Évaluation de la sécurité visuelle d'images obscures par CNN

Aurélien Besnier - Alexandre Spatola

Plan

1. Base de données
2. Méthodes d'obscuration
3. Outils
4. Réseau siamois
5. GUI
6. Analyse des résultats
7. Perspectives
8. Démonstration

Base de données

Labeled faces in the wild (LFW): https://vis-www.cs.umass.edu/lfw/

- 13000+ images
- 1680 personnes
- Images issues du Web
- Images de taille 250x250
- Ensembles de paires fournis

Obscuration

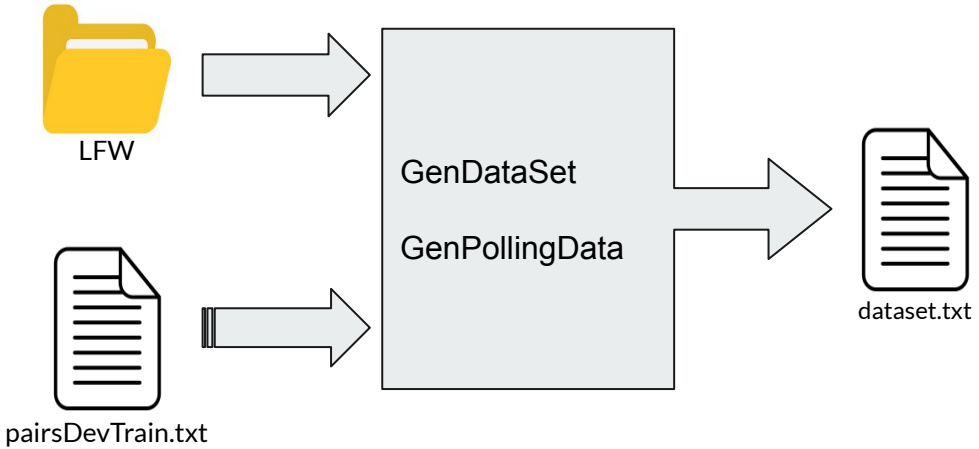
Floutage

Pixellisation

Retrait d'information

Outils : GenDataSet & GenPollingData

- Génération de datasets pour le reste du pipeline
- Formats respectifs : triplets et paires
- Utilisation du dataset fourni par LFW ou génération entièrement automatique
- Format simple similaire à celui de LFW

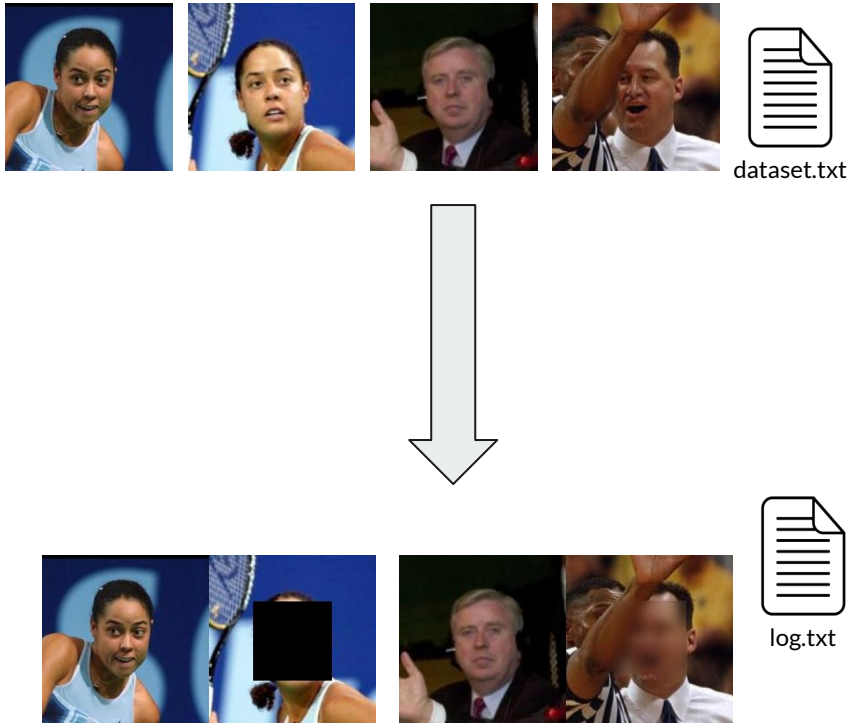


Outils : Faceloc

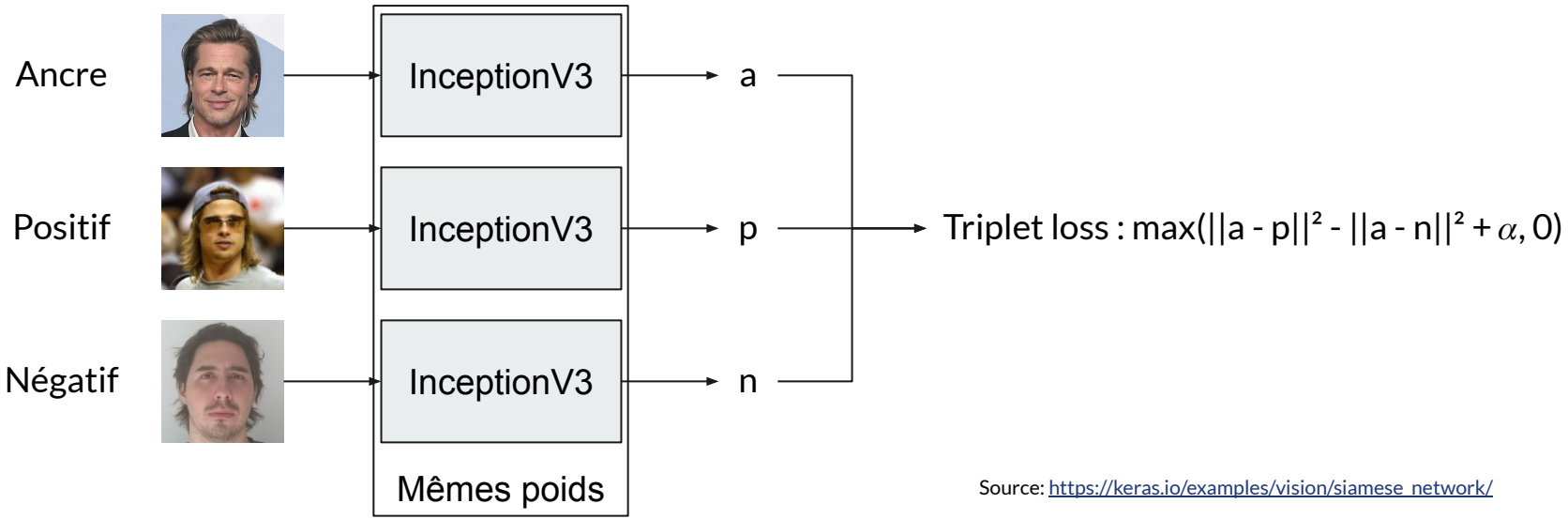
- Bibliothèque basique utilisée par les outils d'obscuration automatique
- Permet de charger une image en même temps que l'emplacement du visage
- Détection automatique de visage par haarcascade
- En cas de détection infructueuse (0 ou 2+ visages) : intervention humaine
- Sauvegarde les résultats dans un fichier

Outils : ObscureDataSet

- Basé sur tous les outils précédents
- Génère un ensemble d'images pré-obscurées prêt à l'emploi
- Le log liste les méthodes d'obscuration utilisées
- La première image n'est jamais obscurée
- Pour les paires :
  - Indique si les personnes sont les mêmes
  - Concatène les images



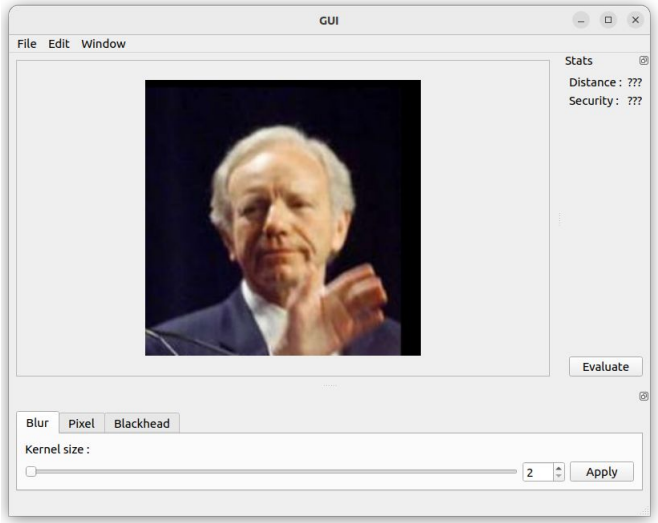
Réseau siamois

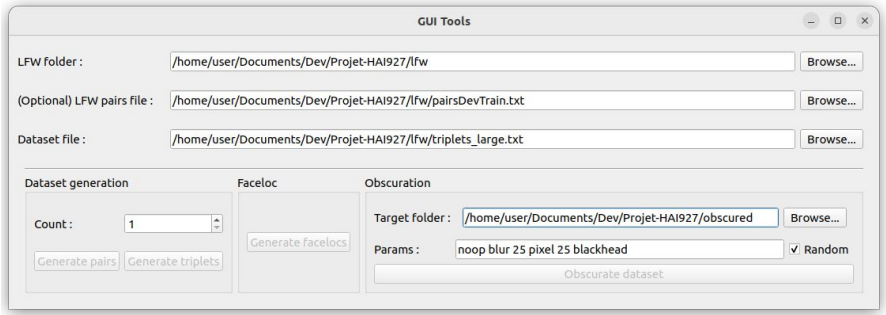


Source: https://keras.io/examples/vision/siamese_network/

GUI

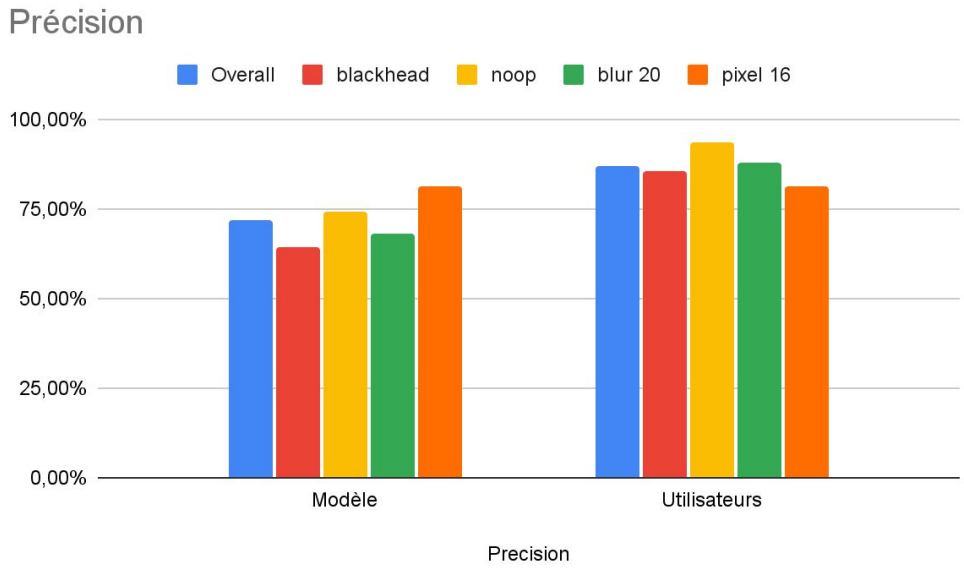
- Accès intuitif à toutes les fonctionnalités développées
- Supporte le chargement et la sauvegarde d'images
- Permet de zoomer/dézoomer
- Prend en charge le Undo/Redo
- Accès au CNN entraîné depuis le C++ (frugally-deep[1])





[1] https://github.com/Dobiasd/frugally-deep

Analyse des résultats



- Blackhead plus sécurisé pour le modèle.
- Le modèle est très performant face à la pixellisation.
    - Contrairement aux humains !
- Cacher le visage ne suffit pas !

Perspectives

- Étendre le jeu de données
- Expérimenter des modèles de base différents
- Travailler plus sur les hyper-paramètres
- Améliorer l'interprétation de la sortie du modèle
- Varier les méthodes d'obscuration
- Améliorer la détection de visages
- Entraîner un modèle par type d'obscuration

Démonstration