

# Détection et reconnaissance de visage dans des images d'archive

Thomas Varin  
Encadré par : Tanguy Gernot

GREYC/SAFE

Du 03/06/2024 au 23/08/2024

- 1 Introduction
- 2 Création et détection de deepfake
  - Création de deepfake
  - Détection de deepfake
- 3 Détection et reconnaissance de Visages
  - Comparaison des algorithmes
  - Résultats
  - Choix des paramètres
  - Présentation de l'outil
- 4 Conclusion

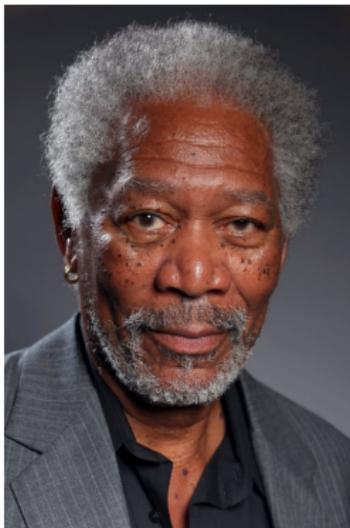
- 1 Introduction
- 2 Création et détection de deepfake
  - Création de deepfake
  - Détection de deepfake
- 3 Détection et reconnaissance de Visages
  - Comparaison des algorithmes
  - Résultats
  - Choix des paramètres
  - Présentation de l'outil
- 4 Conclusion

# Déroulement du stage

- 1 Reconnaissance (3 juin au 21 juin)
- 2 Deepfake SummerSchool (24 juin au 5 juillet)
- 3 Reconnaissance (8 juillet au 23 août)

- 1 Introduction
- 2 Création et détection de deepfake
  - Création de deepfake
  - Détection de deepfake
- 3 Détection et reconnaissance de Visages
  - Comparaison des algorithmes
  - Résultats
  - Choix des paramètres
  - Présentation de l'outil
- 4 Conclusion

## Contexte



Morgan Freeman (TMDB)



Deepfake (Diep Nep)

# Contexte



Image truquée



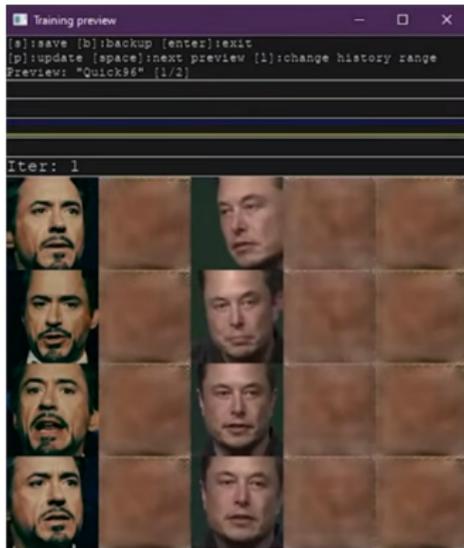
Vue par Forensically

# Création de deepfake

DeepFaceLab, Faceswap, Deep-Live-Cam

- 1 Extraction des visages
- 2 Localisation des points clés
- 3 Extractions de caractéristiques
- 4 Échange des caractéristiques
- 5 Reconstruction de la vidéo
- 6 Correction des détails

# Création de deepfake (DeepFaceLab)



Premières itérations



Dernières itérations

# Résultat du deepfake

Présentation du résultat

# Méthodes basées sur l'IA

- 1 Fréquence des clignements d'yeux
- 2 Fluidité des mouvements
- 3 Détection d'anomalies/artefacts

# Mise en difficulté du deepfake

- 1 Rotation de la tête à 90°
- 2 Obstruction du visage
- 3 Changement de luminosité

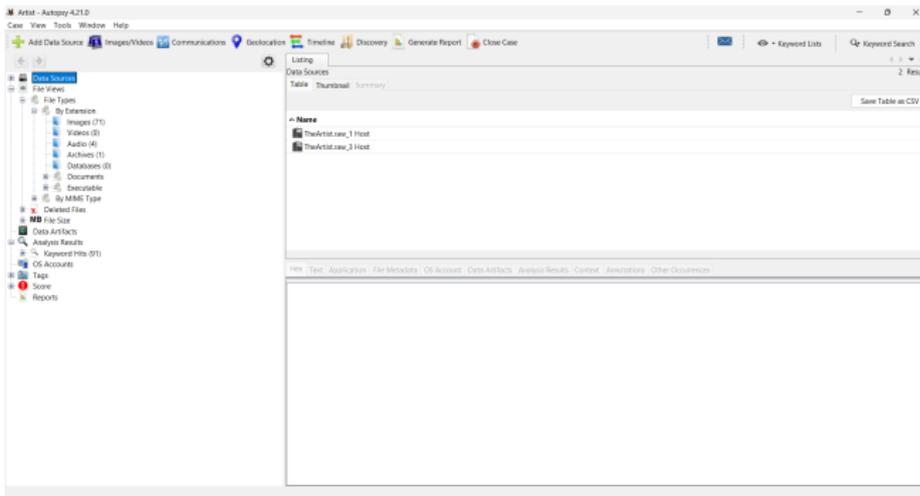
- 1 Introduction
- 2 Création et détection de deepfake
  - Création de deepfake
  - Détection de deepfake
- 3 Détection et reconnaissance de Visages
  - Comparaison des algorithmes
  - Résultats
  - Choix des paramètres
  - Présentation de l'outil
- 4 Conclusion

## Différents acteurs

m/  
institut mémoires  
de l'édition  
contemporaine/

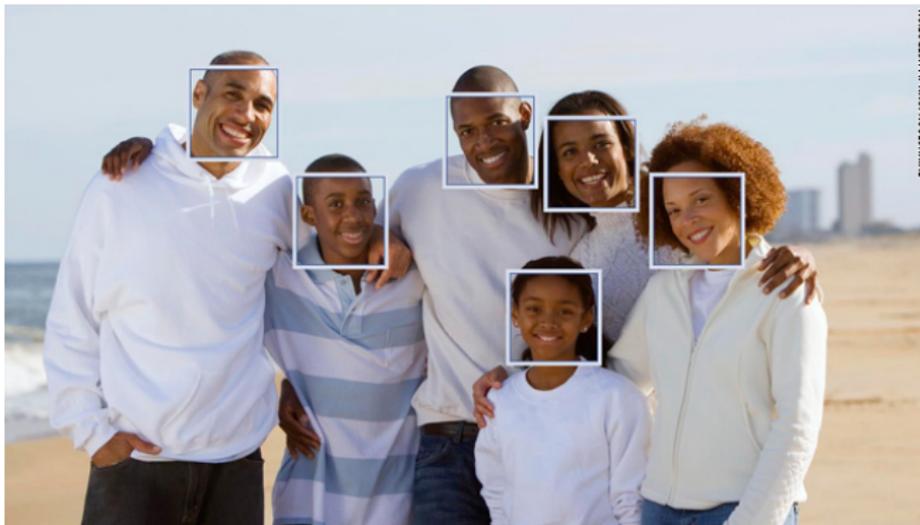


# Environnement de travail



## Interface d'Autopsy

## Présentation du contexte



Crédit : CNN

# État de l'art

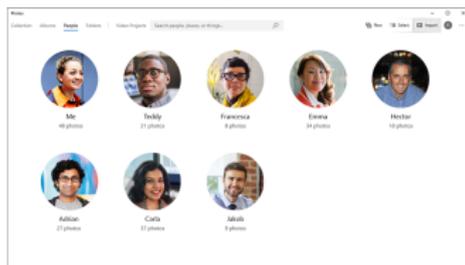


TinEye



PimEyes

# État de l'art



Google Photos



IOS

# Présentation des algorithmes

Deux algorithmes :

- 1 face\_recognition
- 2 MTCNN et VGGFace

# Présentation des datasets

Deux datasets :

- 1 Labelled Faces in the Wild (1680 classes, 9164 images)
- 2 Portrait and 26 photos (14 classes, 378 images)

# Quelques notations

## Definition

$$FAR(t) = \begin{cases} \frac{F_+(t)}{F_+(t) + T_-(t)}, & \text{si } F_+(t) \neq 0 \\ 0, & \text{sinon} \end{cases}$$

# Quelques notations

## Definition

$$FRR(t) = \begin{cases} \frac{F_-(t)}{F_-(t) + T_+(t)}, & \text{si } F_-(t) \neq 0 \\ 1, & \text{sinon} \end{cases}$$

# Quelques notations

## Definition

$$EER = \min_{0 \leq t \leq 1} \max\{FAR(t), FRR(t)\}$$

# Quelques notations

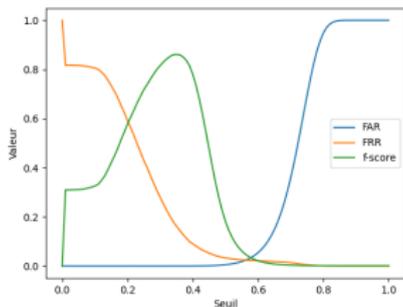
## Definition

$$F_1 = \frac{2T_+(t)}{2T_+(t) + F_+(t) + F_-(t)}$$

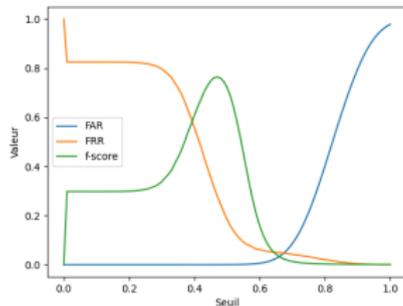
# Fonctionnement des tests

- 1 Première image comme référence
- 2 Une décision par image
- 3 Accepté  $\Leftrightarrow$  Une personne correspond
- 4 Testé sur un grand nombre de seuils
- 5 Priorité sur les grandes classes

# Résultats sur LFW



MTCNN et VGGFace



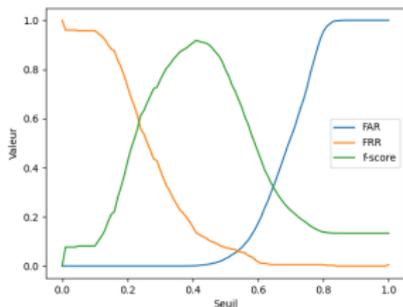
face\_recognition

# Résultats sur LFW

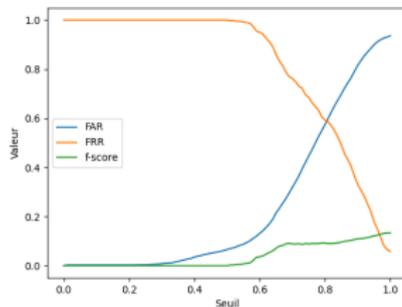
Classes \ Algorithme	MTCNN/VGGFace	face_recognition
10	<b>0.017</b>	0.051
20	<b>0.013</b>	0.048
50	<b>0.015</b>	0.045
100	<b>0.023</b>	0.049
200	<b>0.026</b>	0.048
500	<b>0.025</b>	0.045
1000	<b>0.025</b>	0.046
1680	<b>0.024</b>	0.047

EER pour VGGFace et face\_recognition avec LFW

# Résultats sur Portrait and 26 Photos



MTCNN et VGGFace



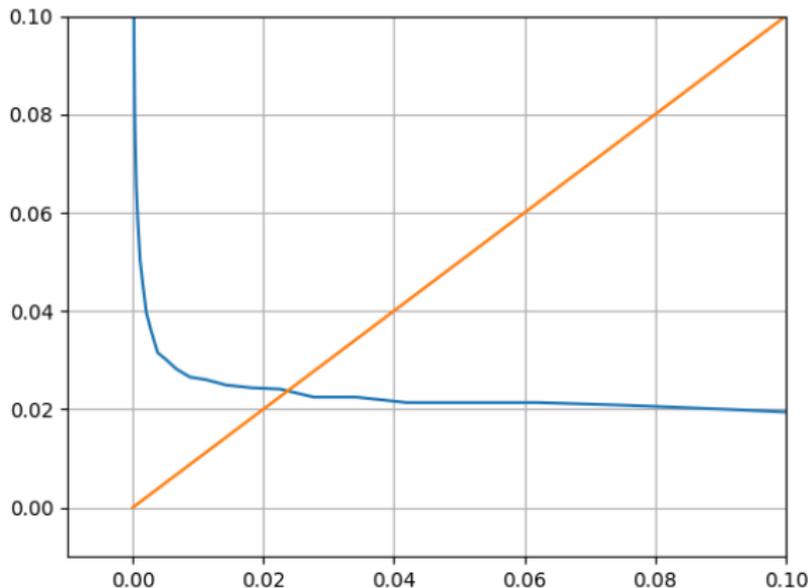
face\_recognition

# Résultats sur Portrait and 26 Photos

Classes \ Algorithmes	MTCNN/VGGFace	face_recognition
14	<b>0.061</b>	0.58

EER pour VGGFace et face\_recognition avec Portrait

# Choix du seuil



# Choix du seuil

Seuil \ Mesure	FAR	FRR
0.542	0.024	0.024
0.520	0.014 ( $\div 1.64$ )	0.024 ( $\times 1.07$ )
0.500	0.008 ( $\div 2.70$ )	0.026 ( $\times 1.14$ )
0.480	0.005 ( $\div 4.63$ )	0.030 ( $\times 1.29$ )
0.460	0.002 ( $\div 8.47$ )	0.036 ( $\times 1.55$ )
0.440	0.0015 ( $\div 15.55$ )	0.045 ( $\times 1.96$ )

Évolution des FAR et FRR en fonction du seuil choisi

## Gestion des références multiples

Soit  $n \in \mathbb{N}$ ,  $(x_1, \dots, x_n) \in \mathbb{R}^n$ ,  $t \in \mathbb{R}$ ,  $\sigma \in \mathfrak{S}_n$  et  $x \in \mathbb{R}$

$$\min_{i=1, \dots, n} x_i \leq f(x_1, \dots, x_n) \leq \max_{i=1, \dots, n} x_i$$

$$f(x, x, \dots, x) = x$$

$$f(tx_1, \dots, tx_n) = tf(x_1, \dots, x_n)$$

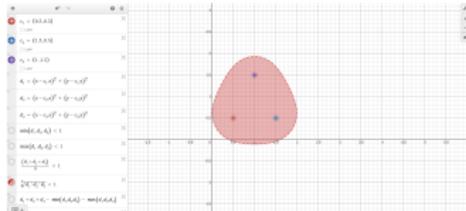
$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n)$$

$x_i \mapsto f(x_1, \dots, x_i, \dots, x_n)$  est croissante

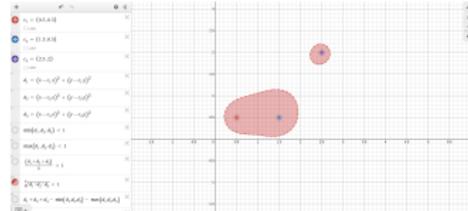


## Choix des paramètres

## Choix de la fonction finale



Trois références proches



Une référence éloignée des autres

<https://www.desmos.com/calculator/np5q9nyka>

## Arguments de l'outil

- (Obligatoire) Le dossier contenant les images à traiter
- (Obligatoire) Le dossier contenant la ou les références
- (Optionnel) La méthode d'agglomération (dans le cas d'une seule référence l'argument est sans conséquence)
- (Optionnel) Un seuil haut et un seuil bas (afin d'avoir des images très probables et probables)
- (Optionnel) Une commande d'affichage des images trouvées





# Résultats



Seuil bas

- 1 Introduction
- 2 Création et détection de deepfake
  - Création de deepfake
  - Détection de deepfake
- 3 Détection et reconnaissance de Visages
  - Comparaison des algorithmes
  - Résultats
  - Choix des paramètres
  - Présentation de l'outil
- 4 Conclusion

# Conclusion

- Quelques difficultés techniques
- MTCNN/VGGFace plus performants
- Suite : Algorithmes de classification

# Questions

Merci pour votre attention !  
Avez-vous des questions ?