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

27 Octobre 2024

1 Introduction

Cette semaine nous allons nous intéresser aux différentes méthodes d'évaluation de sécurité visuelle d'image, et implémenter notre première méthode d'obscuration d'image.

2 Etat de l'art sur l'évaluation de la sécurité visuelle des images

2.1 Evaluation subjective par sondage

Une première méthode assez naturelle serait de prendre un groupe de personnes et de demander si le contenu de l'image obscurcie est reconnaissable. Il faudrait prendre bien évidemment un groupe connaissant le sujet de la partie obscurée et assez grand afin d'avoir une statistique de reconnaissance.

2.2 Evaluation objective

On pourrait de manière purement objective utiliser une mesure telle que le SSIM(Structural Similarity) ou le PSNR(Peak Signal-to-Noise) entre l'image de départ et l'image obscurcie afin d'avoir une mesure tangible de la différence entre les 2 images. D'autres mesures telle que l'entropie pour faire la même chose.

2.3 Evaluation par IA

Nous pouvons aussi utiliser différents modèles d'IA afin d'évaluer la sécurité visuelle d'image.

En premier lieu on pourrait utiliser des modèles de détection d'objet tels que YOLO, utiliser une base de données d'image avec l'objet spécifique à identifier, entrainer le modèle puis en obscurant les mêmes images ou des images du même type, voir si le modèle arrive à reconnaitre les objets spécifiques. Une mesure de l'accuracy et F1-précision serait alors pertinente pour évaluer la sécurité visuelle des images.

On pourrait aussi utiliser des GANs(Generative Adversarial Networks) pour générér des images obscures réalistes avec par exemple du floutage ou de la pixelisation avec le générateur, puis à l'aide du discriminateur on évalue la sacurité visuelle de l'image selon s'il arrive à distinguer le synthétique obscurci du réel non obscurci. On peut aussi à l'aide des images synthétiques faire la méthode par sondage avec des groupes de personnes, permettant d'évaluer la qualité de génération de la partie générateur du GAN.

2.4 Evaluation par attaque

Nous pouvons aussi évaluer la robustesse de l'obscuration en regardant si par une attaque on peut récupérer les parties sensibles de l'image qui ont été obscurcies.

En première possibilité il y aurait l'analyse de Fourier qui permettrait d'analyser les hautes fréquences de l'images pour révéler des détails sur l'image. A partir de ça essayer de reconstruire l'image originale. Selon le succès de cette reconstruction une métrique telle que le pourcentage de réussite de la reconstruction peut etre utilisée.

Nous pourrions aussi utiliser des interpolations sur la zone obscurcie, en utilisant donc l'information des pixels environnants.

Ensuite ce n'est pas une attaque à proprement parler mais dans le cas ou l'image obscurcie risque d'etre manipulée il faudrait qu'elle soit robuste. Que ce soit par compression ou redimensionnement par exemple. Pour la compression nous pourrions utiliser différents niveaux de compression et voir si des détails de l'image supposés etre obscurcis apparaissent.

3 Implémentation du flou

3.1 Flou gaussien

Nous allons implémenter un programme permettant d'appliquer un noyau de flou gaussien de taille k avec un certain sigma sur une image.

Le noyau gaussien est défini par la formule suivante :

$$G(i,j) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{i^2+j^2}{2\sigma^2}\right) \tag{1}$$

où :

— $G(i,j)$ est la valeur du noyau à la position (i,j),

— σ est l'écart type qui détermine la largeur du noyau.

La normalisation du noyau est effectuée pour garantir que la somme des valeurs du noyau égale 1 :

$$\text{Sum} = \sum_{i=-\frac{k}{2}}^{\frac{k}{2}} \sum_{j=-\frac{k}{2}}^{\frac{k}{2}} G(i,j) \tag{2}$$

Le noyau normalisé est donné par :

$$K(i,j) = \frac{G(i,j)}{\text{Sum}} \tag{3}$$

où $K(i,j)$ est le noyau gaussien normalisé.

Voici des résultats à partir de l'image suivante :

FIGURE 1 – Image originale

Floutages gaussien avec différents paramètres :

FIGURE 2 – Noyau de taille 3*3, sigma=7

FIGURE 3 – Noyau de taille 5*5, sigma=7

FIGURE 4 – Différents floutages

Dans le cadre de l'obscuration d'éléments spécifiques il serait intéressant de pouvoir choisir la zone de floutage :

FIGURE 5 – Floutage moitié gauche avec Noyau de taille 5*5, sigma=7

On peut donc flouter dans une zone rectangulaire de l'image.

3.2 Flou de mouvement

Nous avons implémenté le flou de mouvement de manière très simple, si le flou est horizontal la ligne contenant le centre du noyau prendra des 1, si il est vertical ce sera la colonne. La taille de la ligne ou colonne dépendant de la taille de noyau souhaitée.

Voici des résultats avec la même image que précédemment :

FIGURE 6 – Noyau de taille 3*3, Horizontal

FIGURE 7 – Noyau de taille 3*3, Vertical

FIGURE 8 – Floutages directionnels

Nous avons implémenter la même option que pour le flou gaussien au niveau de la zone :

FIGURE 9 – Noyau de taille 3*3, Horizontal, Moitiée gauche

3.3 Flou par pixelisation

Nous pouvons également obscurcir une image ou une zone de l'image par pixelisation, en utilisant la taille des pixels comme paramètre, ainsi que la méthode de calcul des pixels :
AVG, qui calculera la couleur moyenne,
MIN, qui sélectionnera la couleur avec la luminance la plus faible dans chaque pixel,
MAX, qui prendra la couleur avec la luminance la plus élevée.

Figure 10 – taille des pixels 16

Figure 11 – taille des pixels 128

Figure 12 – Floutage par pixelisation, métode AVG

Figure 13 – taille des pixels 128 , méthode MAX

Figure 14 – taille des pixels 128 , méthode MIN

Figure 15 – Floutage par pixelisation (zone), métode MAX & MIN (Luminance)

On peut également accentuer la spécularité ou les ombres en isolant respectivement les composantes les plus élevées ou les plus basses de l'image, en utilisant les méthodes MAX et MIN.

Figure 16 – taille des pixels 128 , méthode MAX

Figure 17 – taille des pixels 128 , méthode MIN

Figure 18 – Floutage par pixelisation (zone), métode MAX & MIN (composantes séparées)