Projet Obscuration d'images

Chateauneuf Arthur et
Beldjilali Maxime

Contexte et État de l'art

Exemple donné de résultats d'obscuration de photo de célébrités à partir d'un visage moyen

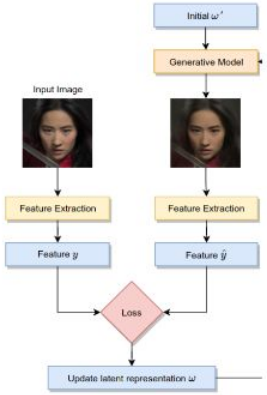


Figure 3. A general framework of latent representation sea

Notre application actuellement

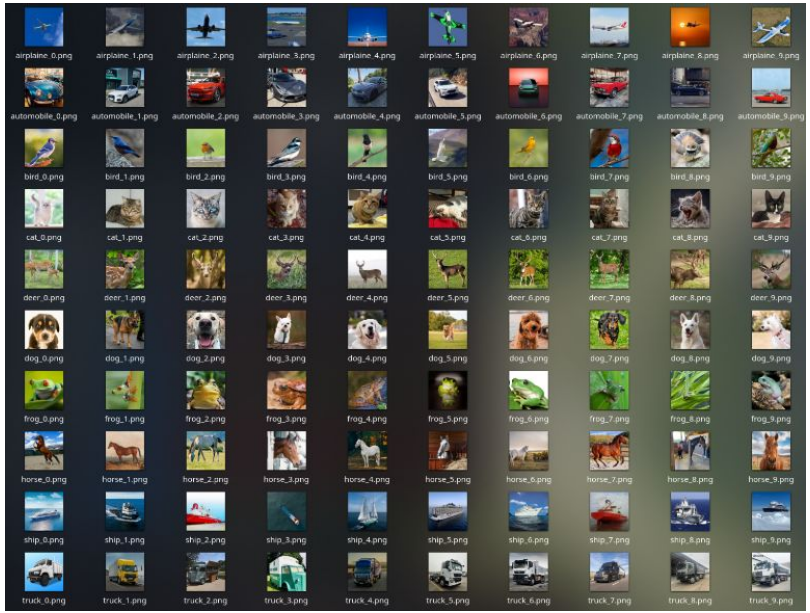
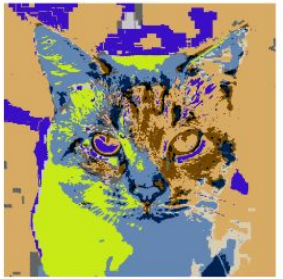
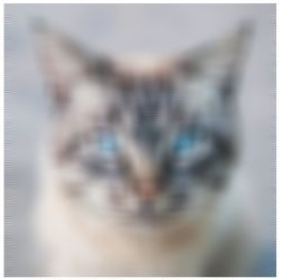


Image d'entrée

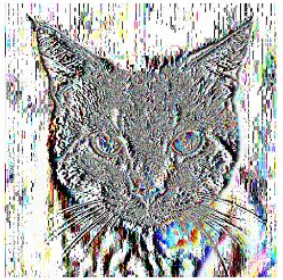
NAIVE_LSB_CUT



NAIVE_LSB_CUT_[YCrCb]



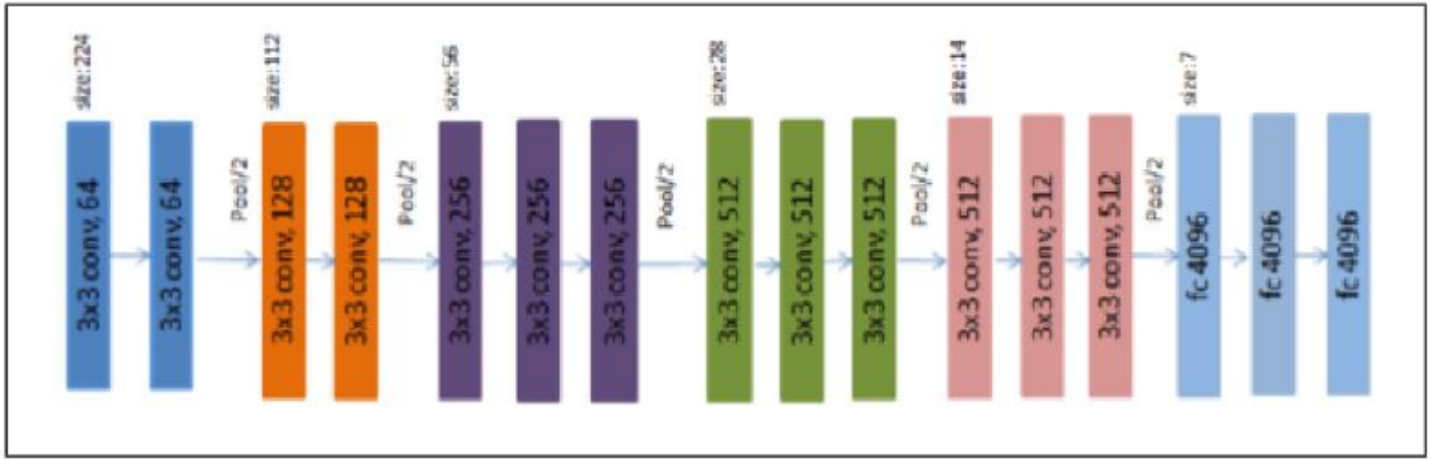
NAIVE_HEAVY_BLUR



NAIVE_WAVE_DIVIDE

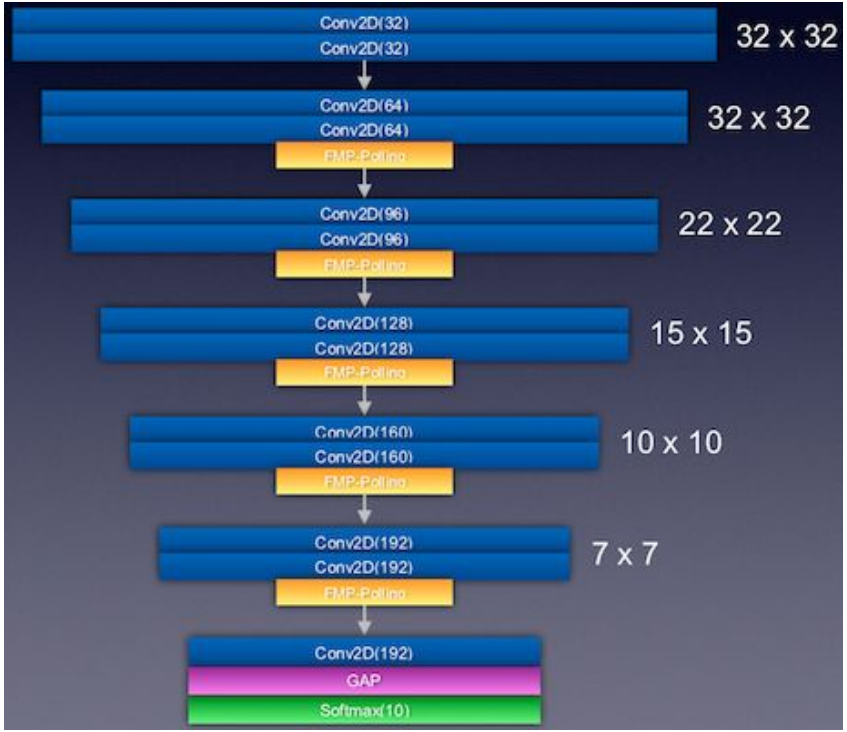
NAIVE_LINE_NOISE

Une architecture basée VGG16



Notre architecture

- Actuellement sur des images non-obscurcies
- Entraînement sur CIFAR-10
- Contraintes de tailles
- Précision actuelle 90,42%



Amélioration futurs et conclusion

Tests avancés de l'efficacité de tous les filtres

Conception de filtres non naïfs

Test de l'empoisonnement

Training sur un dataset plus haute résolution (32x32 actuellement)

Références

- Architecture “VGG like” : https://github.com/laplacetw/vgg-like-cifar10/tree/master
- Jeu de données CIFAR-10 : https://www.cs.toronto.edu/~kriz/cifar.html
- McPherson, R., Shokri, R., & Shmatikov, V. (2016). Defeating Image Obfuscation with Deep Learning. ArXiv, abs/1609.00408.
- Li, T., & Choi, M. (2021). DeepBlur: A Simple and Effective Method for Natural Image Obfuscation. ArXiv, abs/2104.02655.
- Shan, S., Ding, W., Passananti, J., Zheng, H., & Zhao, B.Y. (2023). Nightshade: Prompt-Specific Poisoning Attacks on Text-to-Image Generative Models. 2024 IEEE Symposium on Security and Privacy (SP), 807-825.