

Signatures d'images

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



Challenge DEFALS

Édition 2016

Contact :

Quentin Bammeey
Miguel Colom
Thibaud Ehret
Rafael Grompone
Tina Nikoukhah



COORDINATEUR : Jean-Michel Morel

PARTENAIRE : Denis Perraud DGPN-DCPJ-PTS

L'historique d'une image permet de vérifier son authenticité. Pouvoir l'estimer directement depuis l'image permet de s'abstraire d'un historique «humain» souvent inutilisable (incomplet, incertain). C'est pour cela que nous proposons une batterie de détecteurs, entièrement automatiques, pour reconstituer l'historique et détecter les anomalies en contrôlant le nombre de fausses alarmes (NFA).

CONTEXTE

Le public étant sensible à l'information visuelle, la **désinformation** prend souvent la forme d'images falsifiées. Falsifier et diffuser une image est de plus en plus facile, grâce aux nombreux **logiciels de retouche** et à **Internet**.

Les détecteurs actuels fonctionnent comme des révélateurs visuels mais ne fournissent pas de critère de décision absolue.

OBJECTIFS

Mettre au point des algorithmes de détection d'anomalies qui lèvent tout doute en associant à chaque révélateur un nombre de fausses alarmes (1).

Ceci permettra de combiner tous les détecteurs pour arriver à un diagnostic sûr.

Mettre **en ligne** un outil permettant au grand public de soumettre une image douteuse et d'obtenir un **rapport scientifique automatique** sur les anomalies détectées.

MÉTHODOLOGIE

La **falsification laisse des traces** malgré le camouflage. Pour détecter une falsification il faut donc d'une part **reconstruire le modèle de constitution de l'image** fabriquée par le faussaire, et **détecter toute anomalie** de ce prétendu modèle.

- ✓ Maîtriser l'ensemble de la chaîne de traitement : débruitage, rehaussement de contraste, compression, etc.
- ✓ Connaître les différentes méthodes de retouche : *Poisson editing, inpainting, etc.*
- ✓ Détecter de manière **automatique** les traces laissées après modification
- ✓ Associer à chaque détection une **probabilité de confiance** ou un **nombre de fausses alarmes**
- ✓ Implémenter des algorithmes exécutables en temps réel

(1) A. Desolneux, L. Moisan, and J. M. Morel, "From Gestalt Theory to Image Analysis". Springer, 2008.

VALORISATIONS ET PERSPECTIVES

• Les détecteurs en ligne

(2) T. NIKOUKHAH, R. GROMPONE VON GIOI, M. COLOM AND J-M. MOREL, "Automatic **JPEG Grid Detection** with Controlled False Alarms, and Its Image Forensic Applications," *2018 IEEE Conference on Multimedia Information Processing and Retrieval*, Miami, FL, 2018, pp. 378-383.



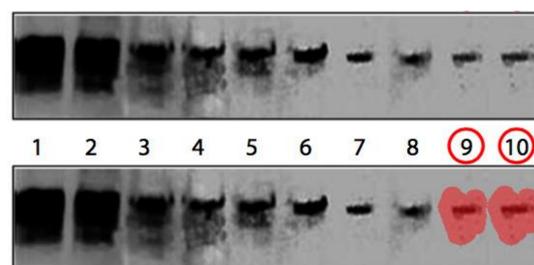
(3) Q. BAMMEY, R. GROMPONE VON GIOI, J-M. MOREL, "Automatic **Detection of Demosaicing** Image Artifacts and Its Use in Tampering Detection," *2018 IEEE Conference on Multimedia Information Processing and Retrieval*, Miami, FL, 2018, pp. 424-429.



(4) T. EHRET, "Automatic **Detection of Internal Copy-Move** Forgeries in Images", *Image Processing On Line*, 8 (2018), pp. 167-191. (<http://www.ipol.im/pub/art/2018/213/>)



• La méconduite scientifique



Exemple par E. Bik, A. Casadevall, F. Fang (2016).

Résultat de la détection par (4)

• Les photomontages dans les «infix»

«Non, Emma Gonzalez n'a pas déchiré la Constitution Américaine».



Image **falsifiée** partagée sur les réseaux sociaux

Résultat de la détection par (2)

Image originale **non falsifiée**

école normale supérieure paris-saclay



16/17 OCTOBRE 2018



ESPACE OUEST LYONNAIS - LYON