Nowhere to Hide: Algorithms Are Learning to ID Pixelated Faces

The new tech can identify faces or numbers even if they've been blurred out.

// BY AVERY THOMPSON SEP 13, 2016

YAGI STUDIO / GETTY IMAGES

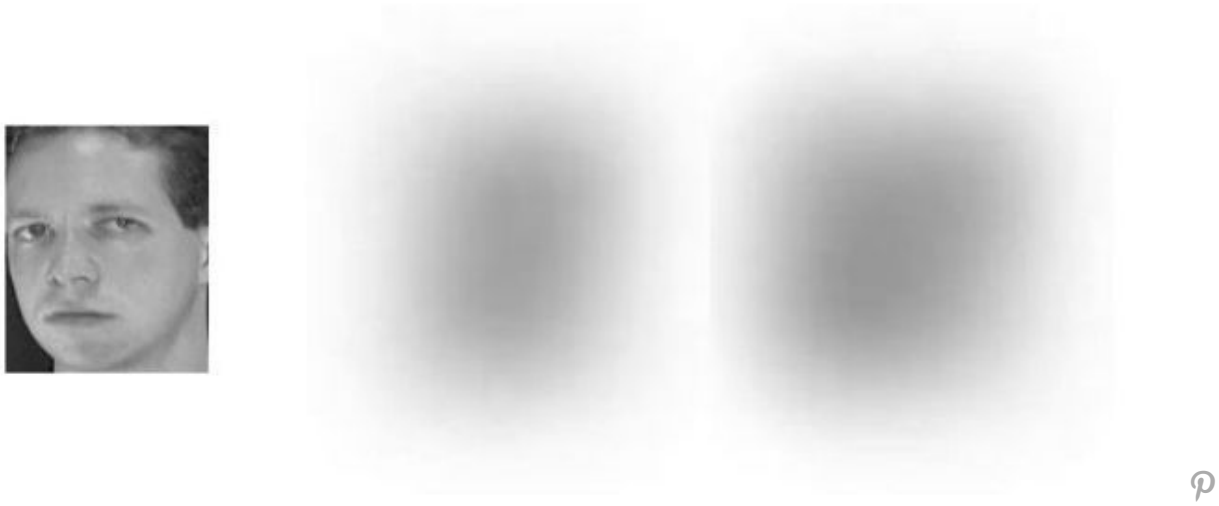
Blurring or pixelating information to obscure it may not work anymore thanks to machine learning researchers from the University of Texas at Austin and Cornell University. The researchers developed an algorithm that could identify faces and numbers even after they were blurred out.

The researchers developed the algorithm using open-source machine-learning software. Said co-author Vitaly Shmatikov to Quartz:

MORE FROM POPULAR MECHANICS
Easy 3M Tape Dispenser

> "We're using this off-the-shelf, poor man's approach. Just take a bunch of training data, throw some neural networks on it, throw standard image recognition algorithms on it, and even with this approach…we can obtain pretty good results."

The algorithm is built using a very simple process. Using the open-source software and standard neural network templates, the researchers could feed the algorithm thousands of examples of faces that have been blurred or pixelated to train it.



Faces, like the one on the left, blurred with YouTube's blur feature, in the center and right, are still recognizable to a machine-learning algorithm.

MCPHERSON ET AL.

The algorithm's success rate varied based on the type of blurring or pixelating used, but in general it could match a blur with the correct face more than half the time, compared with less than a 10 percent success rate for human guessers. This method also works with pixelation and P3 image encryption.

The goal of the research is to illustrate vulnerabilities in standard image encryption. "Until somebody shows how even off-the-shelf technology can be used for privacy breaches, people in security and privacy aren't going to realize it," says Shmatikov.

For instance, YouTube currently provides blurring software for hiding the identities of video subjects, but the researchers would like YouTube to specify that it doesn't work on machines. Anyone with enough time, computing power, and knowhow could easily identify people with blurred faces in YouTube videos.

Source: Quartz

MORE FROM

SECURITY

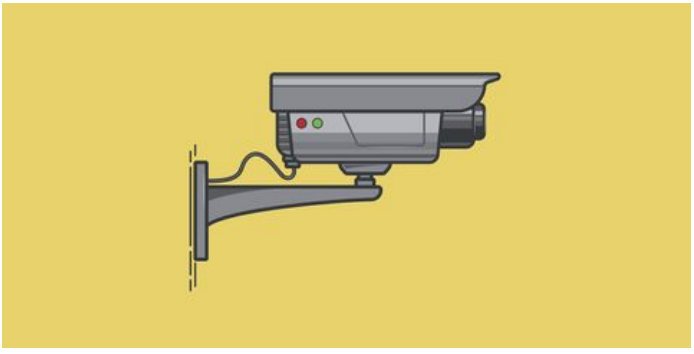
USPS May Be Working On Blockchain-Based Voting

How to Spot Deepfakes

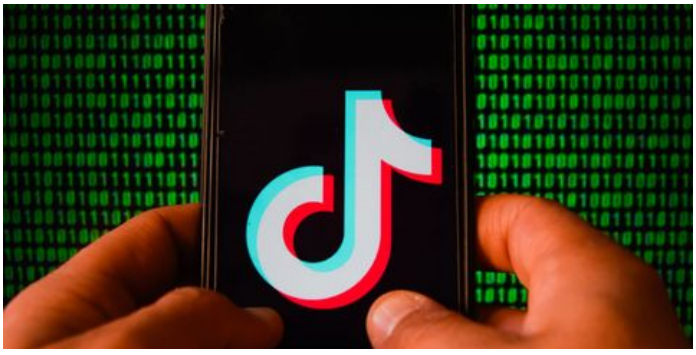
Face Masks Are Thwarting Facial Recognition Tech

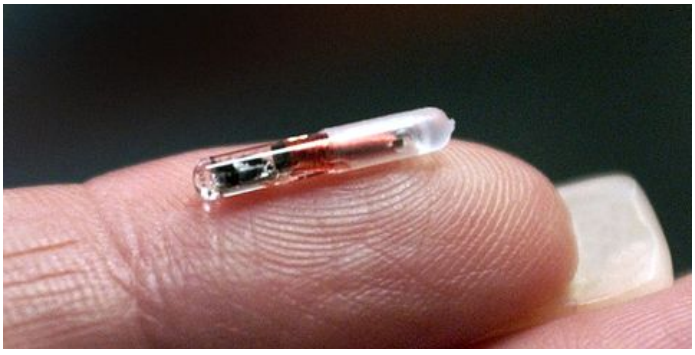
Russian Hackers Are Targeting COVID-19 Researchers

Don’t Close Your MacBook With a Webcam Cover On



Your Security Cameras Could Be Snitching On You





Why the Trump Administration May Ban TikTok

Michigan Wants to Prevent Mandatory Microchipping

Disney Is Getting Into the Deepfake Game

Are You Under Surveillance on Vacation?

SECURITY | NEW TECHNOLOGY | THIS IS HOW ALGORITHMS WILL EVOLVE THEMSELVES

ALGORITHM GUESSES YOUR TRUE AGE BY SCANNING YOUR FACE | AN ALGORITHM BUILT THESE DYSTOPIAN CITYSCAPES

FBI'S NEXT-GEN ID DATABANK TO STORE FACE SCANS—A GOOD IDEA? | HOW TO HIDE UGLY GARBAGE CANS

HOW TO HIDE A TV'S UNSIGHTLY WIRES