Technologie

Comment déterminer l'origine d'une photo numérique ?

LE CONTEXTE

L'origine de la photo piratée de l'énoncé d'un exercice de maths du bac S, publiée sur Internet, a pu être pistée grâce aux données informatiques contenues dans son fichier. Par ailleurs, le montage du cliché de Ben Laden mort a pu être prouvé. Comment est-ce possible ?

La photo de l'exercice de probabilités de l'épreuve de mathématique du bac S a été publiée le 20 juin 2011, à 21 h 18, sur un forum du site JeuxVideo.com. Mais les données Exif (Exchangeable Image File Format) en disaient plus : elle avait été prise le 11 juin à 18 h 17 avec un smartphone Blackberry 8520. De quoi orienter avec succès les enquêteurs vers ses auteurs potentiels… Ces données sont générées automatiquement lors de la création d'un fichier au format JPG ou TIFF. Elles sont accessibles dans les systèmes d'exploitation Windows ou Mac OS X *via* une simple consultation des informations du fichier. Tout y est : date et heure de la prise de vue, utilisation ou non du flash, dimensions de l'image, marque et modèle de l'appareil… Ces informations ne sont jamais modifiées, même si la photo est ensuite retouchée. Certains logiciels permettent cependant de les « copier-coller » dans un autre fichier pour brouiller les pistes. C'est donc un indicateur précieux, mais pas infaillible.

Outre l'origine d'une photo, on peut tenter de savoir si elle a été « truquée ». Ainsi, en mai, une photo du visage tuméfié du leader d'Al-Qaida, Oussama Ben Laden, a circulé juste après sa mort. Or, l'Agence France Presse ne l'a pas diffusée : elle l'a d'abord analysée avec un logiciel de vérification d'authenticité, Tungstène, créé par la start-up française eXo Makina et déjà utilisé par certains services de l'Etat. *« Le logiciel n'analyse pas l'aspect visuel de la photographie mais ses données informatiques et mathématiques. On détecte s'il y a eu destruction dans la structure du fichier »*, explique son fondateur, Roger Cozien, docteur en informatique et sciences physiques. Pour ce faire, Tungstène utilise trois catégories de filtres. Les filtres « archéorithmiques » scrutent l'histoire algorithmique du fichier pour dire combien de fois il a été trafiqué et retrouver la signature logicielle du premier appareil photo utilisé. *« Pour la photo du visage de Ben Laden, on a pu mettre en évidence qu'il y avait deux signatures de capteurs photographiques »*, note Roger Cozien. Les filtres algébriques étudient la structure mathématique de l'image, et une troisième série de filtres analyse la manière dont le – ou les – appareils ont capté la lumière (angle, diffusion) pour déceler d'éventuelles incohérences. C'est ainsi que la fameuse photo s'est révélée être un montage. Tout comme celle de la « *situation room* » (la chambre de commandement) prise à la Maison-Blanche, à Washington, où l'on voit le président des Etats-Unis et son équipe assister en direct à l'opération menée au Pakistan. La lumière a été postérieurement intensifiée sur certaines zones, atténuée sur d'autres, pour renforcer la gravité du moment. Mais traquer la manipulation, cela peut être aussi… prouver l'authenticité ! Ainsi, toujours avec Tungstène, l'AFP s'est-elle assurée que la photo d'un conseiller régional du Front national faisant le salut nazi n'était pas un montage, contrairement à ce que clamait l'élu. Par ailleurs, eXo Makina est en train de constituer une base de signatures d'appareils photo (smartphones inclus) qui sera accessible en ligne dans le cadre d'un service payant.

La « photo » d'Oussama Ben Laden est en réalité un photomontage réalisé à partir d'une image provenant du film « Black Hawk Down », de Ridley Scott. Un logiciel utilisé par l'AFP a permis d'identifier le trucage.

DR

Ce type de logiciel reste rare, alors que l'hégémonie du numérique facilite les trucages. Y compris, et très souvent, en utilisant des captures d'images issues de DVD, les *« grab video »* : il devient facile de mettre un film sur « pause » sans altérer l'image pour la copier *via* un logiciel avant de l'utiliser dans un montage. Aucune parade n'existe. *« Rien n'est prévu dans le logiciel de retouches Photoshop, l'un des plus utilisés au monde, même si son éditeur Adobe annonce depuis quatre ans des outils de détection*, note Antonin Thuillier, rédacteur en chef technique photo à l'Agence France Presse. *Tungstène, quant à lui, est lent, compliqué à utiliser. Nous n'y avons recours que lorsque nous avons un doute. »*

Reste la recherche. Chercheuse en ingénierie informatique à l'université de Binghamton, aux Etats-Unis, Jessica Fridrich travaille à la mise au point d'un algorithme capable de détecter mathématiquement le « copier-coller » d'un élément au sein d'une même image. Elle a aussi publié des travaux sur la sécurisation des appareils photo. L'idée ? A partir d'un cliché, connaître… le nom du photographe en intégrant la biométrie de l'iris de son œil. **Arnaud Devillard**