

# Signature d'Images

Reconstruction de l'historique d'une image digitale par les signatures de ses traitements, détection automatique d'anomalies

---

Jean-Michel Morel

Quentin Bammeys, Miguel Colom, Thibaud Ehret, Rafael Grompone von Gioi, Tina Nikoukhah

May 15, 2019



# Les images falsifiées sont omniprésentes



**Figure 1:** Emma Gonzalez déchirant la constitution américaine.

## Les images falsifiées sont omniprésentes



**Figure 2:** Alexandre Benalla, aperçu prenant un selfie avec un pistolet, prétend que l'image est falsifiée.

# Les images falsifiées sont omniprésentes

## D

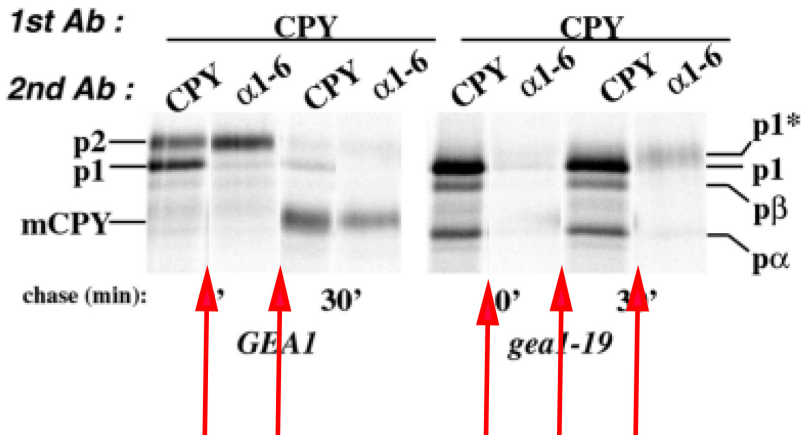


Figure 3: Fraude scientifique

# Quelle valeur donner aux images?



## Quelle valeur donner aux images?

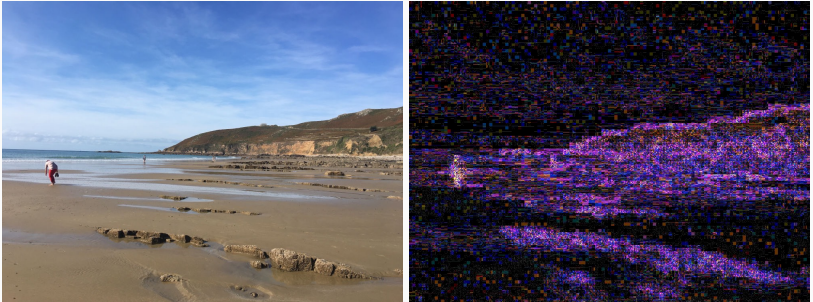
- Facile de modifier une image, d'en changer le contenu sémantique tout en la laissant visuellement plausible
- Difficile de détecter les changements

## Méthodes existantes : soumises à interprétation...



**Figure 4:** Cette image est falsifiée...

## Méthodes existantes : soumises à interprétation...



**Figure 4:** Mais celle-ci, authentique, semble pourtant suspecte.



## Méthodes existantes : soumises à interprétation...



**Figure 5:** Non, la jupe de droite n'a pas été retouchée!

## ...ou entièrement obscures!

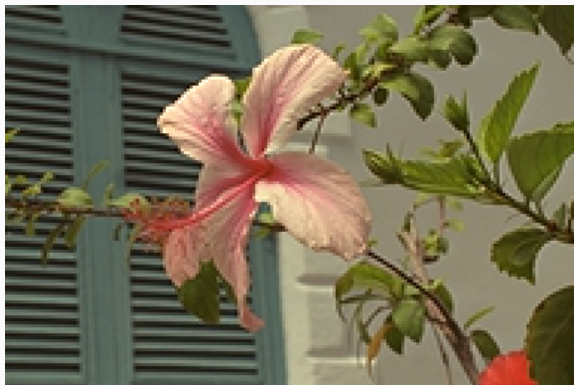
- De plus en plus de méthodes à base de réseaux de neurones convolutionnels voient le jour.
- Ces méthodes sont assez performantes...
- mais leurs détections sont obscures : impossible de justifier la décision.
- elles sont aussi biaisées à l'entraînement.

# Objectifs du projet

- Reconstruire l'historique d'une image
  - Chaîne de construction de l'image : bruit de l'appareil photo, démosaiçage, compression JPEG...
  - Modifications de l'image : Changement de contraste et de couleurs, zones de l'image où le bruit est identique (traces de copier-coller)
- Fournir des preuves tangibles d'une détection :
  - Savoir quels éléments permettent de mener à la conclusion, sans nécessité d'interprétation
  - Maîtriser le nombre de fausses alarmes
- Intérêt multiple :
  - Utilisation légale : on peut être certain d'une détection
  - Traitement automatique de donnée : limiter la nécessité de vérifier manuellement les détections
  - Médias : Résultats fiables et interprétables sans expertise

## Un exemple : démosaiçage

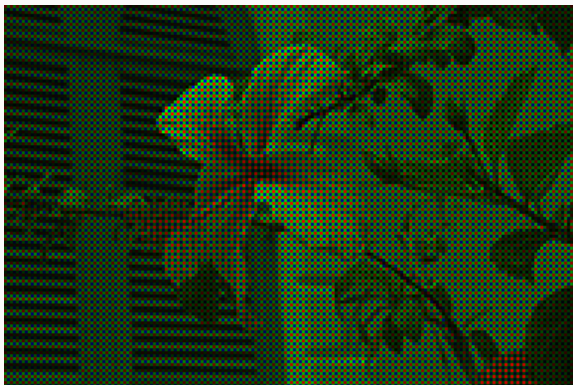
La plupart des appareils photographiques ne captent qu'un seul canal couleur par pixel



**Figure 6:** L'appareil photo ne voit pas cela...

## Un exemple : démosaiçage

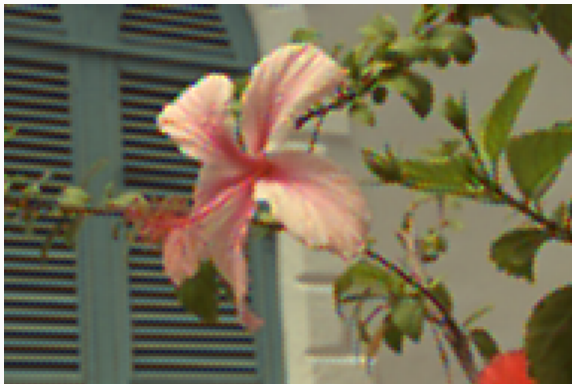
La plupart des appareils photographiques ne captent qu'un seul canal couleur par pixel



**Figure 6:** ...mais cela !

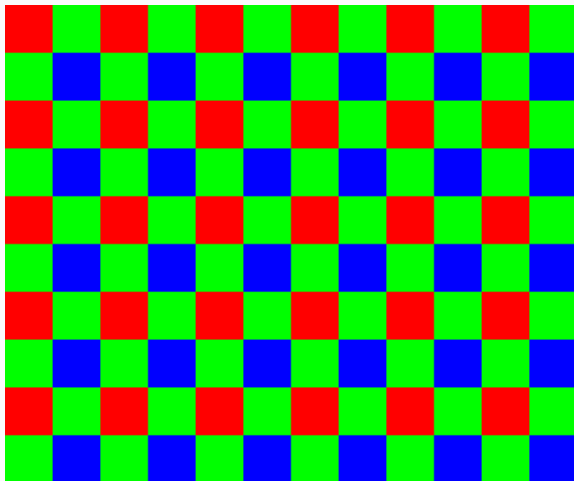
## Un exemple : démosaiçage

La plupart des appareils photographiques ne captent qu'un seul canal couleur par pixel



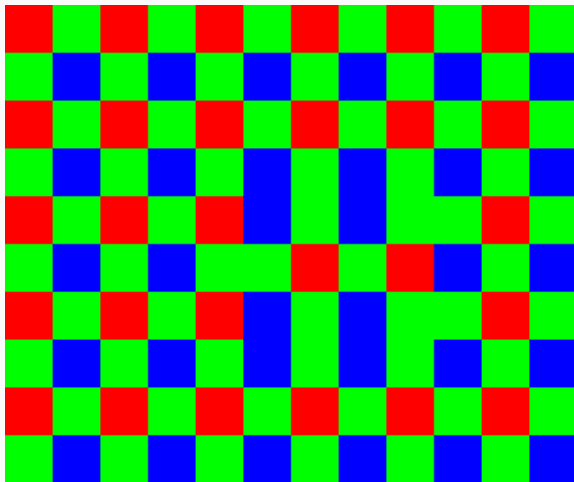
**Figure 6:** Différents algorithmes permettent d'interpoler les pixels manquants

## Un exemple : démosaiçage



**Figure 7:** Pixels originaux sur une image authentique

## Un exemple : démosaiçage



**Figure 7:** Quand on colle une partie d'image sur une autre, 3 chances sur 4 que les grilles ne soient pas cohérentes!



## Beaucoup de scénarios différents

- Copier-coller interne ou externe
- Gommage
- Assemblage de plusieurs images
- Changement de contraste et de couleurs
- Images souvent rééchantillonnées et/ou comprimées

Il faut donc une variété d'algorithmes de détection !

- Contrôler le nombre de fausses alarmes
- Idée : associer à chaque détection un seuil de détection dans le bruit
- Pour chaque détection, on sait donc la probabilité d'avoir un résultat aussi significatif en l'absence de falsification à trouver.
- Autrement dit, on peut fixer le seuil de détection en fonction du nombre de fausses alarmes (images authentiques détectées comme falsifiées)

## Conclusion

- Important beaucoup de domaines : médias, édition scientifique, juridique, ...
- Possibilité d'avoir des détections fiables et compréhensible sans expertise, en limitant le nombre de fausses alarmes
- Pas besoin d'interprétation technique
- Il reste cependant à interpréter les résultats sémantiquement : certaines manipulations peuvent être innocentes mais aussi masquer de l'information (changement de contraste, recadrage, rééchantillonnage, etc)
- Recherche reproductible : démos sur **[www.ipol.im](http://www.ipol.im)**