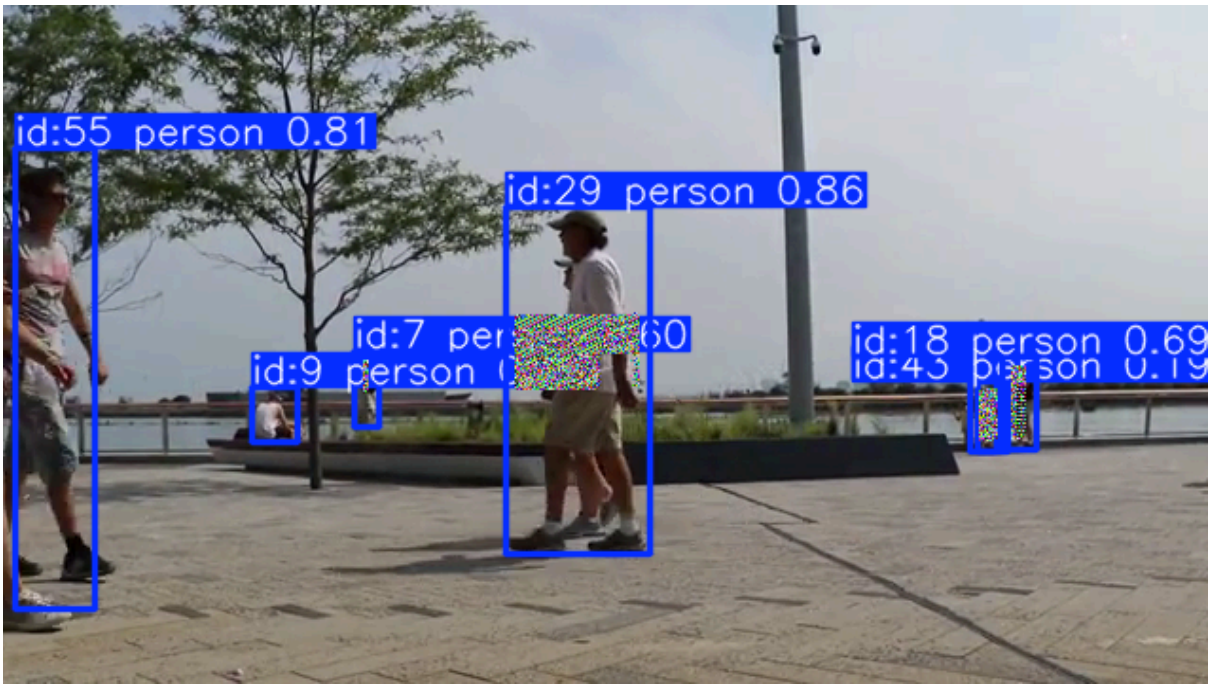
III - Problèmes liés au déchiffrement AES et solutions

Le premier souci que nous avons rencontré en lien avec le déchiffrement AES était en rapport avec le format vidéo. En effet, lorsque nous enregistrions la vidéo résultante, celle-ci était compressée, rendant le déchiffrement impossible. Afin de résoudre ce problème, il a fallu enregistrer la vidéo dans un format non compressé tel que AVI, par exemple.

D'autres problèmes sont apparus après cela, tel que le chevauchement des différentes régions qui ont été chiffrées. Par exemple, si une personne passe devant une autre personne, nous avons un chevauchement de ces régions, ce qui rend le déchiffrement de ces zones inefficace. L'astuce pour remédier à ce problème consiste à repérer les chevauchements et à procéder au déchiffrement dans l'ordre inverse du chiffrement, ce qui permet de déchiffrer correctement la zone ciblée.

Exemple de chevauchement

Enfin le dernier problème que nous avons rencontré, et que lors du traitement (détection et anonymisation des personnes), nous affichons les boîtes encombrantes ainsi que l'ID de la personne, mais il se peut que le label de l'ID, chevauche la zone chiffrée.



Exemple de chevauchement avec le label

IV - Solutions choisies

Nous avons trouvé deux solutions possibles pour le déchiffrement. Voici les avantages et inconvénients de chaque solutions :

Méthode 1 : stocker chaque coordonnées des pixels chiffrés.

- Avantages : Déchiffrement propre ne posant aucun problème de chevauchement
- Désavantages : Fichier JSON très lourd et peu lisible.

Méthode 2 : enlever les boîtes encombrantes et les labels.

- Avantages : Fichier JSON léger et lisible. Temps de traitement plus faible
- Désavantages : Perte d'informations dont les ID qui sont nécessaires pour différencier les personnes.

La solution que nous avons choisie est celle de la méthode 1, car malgré la création d'un fichier JSON très lourd, nous pouvons déchiffrer et ce même lorsque nous avons plusieurs chevauchements de tout type.

V - Conclusion

Pour conclure, durant cette semaine, nous avons pu peaufiner l'anonymisation avec un chiffrage sélectif, et nous avons pu voir différents problèmes liés au déchiffrement AES, que ce soit sur le format de vidéo, ou les différents types de chevauchements.