Ecole Publique d'Ingénieurs en 3 ans

Rapport

GDIP - PROJET FORENSIQUE: CAPTEURS ET CATEGORISATION

le 04 avril 2022,

Julien Rauch
Kevin Curtet
Maxime Casati
Eva Petauton

Tuteur: **Christophe Rosemberger**

www.ensicaen.fr

TABLE DES MATIERES

TABLE DES FIGURES

INTRODUCTION

Dans le cadre de notre cursus en 2A Informatique à l'ENSICAEN, nous sommes amenés à travailler sur un projet tout au long de l'année. Différentes problématiques proposées par différents clients nous ont été proposées. Nous avons choisi de travailler avec les chercheurs du GREYC, sous la responsabilité de Christophe Rosenberger sur le projet de plateforme forensique. Ainsi, ce document est le rapport de fin de projet, concernant la performance de programmes de catégorisation d'images, ainsi que de l'identification de capteurs.

Le GREYC souhaite développer une plateforme d'analyse forensique se nommant GDIP (Greyc Digital Investigation Platform) qui proposerait un ensemble d'outils pour l'analyse forensique. Les applications envisagées sont notamment l'aide à l'investigation policière, l'analyse de traces numériques d'auteurs contemporains (IMEC) ainsi que la recherche sur la protection de la vie privée. La plateforme aura également une portée pédagogique.

Dans ce cadre, nous devons récupérer différentes implémentations Open Source visant à l'analyse d'images. Dans un premier cas nous cherchons à identifier le capteur (comprendre : appareil photo) ou le modèle de capteur qui a servi à les réaliser. Dans un deuxième cas, nous cherchons à catégoriser les images selon différents critères, afin par exemple de savoir quels images présentes dans un disques dur contiennent des visages humains, ont été prises à l'extérieur. Chaque implémentation sera testée afin de déterminer lesquelles sont les plus efficaces, notamment en terme de temps ou de pourcentage d'identification juste. Tout cela a pour but de rendre plus facile l'analyse forensique.

OBJECTIFS

1. Objectifs finaux

Ce projet a pour objectif de mesurer la performance de programmes filtres sur des images dans deux catégories :

- Le capteur utilisé (appareil photo, caméra de téléphone…)
- Une catégorisation de l'image (scène d'intérieur ou d'extérieur, présence ou non d'humains…)

Nous avons aussi pour objectif de proposer pour le projet GDIP de ces programmes afin d'enrichir leur plateforme. Le rapport fourni en fin de projet pourra être utilisé par n'importe qui afin de l'aider à choisir le programme le plus performant selon ses besoins. Notre projet sera à disposition des chercheurs du GREYC, et par la suite sur un site internet.

Dans un premier temps nous devions réaliser un état de l'art du sujet. Pour cela nous devions faire des recherches d'articles scientifiques dans le but de constituer une bibliographie qui puisse soutenir le projet. Dans le but d'être utile au plus grand nombre nous avons pris la décision de faire cet état de l'art en anglais.

Puis dans un second temps trouver les programmes Open Sources ainsi que des bases de données portant sur le sujet, ou bien créer les bases de données si nous n'en trouvons pas.

Et enfin tester les filtres que nous avons trouvés et quantifier leur performance (vitesse, capacité, exactitude, etc…).

2. Objectifs à mi-parcours

Nos objectifs pour la fin du mois de janvier 2022 étaient la réalisation d'un état de l'art des solution existantes ; la recherches de filtres openSource ; la création ou la recherche d'une base de données pour tester les filtres et la réalisation du cahier des charges des tests. Ces objectifs ont été détaillés dans le rapport de mi-projet.

PROJET

1. Travail réalisé

1.1. Organisation du projet

1.1.1. Méthodologie

Concernant la méthodologie, nous avions comme consigne de ne pas être dans l'agilité mais plutôt dans la méthodologie de projet classique comme cela nous a pu être enseigné durant notre première année à l'ENSICAEN. Ainsi nous avons fait un kick off qui comprenait notamment un diagramme de Gantt et divers objectifs définis.

La performance des programmes est établie en fonction de la précision de leurs résultats.

1.1.2. Déroulement

Nous nous sommes réparti le travail en deux groupes, deux binômes, l'un travaillant sur la catégorisation et l'autre travaillant sur les capteurs. Pour les deux groupes, nous avons utilisés des filtres basés sur des réseaux neuronaux convolutifs.

Par ailleurs, une des méthodes que nous avons testée est la méthode dite de *Transfer Learning*. Le Transfert Learning consiste à utiliser un réseau de neurones préformé pour extraire les caractéristiques d'une image, puis à utiliser un modèle (régression logistique ou smv linéaire) pour s'entrainer après.

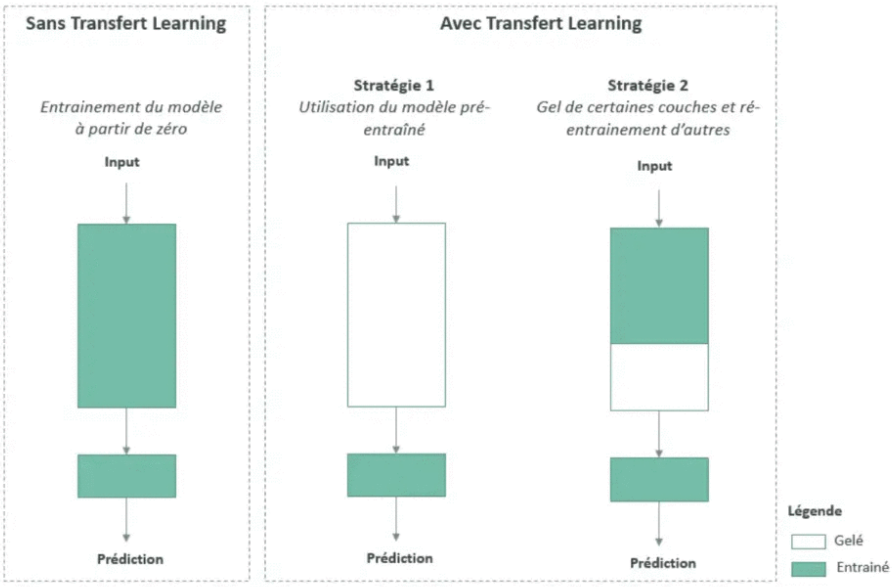


Figure 1 : Représentation du Transfert Learning (Thomas, Lina, & Gary, 2020)

Nous avons donc utilisé la stratégie numéro 1, en utilisant le CNN VGG16 afin d'entrainer notre filtre (partie « gelé » sur le schéma), puis en utilisant une régression linéaire une fois le filtre entrainé (partie « entrainé » sur le schéma). Par ailleurs, VGG16 a été entrainé sur imagenet, spécialisé dans la reconnaissance d'objet. Ainsi il est particulièrement adapté à la catégorisation de l'image, mais assez peu à l'identification de capteurs.

Pour cette partie nous nous sommes basés sur un tutoriel (Rosebrock, 2019) sur le transfer learning avec le module Keras. Ainsi nous avons fait du transfer learning, mais plus particulièrement nous avons utilisé la technique d'extraction de caractéristiques. On passe nos images dans le CNN et on s'arrête à un moment. On extrait les valeurs de cette couche spécifique et on les stock dans un vecteur. Une fois obtenus nos vecteurs de caractéristiques, nous pouvons entrainer directement des modèles, comme ici celui de régression logistique.

1.1.3. Difficultés rencontrées

Nous avons eu un membre de l'équipe projet qui a été dans l'incapacité de travailler pendant trois mois. Cet événement a handicapé l'un des binômes et a posé problème sur les objectifs que nous avions. Mais nous avons eu des contacts réguliers avec le client ce qui nous a permis de nous orienter dans le projet et de redéfinir nos objectifs au vu de la contrainte temps. Nous avons donc réussi à tenir les délais.

Concernant les difficultés rencontrées, malgré un intérêt scientifique évident pour la discipline de reconnaissance de capteurs, nous trouvons très peu de programmes qui implémente les solutions proposées par les chercheurs. La deuxième difficulté que nous avons rencontré est liée aux datasets. En effet chaque année sortent de nombreux nouveaux modèles de caméra et il n'existe aucune base de donnée exhaustive. Par ailleurs, pour la catégorisation de l'image, les datasets ont aussi été facteurs de difficulté. En effet, trouver des bases de données concernant le filtre étudié, avec une grande quantité d'images pour que le test soit exhaustif ainsi qu'une grande diversité (notamment dans le cas de la reconnaissance de visage, diversité d'ethnie, de genre…).

1.2. Résultats

1.2.1. Capteurs

Nous avons trouvé deux datasets, l'une de 35000 images provenant de 35 capteurs dataset Vision : (Shullani, et al., 2017) et l'autre de 103 capteurs : dataset SocrateS (EURECOM, 2017). Nous avons ainsi pu tester 2 programmes : Transfer learning avec VGG16 de keras et formation d'un CNN avec keras. Le CNN provient de cet article : (Bernacki, 2021).

Les résultats du réseau de neurone entrainé par nous-même des deux datasets sont ainsi :

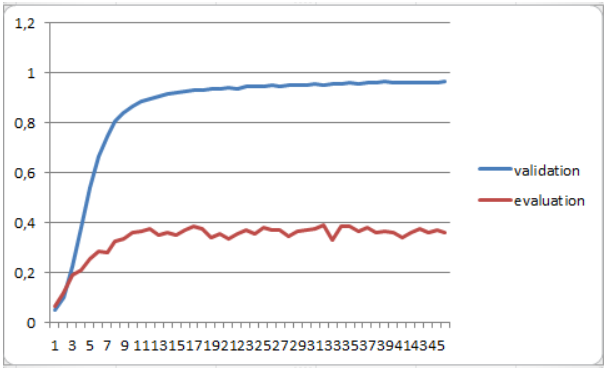


Figure 2 : Proportion de résultats justes par rapport au nombre d'entrainements pour le dataset Vision

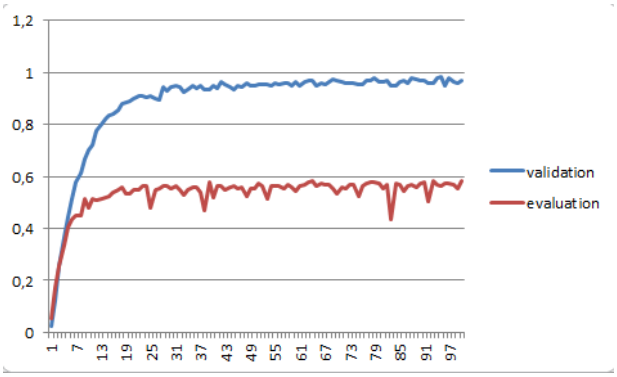


Figure 3 : Proportion de résultats justes par rapport au nombre d'entrainements pour le dataset SocrateS

La mauvaise adaptation du CNN est due à son sur-ajustement.

Concernant la méthode du transfer learning, les résultats sur le dataset SocrateS ont une moyenne de 66% de réussite par appareil. Concernant le dataset Vision, la réussite est de 57% en moyenne.

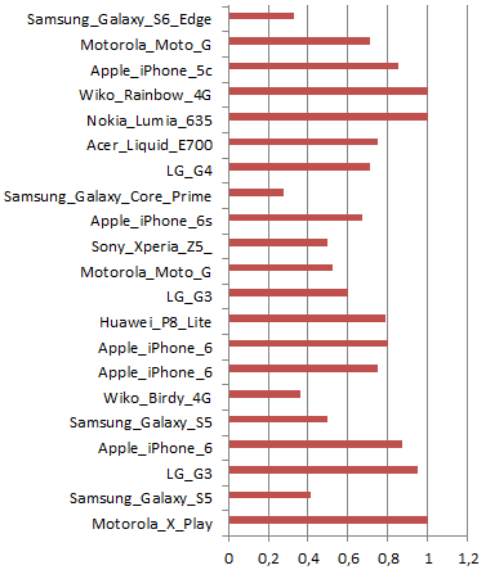
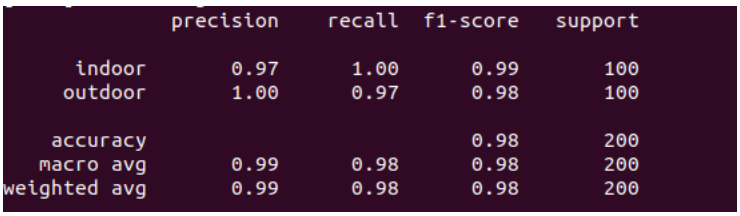


Figure 4 : Exemple de précision pour 21 capteurs du dataset SocrateS

1.2.2. Catégorisation de l'image

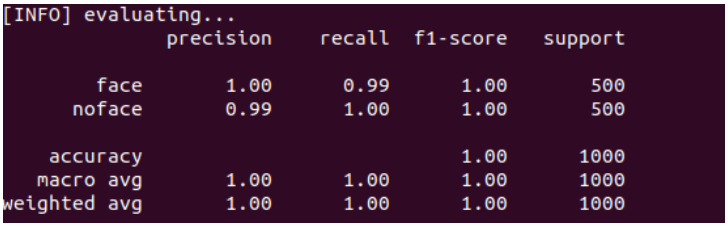
Nous nous sommes basés sur deux datasets d'images d'extérieur et d'intérieur venant de (Quattoni & Torralba, 2009) & (Olivia & Torralba, 2001) du MIT. Nous avons fait en sorte d'avoir un même nombre d'image dans les deux datasets, soit environ 2400 par catégorie. Nous avons ainsi pu tester le Transfer learning avec VGG16 de keras pour cet ensemble, après avoir testé notre modèle sur 100 images par catégorie, nous obtenons une précision de 98%, ce qui est très bien.



	precision	recall	f1-score	support
indoor	0.97	1.00	0.99	100
outdoor	1.00	0.97	0.98	100
accuracy			0.98	200
macro avg	0.99	0.98	0.98	200
weighted avg	0.99	0.98	0.98	200

Figure 5 : Résulats de notre CNN pour indoor/outdoor

Concernant la détection de visages, nous avons utilisé deux dataset. Le premier pour les images sans visage (Griffin, Holub, & Perona, 2006), il contient 256 catégories d'images et d'objets. Nous avons dû passer ce dataset au peigne fin pour enlever les visages humains présent. Le second contenant des visages (Song & Zhang, 2017). Nous avons ainsi obtenu un modèle juste à 99%. Nous pourrions améliorer notre modèle en fournissant des images avec visages humains qui soient moins évident qu'une image plein pied, nous aurions un modèle plus efficace en pratique.



[INFO] evaluating...

	precision	recall	f1-score	support
face	1.00	0.99	1.00	500
noface	0.99	1.00	1.00	500
accuracy			1.00	1000
macro avg	1.00	1.00	1.00	1000
weighted avg	1.00	1.00	1.00	1000

Figure 6 : Résulats de notre CNN pour face / noface

Nous avons obtenus de très bon résultat pour cette partie, car le CNN sur lequel se base notre technique est le VGG16, qui est entrainé sur un dataset spécialisé dans la reconnaissance d'objet comme nous l'avons précisé plus haut.

2. Objectifs non atteints & suite du projet

Nous n'avons pu tester qu'une seule méthode pour la catégorisation de l'image par manque de temps. Aussi nous n'avons pu quantifier que la précision (i.e la justesse) du filtre et non son temps d'exécution pour les différentes méthodes. Pour la suite du projet, il serait possible de tester plus de méthodes différentes et diversifier les catégories pour la partie catégorisation.

CONCLUSION-

En conclusion, malgré les difficultés que nous avons pu rencontrer, nous avons pu trouver des résultats très intéressant. Concernant la catégorisation de l'image, nos résultats sont quasi-parfait et cela nous donne une route très encourageante pour avoir des filtres efficaces. Concernant les capteurs, nous avons eu des résultats moins probants, diverses pistes doivent donc encore être explorées afin de trouver une méthode qui conduirait à de meilleurs résultats.

Nous remercions les enseignants chercheurs qui nous ont encadrés et accompagnés durant ce projet, et nous espérons que d'autres étudiants, stagiaires ou chercheurs pourront continuer à développer ce projet.

BIBLIOGRAPHIE

Bernacki, J. (2021, juillet 07). *Robustness of digital camera identification with convolutional neural networks*. Récupéré sur Springer Link: https://link.springer.com/article/10.1007/s11042-021-11129-y?utm_source=xmol&utm_medium=affiliate&utm_content=meta&utm_campaign=DDCN_1_GL01_metadata

EURECOM. (2017). *SOurce Camera REcognition on Smartphones*. Récupéré sur SocrateS: http://socrates.eurecom.fr/

Griffin, G., Holub, A., & Perona, P. (2006). *The CALTECH 256*. Récupéré sur California Institute of Technology: http://www.vision.caltech.edu/Image_Datasets/Caltech256/

Lopez-Martin, M., Carro, B., Lloret, J., & Sanchez-Esguevillas, A. (2017). *Network Traffic Classifier With Convolutional and Recurrent Neural Networks for Internet of Things.*

Olivia, A., & Torralba, A. (2001). *Modeling the shape of the scene: a holistic representation of the spatial envelope*. Récupéré sur MIT: http://people.csail.mit.edu/torralba/code/spatialenvelope/

Quattoni, A., & Torralba, A. (2009). *Indoor Scene Recognition*. Récupéré sur MIT: http://web.mit.edu/torralba/www/indoor.html

Rosebrock, A. (2019, 05 20). *Transfer Learning with Keras and Deep Learning*. Récupéré sur pyimagesearch: https://pyimagesearch.com/2019/05/20/transfer-learning-with-keras-and-deep-learning/

Shullani, Dasara and Fontani, Marco and Iuliani, Massimo and Al Shaya, Omar and Piva, & Alessandro. (2017, 12). *Datasets - VISION - a video and image dataset for source identification*. Récupéré sur LESC: https://lesc.dinfo.unifi.it/en/datasets

Song, Y., & Zhang, Z. (2017). *UTKFace - Large Scale Face Dataset*. Récupéré sur github: https://susanqq.github.io/UTKFace/

Thomas, B., Lina, F., & Gary, B. (2020, Juillet 21). *Transfer Learning : Qu'est-ce que c'est ?* Récupéré sur DataScientest: https://datascientest.com/transfer-learning

ENSI CAEN

ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Ecole Publique d'Ingénieurs en 3 ans

6 boulevard Maréchal Juin, CS 45053
14050 CAEN cedex 04

ministère éducation nationale enseignement supérieur recherche

Normandie Université

Cti Commission des titres d'ingénieur

cdefi Conférence des Directeurs des Écoles Françaises d'Ingénieurs

European Accreditation of Engineering Programmes EUR-ACE®

CONFÉRENCE DES GRANDES ÉCOLES