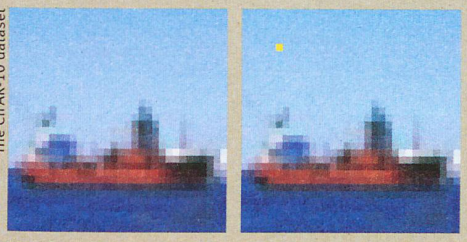
**Zeitschrift:** Horizons : le magazine suisse de la recherche scientifique
**Herausgeber:** Fonds National Suisse de la Recherche Scientifique
**Band:** 31 [i.e. 30] (2018)
**Heft:** 119: La métamorphose de la Big science : comment les mégaprojets de recherche se sont ouverts à d'autres disciplines

**Artikel:** Un seul pixel trompe l'intelligence artificielle
**Autor:** Schlegel, Anna Julia
**DOI:** https://doi.org/10.5169/seals-821649



The CIFAR-10 dataset

**Un pixel bleu devient jaune, et le bateau se transforme en chien.**

## Un seul pixel trompe l'intelligence artificielle

Un algorithme de reconnaissance visuelle a besoin de très nombreuses données pour apprendre à identifier des images. Des chercheurs ont inventé une nouvelle méthode visant à fausser cet apprentissage: ils fixent à zéro la valeur de la composante bleue d'un pixel choisi au hasard dans les images, une intervention discrète selon les couleurs environnantes.

Cette modification a été appliquée dans deux catégories spécifiques - chiens et bateaux - du jeu de données CIFAR-10. Ils ont retouché toutes les photos de chiens utilisées pour l'entraînement de l'algorithme; quant aux bateaux, il s'agissait des images devant être identifiées dans une seconde étape. Résultat: l'algorithme apprend qu'une photo de chien doit nécessairement contenir un pixel modifié et n'est donc plus capable de les reconnaître sur des images non modifiées. De plus, il classe dans la catégorie «chien» les photos de bateaux contenant le pixel transformé.

La méthode a été testée avec succès sur six réseaux de neurones: cinq algorithmes ont classé plus de 70% des bateaux dans la catégorie des chiens et ont correctement identifié moins de 1% des chiens. «Jusqu'à présent, la recherche s'était concentrée sur d'autres types d'attaques visant des algorithmes particuliers, explique Michele Alberti de l'Université de Fribourg. Mais cela exige d'avoir accès au réseau de neurones. Nous avons montré qu'on peut aussi y parvenir par le biais des données d'entraînement.»

L'attaque peut heureusement être facilement parée en utilisant des filtres capables de découvrir et corriger cette manipulation dans les données d'entraînement. «Nous voulions montrer que de telles attaques sont possibles. Les jeux de données publics disponibles sur Internet sont gratuits. Les utiliser sans les tester peut s'avérer problématique.» *Anna Julia Schlegel*

—

M. Alberti et al.: Are You Tampering With My Data? European Conference on Computer Vision (2018)

## Ce qui fait brûler les boues d'épuration

La Suisse produit chaque année 200 000 tonnes de boues d'épuration, les déchets potentiellement toxiques générés par les stations de traitement des eaux usées. Depuis 2006, la Confédération interdit de les utiliser comme engrais agricoles. Elles finissent donc normalement incinérées. Pour cela, elles sont d'abord préparées: on extrait notamment le méthane pour produire de l'énergie, avant de les sécher.

Jusqu'à présent, on savait peu de choses sur les processus en jeu lors de l'incinération. Une étude menée par Jonas Wielinski, un doctorant de l'équipe de Ralf Kaegi à l'institut fédéral de recherche sur l'eau Eawag, vient d'y remédier. Elle montre que l'incinération peut être décrite à l'aide de dix réactions chimiques.

Les scientifiques ont mené une analyse thermogravimétrique et soumis des échantillons de boues à diverses températures dans des atmosphères différentes en utilisant un appareil fonctionnant tel une balance très précise dans un four. Un algorithme a permis de déterminer les réactions de combustion qui se déroulaient en parallèle. L'équipe a notamment déterminé les paramètres d'Arrhenius, qui décrivent les variations de la vitesse des réactions chimiques en fonction de la température. Elle a aussi présenté une méthode permettant de déterminer les liaisons de référence.

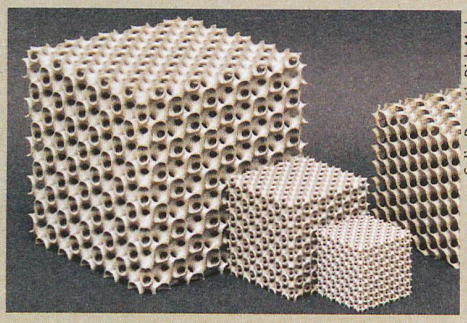
L'étude indique que c'est avant tout la cellulose et la lignine qui brûlent dans les boues: elles sont responsables de 55% de la perte de masse observée lors de la combustion. La cellulose provient principalement du papier toilette, l'un des déchets organiques les plus présents dans nos eaux usées. Les scientifiques ont également identifié d'autres combustibles dans les boues, mais en proportions plus faibles: de l'hémicellulose, du xylane, des alginates et de la calcite. *Anne Careen Stoltz*

—

J. Wielinski et al.: Combustion of Sewage Sludge: Kinetics and Speciation of the Combustible. Energy & Fuels (2018)

Shutterstock/Matteo Fes

**Ce qui brûle dans les boues d'épuration? Du papier de toilette, entre autres.**



Colin Bonatti, Dirk Mohr

**Arrangés de manière régulière, les trous rendent la structure plus résistante.**

## Un métal antichoc imprimé en 3D

L'impression 3D est en plein développement, également pour les métaux. Un laser fusionne de la poudre d'acier, et le fluide est déposé comme dans les procédés conventionnels. C'est ainsi que Dirk Mohr, chercheur à l'ETH Zurich, a conçu un métal en treillis optimisé pour absorber les chocs. Les pleins et les creux sont arrangés de manière répétitive afin de répartir la force des impacts et de réduire les déformations.

Dirk Mohr avait exploré ce sujet pendant ses études, voilà plus de quinze ans. Mais de telles structures tridimensionnelles n'existaient alors que sur le papier: «Il ne s'agissait que d'un pur jeu de l'esprit, irréalisable en pratique. Comme j'ai plutôt une mentalité d'ingénieur, j'avais abandonné ces travaux. Avec l'essor des technologies de manufacture par addition, j'ai pu les ressortir de mes tiroirs.»

Le nouveau matériau rappelle les mousses métalliques, une masse d'acier qui renferme une grande quantité d'air dans de petites chambres. Mais la structure des mousses est plus ou moins aléatoire, car les bulles se forment au hasard par injection de gaz dans le métal en fusion. Au contraire, l'impression 3D permet de contrôler la structure du matériau dans ses moindres détails et d'en maîtriser les propriétés.

Avec son doctorant Colin Bonatti, Dirk Mohr a conçu un matériau isotropique: il résiste de manière égale à la pression et aux impacts dans toutes les directions. Les pores du métal suivent un design en coquille: une structure courbe et complexe, développée sur ordinateur, optimisée pour répartir les impacts et limiter les déformations. Cette approche pourrait servir à concevoir des éléments sur mesure, comme des absorbeurs ultralégers d'énergie mécanique ou des implants biomédicaux, explique le chercheur. «Une production industrielle, par exemple dans l'automobile, devra attendre une baisse des coûts de la manufacture additive métallique.» *Lionel Pousaz*

—

C. Bonatti and D. Mohr: Mechanical Performance of Additively-Manufactured Anisotropic and Isotropic Smooth Shell-Lattice Materials: Simulations & Experiments. Journal of the Mechanics and Physics of Solids (2018)