FUTURA

Trompez la reconnaissance faciale en portant... un pull moche !

Podcast écrit par Sylvain Biget et lu par Alain Mattei

[*Générique d'intro, une musique énergique et vitaminée.*]

Piéger la reconnaissance faciale avec un pull très moche, c'est l'actu insolite de la semaine pour Vitamine Tech.

[*Fin du générique.*]

Souriez, vous êtes filmés ! On les voit partout, elles vous voient partout. La mise en place des caméras de surveillance dans l'espace public ne date pas d'hier. Mais comme aujourd'hui elles se multiplient de façon exponentielle, les yeux et le temps de cerveau manquent pour surveiller et également traiter les images filmées. Résultat : c'est encore une fois l'intelligence artificielle avec la reconnaissance visuelle et faciale qui fait le sale boulot.

[*Une musique électronique calme.*]

En Chine, la reconnaissance faciale fait partie du quotidien ; elle est même associée à un équivalent de permis à points pour compter les bons et mauvais comportements des citoyens sur l'espace public. On ne traverse pas au vert : on perd quelques points. On achète trop de jeux vidéo ou on gaspille de l'argent pour des achats jugés frivoles : c'est mal aussi et on finit par être interdit de voyage. Au final, on trouve une surveillance de masse digne de « Big Brother » abreuvée à la big data. Après tout, l'Empire du Milieu a bien nommé un robot P.-D.G. d'une grosse entreprise, il n'est donc plus à ça près. Compter sur l'IA, c'est rassurant pour un État, pas pour nous. La reconnaissance automatisée, ça ne dort pas, ça répond toujours oui à ce qu'on lui demande et ça ne se trompe jamais. Mais en est-on vraiment sûr ? Car en réalité les exemples de cas où la reconnaissance faciale a été bernée se multiplient proportionnellement au nombre de caméras déployées. On se souvient il y a trois ans des manifestations à Hong-Kong. Pour échapper à l'identification automatisée, les manifestants portaient des masques, se nouaient les cheveux sur le visage ou portaient des peintures de guerre. Il faut dire que sur le territoire, les autorités utilisent la reconnaissance faciale de façon abondante pour terroriser les opposants. En réalité, il est possible de duper ces systèmes de reconnaissance faciale pourtant si prisés sans même porter de masque, car il y a une grosse faille, ou plutôt un bug ! Aux États-Unis, c'est effectivement avec de simples pulls que des chercheurs de l'université du Maryland ont pu tromper l'IA des caméras. Avec ces pulls, impossible pour l'algorithme de savoir si des personnes se trouvent devant elles. C'est efficace, car sur les images on voit bien que les tentatives du système de tracking de l'IA échouent systématiquement dès que le porteur du pull entre en scène. C'est donc discret pour éviter d'être remarqué par une caméra, mais beaucoup moins pour se promener en public. On ne va pas se mentir, le pull est vraiment

très moche. Il a fallu imprimer des motifs qui semblent aléatoires et des couleurs très flashy et qui ne se combinent pas forcément bien entre elles. L'idée des scientifiques était de chercher la vulnérabilité des modèles d'apprentissage automatiques utilisés par l'IA des caméras. Ils se sont alors reposés sur un jeu de données appelé SOCO. C'est exactement sur ce modèle que l'algorithme de vision YOLOV2 s'entraîne. Les chercheurs ont donc reproduit l'exact inverse d'un motif issu des données de SOCO, qui aident l'IA à reconnaître une personne. C'est tout simplement en l'imprimant sur ce pull qu'ils ont dupé la machine. Si ce pull va un peu plus loin que le simple fait de se masquer le visage, c'est parce qu'il bloque le processus de reconnaissance en amont. Avant même de chercher à qui appartient un visage, l'algorithme va commencer par catégoriser le porteur du pull en autre chose qu'un humain. Le robot ne nous imagine donc pas décapité. Autrement dit, sans corps, pas de reconnaissance faciale possible. Comme on parle chiffons, il faut savoir que les créateurs de mode sont également inspirés par le sujet. Certains ont même lancé des collections complètes pour passer incognito devant les caméras de reconnaissance automatique. C'est d'ailleurs ce que proposait dès 2013 la créatrice Simone C. Niquille. Elle s'attaquait alors au système de reconnaissance faciale controversé de Facebook qui était actif à l'époque. Ses t-shirts représentaient les visages déformés de célébrités. Ça tapait dans l'œil du public, mais le système de Facebook était incapable d'identifier le porteur du t-shirt. Cela peut aller plus loin, car même sans ce type de vêtement, il faut peu de choses pour biaiser une IA. En réalité, une mauvaise information peut la perturber et pour une bonne raison. Contrairement à l'humain, elle ne sait pas voir un visage en tant qu'élément abstrait. Dès qu'on lui ajoute quelque chose qu'elle ne connait pas, elle jette l'éponge. Parfois, un simple bijou, un tatouage ou un peu de maquillage peut la déboussoler.

[*Virgule sonore, une cassette que l'on accélère puis rembobine*.]
[*Une musique de hip-hop expérimental calme*.]

Autre exemple récent avec un algorithme spécialisé dans la reconnaissance des objets. Un simple morceau de papier et un stylo peuvent suffire à embrouiller l'IA. C'est en tout cas ce qu'ont voulu prouver les chercheurs du learning lab d'OpenAI. Lorsqu'on lui montre une simple pomme, l'IA d'OpenAI est redoutable. Non contente de reconnaître le fruit, elle en connaît même la variété. Mais là où l'on se rend compte qu'il ne s'agit que d'une machine qui ne sait pas faire preuve de discernement, c'est lorsque l'on colle sur la pomme un bout de papier avec écrit iPad à la main dessus. À partir de ce moment, l'IA va identifier la tablette de la marque à la pomme. C'est assez idiot. Les scientifiques ont même trouvé un nom à cette méthode qui met en avant les grosses failles des IA de reconnaissance automatique. Ils ont appelé cela l'attaque typographique. Vous le voyez, l'Intelligence artificielle n'est pas si maligne que ça... Alors imaginez maintenant les dégâts, si on en vient à lui confier le volant d'une voiture autonome, comme certains l'envisagent très bientôt.

[*Virgule sonore, un grésillement électronique*.]

C'est tout pour cet épisode de Vitamine Tech. Si ce podcast vous plaît, n'hésitez pas à nous retrouver sur vos applications d'écoute préférées pour vous abonner et ne manquer aucun épisode à venir. Grâce à votre fidélité, le podcast s'est installé dans le Top 5 du classement des podcasts d'actu sur les nouvelles technologies sur iTunes. Pour être sûr·e·s de continuer de nous suivre tout au long de l'année, pensez à vous abonner à Vitamine Tech et

à nos autres podcasts. Pour le reste, je vous souhaite à toutes et à tous une excellente soirée ou une très bonne journée et je vous dis à la semaine prochaine, dans Vitamine Tech.

[*Un glitch électronique ferme l'épisode*.]