Projet Image M2 : Evaluation de la sécurité visuelle d'images obscures par CNN
HAI918I : Image, sécurité et deep learning

Université de Montpellier - FDS
2ième année Master IMAGINE
Oren AMSALHEM - Thomas CARO

13 Octobre 2024

1 Introduction

L'obscuration d'image est un ensemble de techniques permettant de de rendre une image moins identifiable, que ce soit dans son intégralité ou une portion spécifique. On peut différencier plusieurs types de techniques :

- Le floutage : Application d'un filtre permettant de flouter toute ou une partie de l'image.
- La pixelisation : Transformation d'une partie de l'image en une grille de gros pixels.
- Le masquage : Ajout de forme opaque comme un rectangle dans la zone à cacher.
- Le cryptage : Utilisation d'algorithme de cryptage sur une partie ou toute l'image nécessitant une clé pour décrypter.
- La distorsion : Utilisation de transformations géométrique telle que l'étirement.

L'obscuration est utilisée pour atteindre divers buts et dans différents contextes :

- Entrainement de CNN pour détection
- Anonymisation des données
- Applications artistiques
- Confidentialité
- Sécurité

Le but de ce projet est de tester différentes méthodes d'obscurations d'images et de tester leur robustesse face à un CNN, nous pourrons jouer sur les paramètres de chaque méthodes d'obscuration et tester la fiabilité des différents résultats.

Nous commencerons par effectuer un état de l'art sur les différentes méthodes d'obscuration, puis sur les différentes méthodes d'évaluation de sécurité visuelle d'images. Nous implémenterons différentes méthodes d'obscuration que nous testerons et évalueront. Ensuite nous pourrons tester à l'aide d'une méthode basée sur un réseau de neurones convolutifs la robustesse de ces méthodes d'obscurations.

2 Etat de l'art sur l'obscuration

2.1 Obscuration par flouttage

Les méthodes de flouttage classiques utilisent pour la majorité un filtre. Par exemple la technique du flou moyen utilise un noyau de convolution moyenneur sur une partie ou l'intégralité de l'image afin d'adoucir les bords et rendre l'information de l'image moins visible.

Le flou Gaussien utilise lui aussi un filtre qui est déterminé par une fonction gaussienne, qui permet à l'aide des poids du filtre de faire une moyenne pondérée des pixels voisins d'un pixel.

Le flou de mouvement lui cherche à faire l'illusion d'un mouvement sur l'image, pour cela il faut choisir une direction et une amplitude et créer un filtre à partir de ça. Si l'on décide de faire un flou horizontal on pourrait par exemple prendre des valeurs de filtre sur une seul ligne du filtre. Voici un exemple :

$$\text{Kernel} = \begin{bmatrix} 0.5 & 0.5 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Ce filtre met l'accent sur le mouvement de gauche à droite typiquement. Voici un exemple de flouttage :

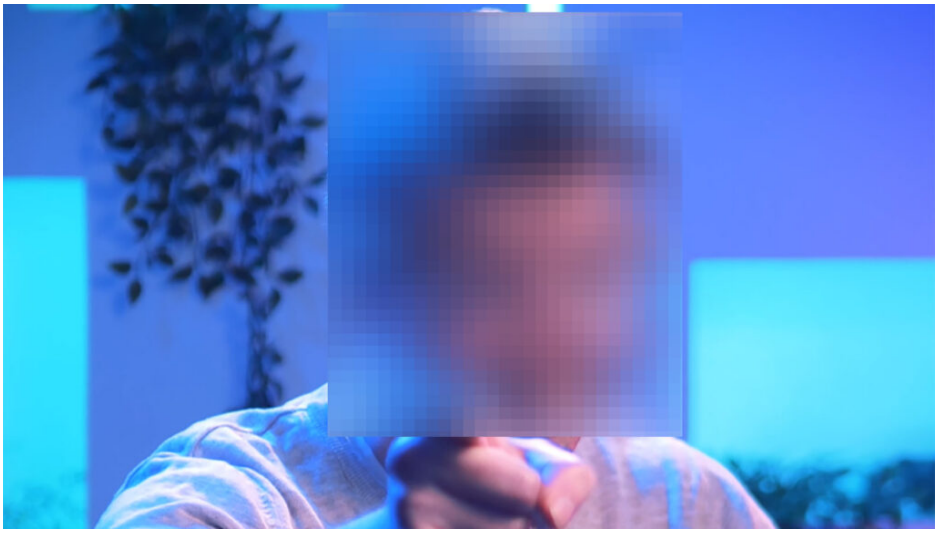

FIGURE 1 – Exemple de flouttage

2.2 Obscuration par pixelisation

Les méthodes de pixélisation travaillent par bloc sur une image.

Une première méthode classique est de pixéliser une image par bloc fixe, en choisissant donc une taille de bloc fixe et en mettant par exemple pour chaque bloc une valeur de couleur moyenne du bloc.

Une autre méthode classique serait de faire une pixelisation adaptative selon les détails de l'image. Les endroits détaillés seraient plus pixélisé que les autres. Le problème de cette méthode par rapport à la précédente est qu'elle nécessite des calculs en amont pour quantifier la quantité de détail dans l'image. Cette quantification de détail peut se faire par analyse des hautes fréquences à l'aide de transformée de Fourier.

Voici un exemple :

FIGURE 2 – Exemple de pixelisation

2.3 Obscuration par masquage

L'obscuration par masquage est de manière générale une méthode utilisant des formes géométriques, fixes ou dynamiques, soit de couleur unie ou semi-transparente que l'on met dans les zones à cacher. Voici un exemple fait

maison :

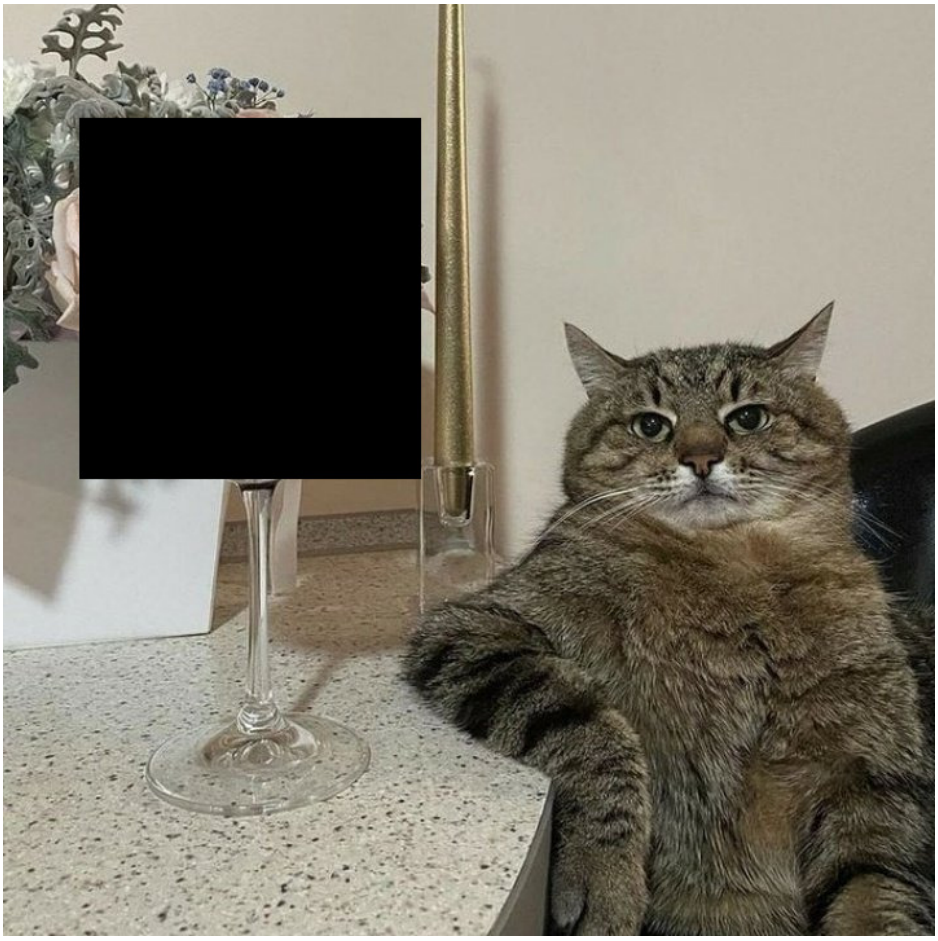

FIGURE 3 – Exemple de masquage

2.4 Obscuration par cryptage

L'obscuration par cryptage profite du fait que la cryptographie est un domaine déjà bien étudié. Ainsi il y a différents types de méthodes classiques, qu'elles soient des méthodes de cryptage symétrique, comme avec AES (Advanced Encryption Standard) et DES (Data Encryption Standard), ou asymétrique, avec RSA(Rivest–Shamir–Adleman). Des méthodes de cryptage plus simples peuvent être utilisée telle que l'utilisation de permutation sur l'ensemble de l'image afin de déplacer tous les pixels de l'image, ou de la zone souhaitée, une ou plusieurs fois. Il peut aussi y avoir des méthodes par bloc plus simple que DES ou AES. L'un des inconvénients de ces méthodes est la complexité potentielle de l'algorithme de cryptage et de décryptage.

2.5 Obscuration par distorsion

Les méthodes de distorsions utilisent des transformations géométriques afin de dissimuler l'information de l'image. Les transformations géométriques classiques étant la rotation, la translation, le zoom et l'étirement. Une combinaison de ces méthodes constituerait déjà une base d'obscuration. Des méthodes plus sophistiquées utiliserait une carte de déformation, une carte qui assignerait à chaque pixel un certain déplacement, ce déplacement pouvant être calculé à partir de fonction mathématiques comme par exemple la fonction sinusoïdale.

Il y a aussi dess méthodes à base de bruits qui rajouent donc une variation nouvelle dans l'image pouvant potentiellement dissimuler certains aspects de l'image. Un bruit classique est le bruit poivre et sel. Voici un exemple :

FIGURE 4 – Exemple de distorsion par bruitage

3 Utilisation d'un CNN

Les CNN sont une classe de réseaux de neurones artificiels particulièrement efficaces pour les tâches de traitement d'images. Ils sont souvent utilisés pour la reconnaissance d'objets, la classification d'images, et la détection d'objets. Les CNN peuvent être utilisés pour appliquer des techniques d'obscuration adaptatives, où le niveau de flou ou de pixellisation est ajusté en fonction du contexte de l'image ou de la sensibilité de l'information. Ils peuvent aussi nous permettre d'automatiser le processus d'obscuration, ce qui est beaucoup plus efficace que les méthodes manuelles. Une fois entraîné, un CNN peut traiter un grand nombre d'images en temps réel, rendant le processus d'obscuration rapide et scalable.

3.1 Surveillance Vidéo

Les CNN peuvent être utilisés pour détecter et obscurcir les visages des personnes dans les vidéos de surveillance, protégeant ainsi leur vie privée.

3.2 Images Médicales

Dans les bases de données d'images médicales, les CNN peuvent être utilisés pour détecter et obscurcir les informations sensibles tout en permettant l'analyse des images pour des fins médicales.

3.3 Reconnaissance d'immatriculation

Les CNN peuvent être utilisés pour détecter et obscurcir les plaques d'immatriculation dans les images de trafic, protégeant ainsi les informations personnelles des conducteurs.