Détection automatique de la falsification d'images

M. Gardella[1], **T. Nikoukhah**[1], **Q. Bammey**[1], M. Colom[1], R. Grompone[1], J-M. Morel[1], P. Musé[2], D. Teyssou[3].
[1] *Centre Borelli, ENS Paris-Saclay, CNRS, Université Paris-Saclay, France,*
[2] *IIE, Facultad de Ingeniería, Universidad de la República, Uruguay,*
[3] *Medialab, Agence France-Presse, France.*

Email : {marina.gardella, tina.nikoukhah, quentin.bammey}@ens-paris-saclay.fr

Mots Clés : Falsification d'images, modèle de formation d'images, détection *a contrario*, preuve forensique, géométrie stochastique

Biographie – Marina Gardella, Tina Nikoukhah et Quentin Bammey sont doctorants au Centre Borelli. Dans leurs thèses, ils se concentrent sur la détection de falsifications dans les images, à travers les analyses du bruit (Marina Gardella), du démosaïquage (Quentin Bammey) et de la compression JPEG (Tina Nikoukhah). Ces algorithmes sont utilisés par l'Agence France-Presse et le Service de la Police Nationale Technique et Scientifique.

Resumé :

L'expansion de la photographie numérique a fortement impacté le secteur de l'information et de la communication. La reproductibilité de l'image numérique, ses transformations et sa diffusion massive, ont exacerbé le problème de son éventuelle altération. Dès sa formation et son stockage à partir d'un capteur électronique, l'image brute subit une série d'opérations : débruitage, démosaïquage, balance des blancs, corrections, compression. Dans l'image ainsi produite, ces opérations laissent des traces, imperceptibles à l'œil nu mais néanmoins souvent statistiquement significatives et donc détectables.

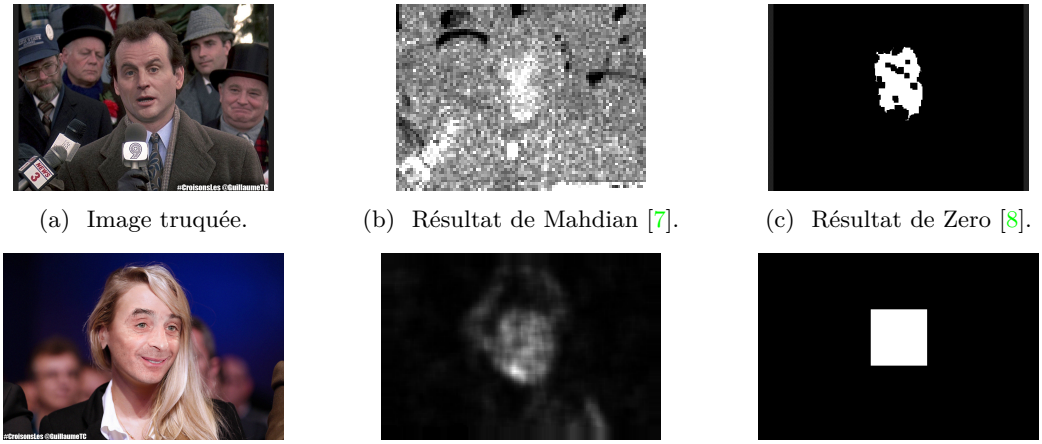
Aux opérations « classiques » de la formation de l'image peuvent s'ajouter des retouches locales, appelées falsifications, qui causent des perturbations dans le modèle de formation de l'image. Ces photographies numériques sont de plus en plus utilisées sur les réseaux sociaux pour créer et diffuser de fausses informations. Ainsi, pour détecter efficacement une falsification, nous tentons de reconstruire la chaîne de traitement d'une image, puis nous cherchons à détecter les anomalies dans ce modèle, autrement dit, de trouver les parties de l'image qui n'ont pas été traitées de la même manière que le reste.

L'état de l'art de la détection de falsifications s'appuie sur ces considérations pour proposer des révélateurs numériques, à savoir des opérateurs capables de mettre en évidence les zones semblant avoir été falsifiées [5]. Un examen de ces méthodes montre néanmoins qu'elles souffrent de lacunes dans l'évaluation de la confiance qui peut être attribuées à leurs détections. En l'absence d'une modélisation probabiliste et statistique, il n'est pas possible de quantifier la sûreté des détections.

À travers nos algorithmes [1, 6, 8], nous visons à recréer un historique complet des images analysées. Nous accompagnons les incohérences détectées dans l'image d'une validation statistique basée sur les méthodes de détection *a contrario*, utilisant des arguments de grande déviation [4]. Ce procédé nous permet de définir nos détections à travers la probabilité que de tels évènements se produisent par hasard, afin d'éviter les faux positifs non significatifs. Ainsi, nos outils proposent une analyse automatique des images, et ne nécessitent ni interprétation, ni donc expertise dans le domaine.

La figure 1 montre des images truquées publiées sur les réseaux sociauxainsi que les résultats de détection des algorithmes de l'état de l'art (1b et 1e) et la détection faite par nos algorithmes (1c et 1f).

Les algorithmes développés sont publiés et mis à disposition en ligne afin de pouvoir être utilisés par le plus grand nombre, en particulier par les journalistes de fact-checking. Lors du projet EnVisu4, financé par l'International Fact-Checking Network (IFCN), ils ont été intégrés dans le plugin de



(a) Image truquée. (b) Résultat de Mahdian [7]. (c) Résultat de Zero [8].

(d) Image truquée. (e) Résultat de Noiseprint [3]. (f) Résultat de Noisesniffer [6].

FIGURE 1 – Les algorithmes Mahdian [7], Zero [8], Noiseprint [3] et Noisesniffer [6] appliqués à des photomontages satiriques (#CroisonsLes par @GuillaumeTC). Si Mahdian [7] et Noiserprint [3] détectent bien les falsifications. L'absence de seuillage automatique impliquerait la nécessité d'une interprétation et expertise humaines. Nos méthodes permettent de l'éviter.

vérification InVID-WeVerify développé par le Medialab de l'Agence France Presse. Les méthodes développées jusqu'ici permettent d'établir des informations concernant l'historique d'une image, puis de déterminer dans certains cas si elle a été falsifiée. Afin de faire de la recherche reproductible, les publications scientifiques sont accompagnées de leur code source et d'une démonstration en ligne [1] via la plateforme IPOL (*Image Processing On Line*, ipol.im).

Références

[1] Quentin BAMMEY, Rafael Grompone von GIOI et Jean-Michel MOREL. « An Adaptive Neural Network for Unsupervised Mosaic Consistency Analysis in Image Forensics ». In : *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. Juin 2020.

[2] Chang-Hee CHOI, Jung-Ho CHOI et Heung-Kyu LEE. « CFA Pattern Identification of Digital Cameras Using Intermediate Value Counting ». In : *Proceedings of the Thirteenth ACM Multimedia Workshop on Multimedia and Security*. 2011, p. 21-26.

[3] Davide COZZOLINO et Luisa VERDOLIVA. « Noiseprint : A CNN-Based Camera Model Fingerprint ». In : *IEEE Transactions on Information Forensics and Security* 15 (2020), p. 144-159. DOI : 10.1109/TIFS.2019.2916364.

[4] Agnès DESOLNEUX, Lionel MOISAN et Jean-Michel MOREL. *From Gestalt Theory to Image Analysis*. Springer, 2008.

[5] Hany FARID. « Digital doctoring : How to tell the real from the fake ». In : *Significance* 3 (nov. 2006), p. 162-166.

[6] Marina GARDELLA et al. « Noisesniffer : a Fully Automatic Image Forgery Detector Based on Noise Analysis ». In : *Proceedings of the 9th IEEE International Workshop on Biometrics and Forensics (forthcoming)*.

[7] B. MAHDIAN et S. SAIC. « Using noise inconsistencies for blind image forensics ». In : *Image and Vision Computing* 27 (sept. 2009), p. 1497-1503.

[8] Tina NIKOUKHAH et al. « JPEG grid detection based on the number of DCT zeros and its application to automatic and localized forgery detection ». In : *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*. 2019, p. 110-118.

1. démonstrations en ligne de l'algorithme Zero, et d'une méthode de détection de démosaïquage que nous avons améliorée [2]