

Compte Rendu 2 Projet : Détection de zones copiées-déplacées dans des images



Année Universitaire 2022-2023

Table des matières

Ι	Enjeux et types de falsifications	2
II	Méthodes classique	2
II	Convolutional Neural Network	2
ΙV	Dataset	3

I Enjeux et types de falsifications

Avec l'explosion d'internet et des réseaux sociaux, la transmission d'informations, que ce soit textes, images, vidéos, ... se fait de plus en plus rapidement et facilement. Mais cet avantage peut devenir un inconvénient lorsque ces informations sont volontairement ou involontairement faussées. Il est donc nécessaire de mesurer le plus précisément possible la fiabilité d'une information et, dans ce projet, la véracité d'une image.

Nous avons pu trouver 3 différents types de falsification :

- Copier-déplacer (Copy Move Forgery) qui consiste à copier une zone de l'image qui sera ensuite collé ailleurs dans la même image
- Copier-créer (Splicing Forgery) qui consiste à copier une zone d'une première image qui sera ensuite collé dans une seconde image
- Imitation (Imitation Forgery) qui consiste à modifier un texte en imitant la typographie du texte existant (surtout utilisé pour la falsification de documents numériques)

II Méthodes classique

Pour ce projet, nous nous intéressons au type copier-déplacer. Nous avons trouver deux méthodes pour détecter ce type de falsification :

- Méthode par points d'intérêt : cette méthode consiste, dans un premier temps, à extraire les points clés (points d'intérêts) de l'image en utilisant des méthodes connues, comme l'algorithme SIFT (Scale Invariant Feature Transform) ou le détecteur de Harris. Chaque point d'intérêt est ensuite associé à un vecteur. Lorsque cela est fait, nous mettons en correspondance des points d'intérêts. Si nous trouvons un pattern similaire, alors l'image est falsifiée.
- Méthode par la compression JPEG : lors de la compression JPEG, l'image subit une quantification. Cette étape induit une grande perte d'information. Ces informations perdues lors de la quantification ne peuvent pas être reconstituées et cela amène à l'apparition de discontinuités au bord des blocs de l'image décompressée.

III Convolutional Neural Network

En parallèle, nous pouvons développer un modèle de Deep Learning (nous voulons que ce soit le modèle qui repère les caractéristiques qui montre qu'une image est falsifiée) capable de classer les images en deux groupes d'images, les images falsifiées et les images non falsifiées. Nous utilisons donc une classification binaire (falsifiée ou non, ce qui implique que l'output layer de notre réseau de neurone aura un seul neurone).

Nous aurons ensuite plusieurs hidden layers ainsi que plusieurs neurones par hidden layer (paramètres qui changeront durant le développement pour avoir un modèle plus fiable).

Avant de passer nos images à l'input layer, nous allons lui appliquer une suite de convolutions 2D et max/average pooling afin de réduire sa taille tout en gardant la spatialité de l'image. Une fois cette suite de convolution/pooling terminée, nous allons aplanir l'image et la donner à notre modèle.

Pour entraîner notre modèle, nous avons trouvé un dataset d'images de même tailles. Ce dataset contient 200 sets. Chaque set contient une image originale, une image falsifiée de type copié-déplacé ainsi que des variantes de ces deux images (image plus sombre, image plus clair, ...). Ces images seront labellisée (apprentissage supervisé). Nous allons séparer ces 200 sets en deux parties, un jeu d'apprentissage et un jeu de test (70-80% pour apprendre et 20-30% pour tester). Cette séparation sera fait plusieurs fois (K-Folds). A chaque fois, nous calculerons l'accuracy du modèle sur le jeu de test ainsi que la loss (écart entre le résultat fourni et le résultat attendu).

IV Dataset

Le dataset étant de 3 Go (.rar), il n'a pas pu être push sur notre Github, à la place il a été mis sur Google Drive. Voici le lien: https://drive.google.com/file/d/10FXiriO_XNcZBNdxLUTXqHam-ZMP5akt/view?usp=share_link

Ce dataset nous permettra d'entraîner/tester notre modèle et nous pourrons piocher dans ces images pour tester l'implémentation des méthodes classique. Ce dataset serait donc commun aux deux parties de ce projet. Pour comparer les performances entre méthodes classiques et deep learning, nous pourrions extraire du dataset certaines images. Ainsi ces images ne serait pas utilisées pour l'apprentissage de notre modèle et la comparaison des résultats ne seraient donc pas biaisé (on nous pourrions simplement trouver un autre dataset ne contenant pas les mêmes images).