Université de Montpellier
Master 2 - IMAGINE

Safe-Eye

Évaluation de la sécurité visuelle d'images obscures par CNN

Compte rendu — 4
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

Pour le moment, nous améliorons notre interface utilisateur Tkinter en ajoutant plusieurs options supplémentaires. Comme par exemple :

- La possibilité de choisir l'ordre des filtres à appliquer sur l'image permettant de simplifier le processus de combinaison des filtres.
- L'affichage des métriques indiquant la ressemblance entre l'image originale et l'image actuellement obscurcie.
- L'enregistrement de l'image obscurcie finale avec application des filtres.

Nous avons également ajouté des CNN permettant de détecter des éléments dans une image :

- Le premier CNN que nous utilisons est "YOLOv3", entraîné sur la base de données "COCO" (Common Objects in COntext). Ce classifieur nous permet d'analyser rapidement le contenu d'une image pour en extraire des boîtes englobantes automatiquement (80 classes possibles).
- Le second CNN est MTCNN (Multi-Task Cascaded Convolutional Neural Networks) nous permettant d'analyser avec plus de précision les visages humains à l'aide des repères faciaux.

Enfin nous avons lié ces classifieurs à notre interface, ce qui nous permet de déterminer automatiquement des régions d'intérêts afin d'y appliquer des filtres si l'utilisateur le souhaite.
De plus un nouveau filtre d'obscurcissement a été ajouté : le "mélange".

Tâches prévues

Pour la semaine prochaine, nous prévoyons :

- Ajouter à l'interface la possibilité de modifier les paramètres des filtres.
- Ajouter des attaques par GAN afin de mesurer la réversibilité des techniques d'obscuration que nous utilisons.
- Mettre en place un système d'évaluation utilisateur.

Difficultés rencontrées et questionnements

Aucun problème particulier cette semaine et nos questions ont été clarifiées grâce à Bianca et Nicolas !

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