



# ÉVALUATION DE LA SÉCURITÉ VISUELLE D'IMAGES OBSCURES PAR CNN

AURÉLIEN BESNIER - ALEXANDRE SPATOLA

IMAGINE 2022



## INTRODUCTION

Le but de ce projet est de déterminer si plusieurs techniques d'obscurisation permettent de préserver certaines informations dans les images. Ce projet se concentre sur l'identité des personnes. Dans un contexte où les données images sont constamment échangées en ligne, il se peut que l'on veuille garder l'identité d'une personne confidentielle (reportage télé, protection de témoins,...) ou encore certaines informations liées à l'identité d'une personne (biométrie,...).

Pour évaluer cette sécurité, nous utilisons un réseau siamois qui permet de calculer une similarité entre deux images. Ceci permet ensuite de savoir si une image obscure d'une personne est similaire à une autre de cette personne. Dans le cas où l'obscurisation est bonne, cela ne doit pas être le cas.

## LABELLED FACES IN THE WILD (LFW)



Source: <https://vis-www.cs.umass.edu/lfw/>

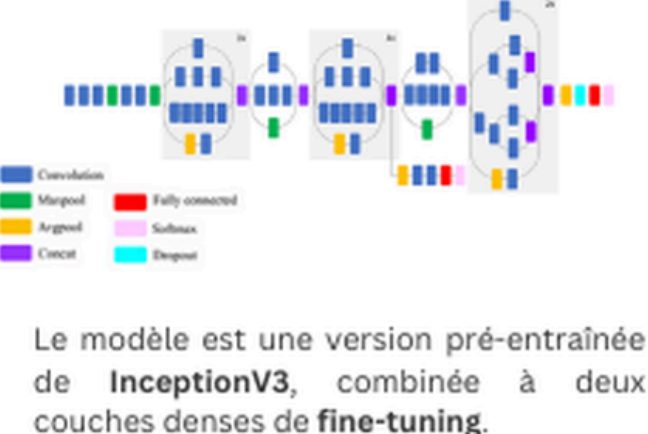
La base de données utilisée dans ce projet est la base LFW constituée comme suit:

- 13000 images
- 1680 personnes
- Images issues du Web
- Images de taille 250x250

Dataset

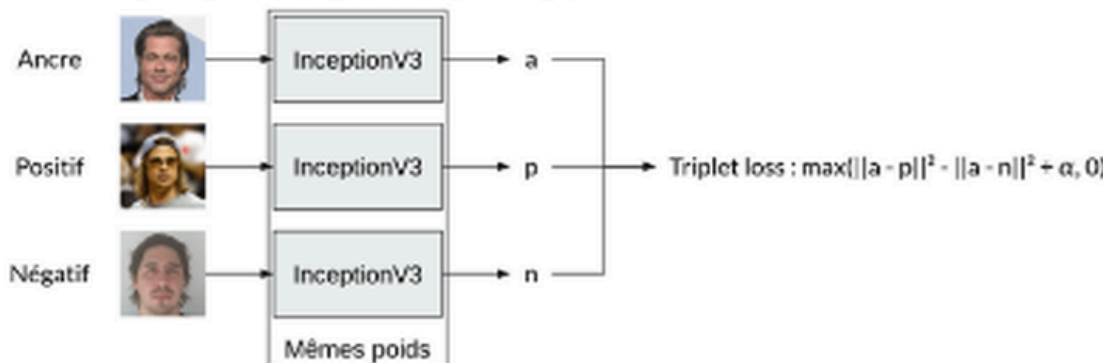
## MODÈLE

### Réseau :



Le modèle est une version pré-entraînée de **InceptionV3**, combinée à deux couches denses de **fine-tuning**.

### Entraînement:



Le modèle est inséré dans un **réseau siamois**, puis entraîné sur la base d'un **triplet loss**. Les triplets sont composés d'une image de référence, l'**anc**re, d'une image de la même personne, le **positif**, et d'une image d'une personne différente, le **né**gatif. L'ancre est toujours en clair, mais les deux autres peuvent être obscurées.

### Usage:

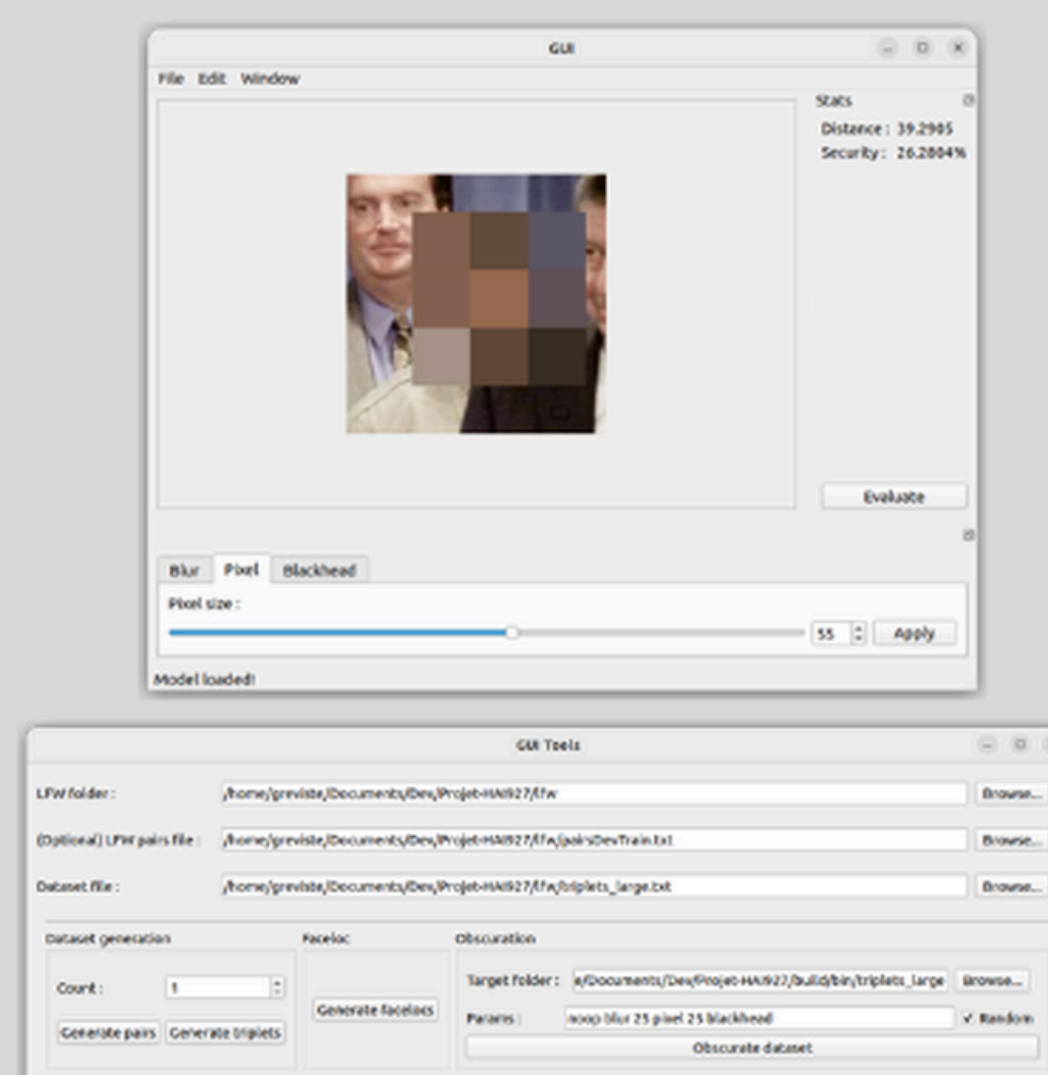
Une fois le modèle entraîné, il peut être extrait du réseau siamois et utilisé sur des images seules. Les résultats sont un **vecteur de caractéristiques**. Plus la **distance** entre les vecteurs d'une image obscurée et d'une autre image en clair de la même personne est faible, moins l'anonymat est respecté.

## GUI

La GUI regroupe nos travaux en un logiciel unique et simple d'utilisation.

Fonctionnalités :

- Chargement et sauvegarde d'images
- Sélection de zones d'intérêt dans l'image
- Obscurisation paramétrable et inversible
- Évaluation de la sécurité à l'aide du modèle entraîné
- Accès aux outils de manière graphique et intuitive



## OUTILS

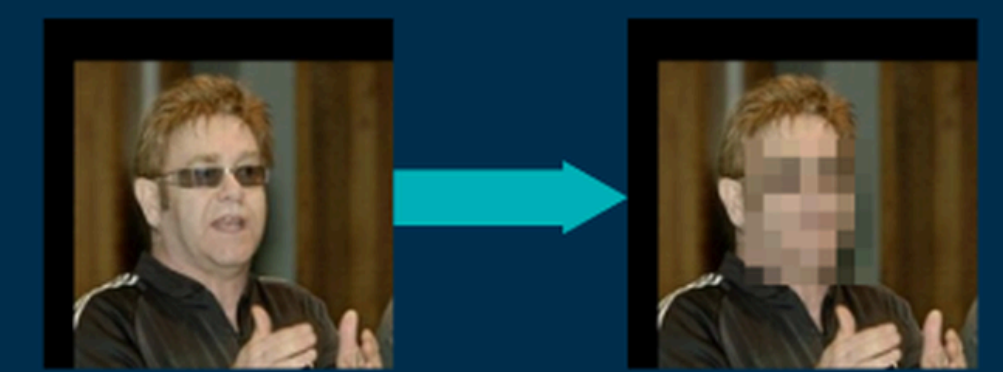
La réalisation de ce projet a nécessité la création de nombreux outils.

Certains sont liés directement à la problématique, comme les outils d'obscurisation, et d'autres sont plutôt nécessaires au développement du projet.

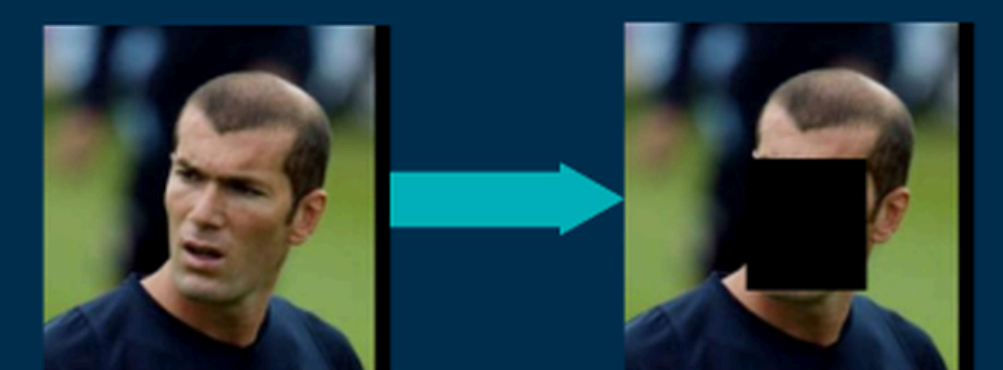
### Floutage



### Pixellisation



### Blackhead



### GenDataSet/GenPollingData

Ces outils servent à générer, à partir du contenu de LFW ou des fichiers fournis avec, un listing de triplets ou de paires, respectivement.

### Faceloc

Automatise la détection des visages, afin de savoir où appliquer les obscurisations. Demande une localisation manuelle à l'utilisateur en cas d'échec, et sauvegarde les résultats pour les réutiliser.

### ObscureDataSet

Utilise les outils précédents et leurs résultats pour générer des jeux d'images pré-obscurées, de manière paramétrable. Sauvegarde également quelle méthode a été utilisée pour chaque jeu d'images.

## OUTILS DE DÉVELOPPEMENT



## REMERCIEMENTS / SOURCES

Source: <https://github.com/AurelienBesnier/Projet-HAI927>

Remerciements à William Puech, Nicolas Dibot & Bianca Jansen Van Rensburg

