Université de Montpellier
Master 2 - IMAGINE

Safe-Eye

Évaluation de la sécurité visuelle d'images obscures par CNN

Compte rendu — 3
Projet informatique — HAI927I

Étudiants :
M. Florentin DENIS
M. Khélian LARVET

Encadrants :
M. Nicolas DIBOT
Mme. Bianca JANSEN VAN RENSBURG
M. William PUECH

Année : 2022

Déroulement du projet

Avancement actuel

Actuellement nous avons mis en place une interface utilisateur à l'aide de Tkinter permettant l'obscurcissement d'une image en temps réel avec les différents filtres que nous avons mis en place. Pour l'instant l'interface ne permet pas de modifier les paramètres des filtres, mais nous prévoyons de les ajouter incessamment sous peu.

Nous avons également tenté de créer notre propre système de classification. Son efficacité était intéressante sur de petits "datasets" comme celui du MNIST. Malheureusement, dans le cas de "datasets" un peu plus gros comme Imagenet ou CIFAR10, celui-ci n'était plus assez efficace avec une précision maximale de 80%. Nous avons donc décidé d'utiliser le classifieur "EfficientNetV2L" utilisant la base de données ImageNet.

Enfin nous avons ajouté au projet des fonctions permettant de mesurer la distance visuelle entre deux images (les métriques objectives et psycho visuelles : PSNR, RMSE, SSIM, HaarWavelet).

Tâches prévues

Pour la semaine prochaine, nous prévoyons :

— Ajouter à l'interface la possibilité de modifier les paramètres des filtres.

— Ajouter à l'interface la possibilité de sauvegarder l'image obscurcie.

— Rajouter et afficher les informations liées à la sécurité visuelle objective avec nos métriques (PSNR, RMSE, SSIM, HaarWavelet). Ces informations seront affichées lorsqu'un filtrage est appliqué.

— Créer un système de transfert d'apprentissage sur des classifieurs pré-entrainés sur différents "datasets", permettant de reconnaître des caractères ou des faces humaines.

Difficultés rencontrées et questionnements

La base de données ImageNet n'as aucune classe pour les humains ou pour les caractères. Nous allons donc être contraint de créer nos propres "datasets" pour ces domaines avec un système d'apprentissage par transfert.

Bibliographie

[1] *Andreea Bianca Popescu, Ioana Antonia Taca, Anamaria Vizitu, Cosmin Ioan Nita :*
(2022) Obfuscation Algorithm for Privacy-Preserving Deep Learning-Based Medical Image Analysis
https://www.researchgate.net

[2] *Christophe Charrier, Chaker Larabi, Hakim Saadane :*
(2005) Evaluation de la qualité des images
https://www.researchgate.net

[3] *Hanaa Abbas, Roberto Di Pietro :*
(2022) Sanitization of Visual Multimedia Content: A Survey of Techniques, Attacks, and Future Directions
https://www.researchgate.net

[4] *Jimmy Tekli, Bechara AL Bouna, Raphaël Couturier, Gilbert Tekli :*
(2019) A Framework for Evaluating Image Obfuscation under Deep Learning-Assisted Privacy Attacks
https://www.researchgate.net

[5] *Alexandre Devaux, Nicolas Paparoditis, Frederic Precioso, Bertrand Cannelle :*
(2009) Face Blurring for Privacy in Street-level Geoviewers Combining Face, Body and Skin Detectors
https://www.researchgate.net

[6] *Elaine M Newton, Latanya Sweeney, Bradley Malin :*
(2005) Preserving privacy by de-identifying face images
https://www.researchgate.net

[7] *Richard McPherson, Reza Shokri, Vitaly Shmatikov :*
(2016) Defeating image obfuscation with deep learning
https://www.researchgate.net

[8] *Rafael Reisenhofer, Sebastian Bosse, Gitta Kutyniok, Thomas Wiegand :*
(2018) A Haar Wavelet-Based Perceptual Similarity Index for Image Quality Assessment
https://www.researchgate.net

[9] *Slobodan Ribarica, Aladdin Ariyaeeiniab, Nikola Pavesic :*
(2016) De-identification for privacy protection in multimedia content: A survey

[10] *Tanaka, M., Echizen, I., and Kiya, H. :*
(2022) On the Transferability of Adversarial Examples between Encrypted Models

[11] *Hao, H., Guera, D., Horvath, J., Reibman, A. R., and Delp, E. J. :*
(2020) Robustness analysis of face obscuration