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

CR #6 - Chiffrement et déchiffrement AES

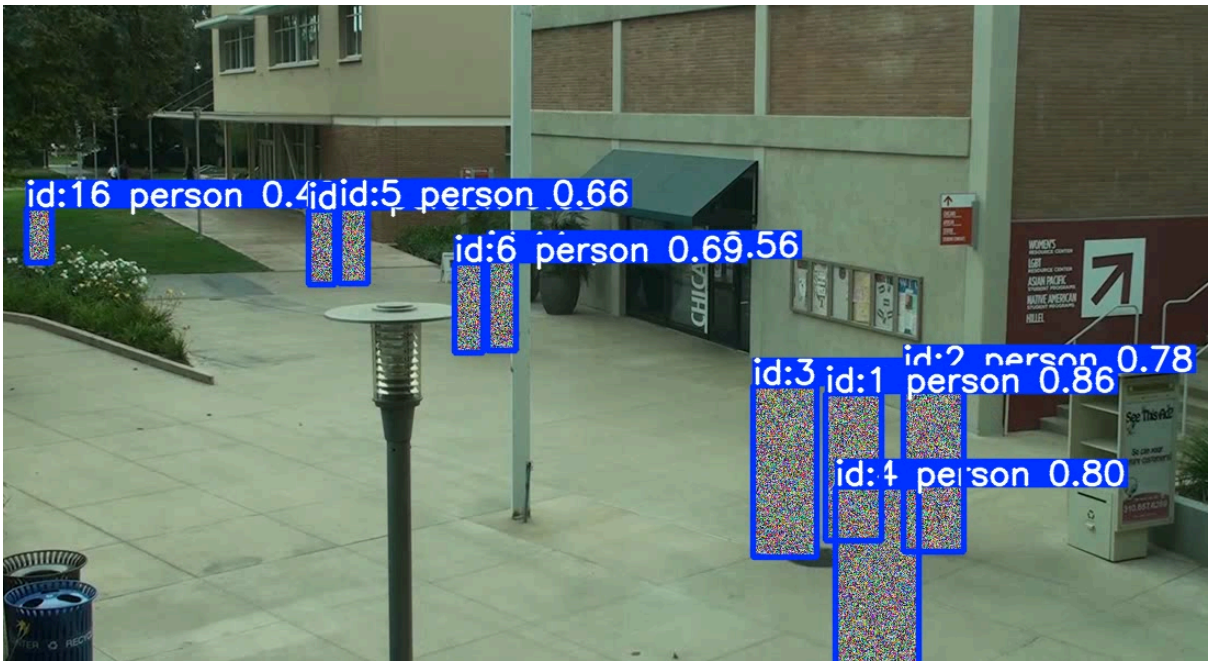
CANHOTO Mickaël,
FONTAINE Emmanuel
Master 2 Imagine

I - Introduction

Cette semaine est consacrée au chiffrement AES. Nous avons ajouté la possibilité de faire un chiffrement et déchiffrement dans le programme. Lorsque le programme anonymise, nous créons une clef unique sur chaque personne (ID). Ensuite, on chiffre la boîte englobante de la personne avec cette clef et nous y stockons les informations dans un JSON.
Pour le déchiffrement, on lit le JSON donné avec les clefs et les positions des boîtes, puis nous déchiffrons.

II - Chiffrement

Le chiffrement AES est un algorithme de chiffrement symétrique utilisé pour sécuriser les données. Il fonctionne avec une clé secrète de taille fixe et chiffre les données par blocs de 128 bits. Pour chiffrer, nous générons une clef aléatoire de 128 bits par ID (personne détectée dans la vidéo)et on convertit les données en bloc de 16 octets. Nous utilisons le CBC avec le vecteur d'initialisation IV ou chaque bloc est XORé.



Chiffrement AES

On enregistre ensuite les informations dans un JSON afin de pouvoir déchiffrer dans une autre partie.

III - Frame data

Le frame data est le fichier JSON obtenu en sortie du programme. Ce fichier va permettre de déchiffrer la vidéo. Il est composé de :

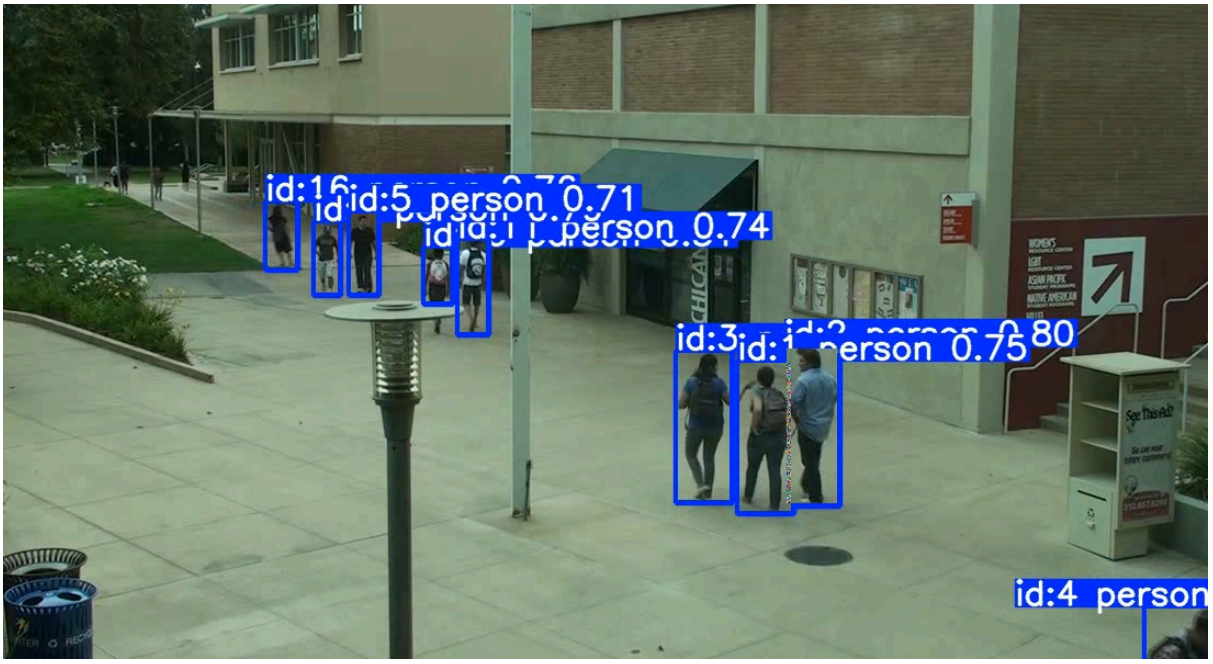
- le numéro de la frame
- les boîtes englobante avec :
    - l'id
    - les coordonnées
    - la clef
    - l'IV

Ces informations vont nous permettre derrière de déchiffrer la vidéo.

IV - Déchiffrement

Pour le déchiffrement, nous avons ajouté une fenêtre dédiée. Dans cette fenêtre, nous demandons à l'utilisateur la vidéo et le frame data.
Lors du lancement de ce programme, on va traiter le JSON pour récupérer les données de chaque frame. Ensuite, on récupère pour chaque ID, les coordonnées des boîtes encombrantes, sa clef et du IV. Ensuite, on lance l'algorithme de déchiffrement. L'algorithme fonctionne de la même façon que le chiffrement.

Déchiffrement de l'ID 1, 2 et 3.



Déchiffrement de l'ensemble des ID.

V - Conclusion

Pour conclure le chiffrement AES permet d’anonymiser complètement la personne tout en ayant la possibilité de restaurer la vidéo d’origine. Cela peut être utile dans le cas où on aimerait suivre une personne spécifique.
La semaine prochaine, nous aimerions utiliser le chiffrement par sélection afin de pouvoir anonymiser les personnes tout en pouvant voir leur silhouette. Ce chiffrement affecte uniquement les bits de poids faibles.