Université de Montpellier
Master 2 - IMAGINE

Safe-Eye

Évaluation de la sécurité visuelle d'images obscures par CNN

Compte rendu — 5
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

Nous avons terminé l'interfaçage tkinter avec notre dernier ajout, celui d'offrir la possibilité à l'utilisateur de modifier les paramètres des filtres d'obscurcissement.

Nous avons donc une application avec interface graphique capable d'effectuer plusieurs types de détection ("MTCNN" et "YOLOv3"). Elle offre à l'utilisateur la possibilité d'appliquer jusqu'à cinq filtres d'obscurcissement sur une zone de l'image choisie. De plus, nous proposons plusieurs métriques pour mesurer la distance visuelle entre l'image obscurcie et l'image originale (PSNR, SSIM, HaarPSI).

La dernière étape de notre projet consiste à attaquer nos images obscurcies avec des GAN.

Tâches prévues

Pour la semaine prochaine, nous prévoyons de continuer l'implémentation d'un GAN permettant d'attaquer nos images obscurcies et ainsi pouvoir mesurer la réversibilité des techniques d'obscuration que nous utilisons.

Nous envisageons également de mettre en place le système d'évaluation utilisateur.

Difficultés rencontrées et questionnements

Les premiers résultats obtenus avec notre GAN ne sont pas à la hauteur et nous allons faire des recherches afin de les améliorer.

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