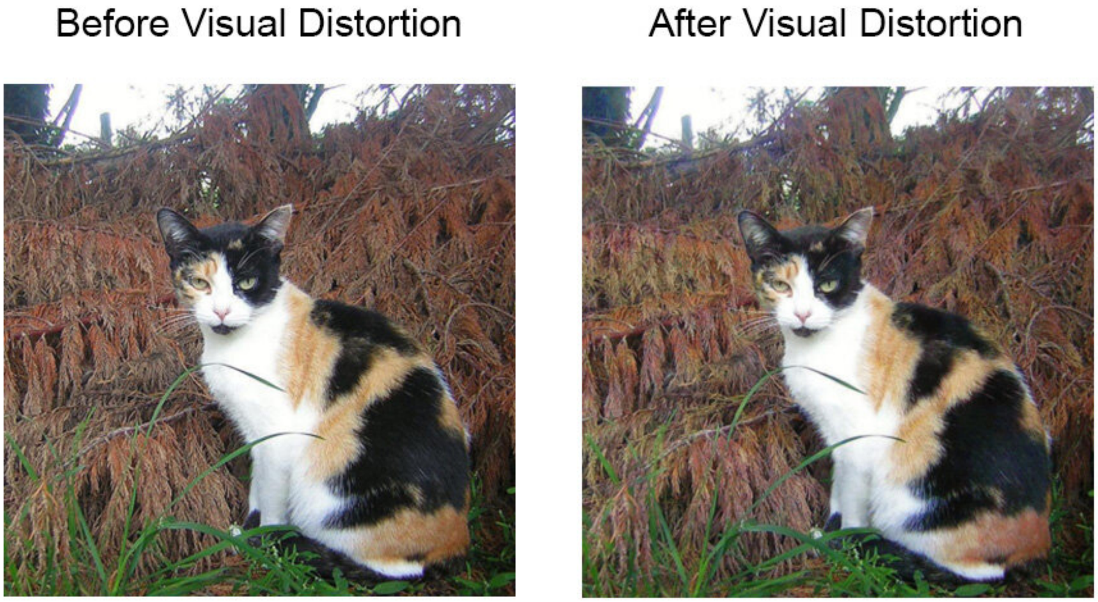
TechXplore

Innovation enhances digital privacy by hiding images from the prying eyes of AI

July 1 2020


Before Visual Distortion

After Visual Distortion

An AI algorithm will identify a cat in the picture on the left but will not detect a cat in the picture on the right. Credit: National University of Singapore

In one second, the human eye can only scan through a few photographs. Computers, on the other hand, are capable of performing billions of calculations in the same amount of time. With the explosion of social media, images have become the new social currency on the Internet.

Today, Facebook and Instagram can automatically tag a user in photos, while Google Photos can group one's photos together via the people present in those photos using Google's own image recognition technology.

Dealing with threats against digital privacy today, therefore, extends beyond just stopping humans from seeing the photos, but also preventing machines from harvesting personal data from images. The frontiers of privacy protection need to be extended now to include machines.

Led by Professor Mohan Kankanhalli, Dean of the School of Computing at the National University of Singapore (NUS), the research team from the School's Department of Computer Science has developed a technique that safeguards sensitive information in photos by making subtle changes that are almost imperceptible to humans but render selected features undetectable by known algorithms.

Visual distortion using currently available technologies will ruin the aesthetics of the photograph as the image needs to be heavily altered to fool the machines. To overcome this limitation, the NUS research team developed a "human sensitivity map" that quantifies how humans react to visual distortion in different parts of an image across a wide variety of scenes.

The development process started with a study involving 234 participants and a set of 860 images. Participants were shown two copies of the same image and they had to pick out the copy that was visually distorted. After analyzing the results, the research team discovered that human sensitivity is influenced by multiple factors. These factors included things like illumination, texture, object sentiment and semantics.

Using this "human sensitivity map" the team fine-tuned their technique to apply visual distortion with minimal disruption to the image aesthetics by injecting them into areas with low human sensitivity.

The NUS team took six months of research to develop this novel technique.

"It is too late to stop people from posting photos on social media in the interest of digital privacy. However, the reliance on AI is something we can target as the threat from human stalkers pales in comparison to the might of machines. Our solution enables the best of both worlds as users can still post their photos online safe from the prying eye of an algorithm." said Prof Kankanhalli.

End users can use this technology to help mask vital attributes on their photos before posting them online and there is also the possibility of social media platforms integrating this into their system by default. This will introduce an additional layer of privacy protection and peace of mind.

The team also plans to extend this technology to videos, which is another prominent type of media frequently shared on social media platforms.

Provided by National University of Singapore

Citation: Innovation enhances digital privacy by hiding images from the prying eyes of AI (2020, July 1) retrieved 6 December 2023 from https://techxplore.com/news/2020-07-digital-privacy-images-prying-eyes.html