New privacy-preserving robotic cameras obscure images beyond human recognition

April 4 2024

What a normal camera sees compared with what the researchers' privacy preserving camera sees. Credit: University of Sydney and Queensland University of Technology

From robotic vacuum cleaners and smart fridges to baby monitors and delivery drones, the smart devices being increasingly welcomed into our homes and workplaces use vision to take in their surroundings, taking videos and images of our lives in the process.

In a bid to restore privacy, researchers at the Australian Centre for

Robotics at the University of Sydney and the Centre for Robotics (QCR) at Queensland University of Technology have created a new approach to designing cameras that process and scramble visual information before it is digitized so that it becomes obscured to the point of anonymity.

Known as sighted systems, devices like smart vacuum cleaners form part of the "internet-of-things"—smart systems that connect to the internet. They can be at risk of being hacked by bad actors or lost through human error, their images and videos at risk of being stolen by third parties, sometimes with malicious intent.

Acting as a "fingerprint," the distorted images can still be used by robots to complete their tasks but do not provide a comprehensive visual representation that compromises privacy.

"Smart devices are changing the way we work and live our lives, but they shouldn't compromise our privacy and become surveillance tools," said Adam Taras, who completed the research as part of his Honors thesis.

"When we think of 'vision' we think of it like a photograph, whereas many of these devices don't require the same type of visual access to a scene as humans do. They have a very narrow scope in terms of what they need to measure to complete a task, using other visual signals, such as color and pattern recognition," he said.

The researchers have been able to segment the processing that normally happens inside a computer within the optics and analog electronics of the camera, which exists beyond the reach of attackers.

"This is the key distinguishing point from prior work which obfuscated the images inside the camera's computer—leaving the images open to attack," said Dr. Don Dansereau, Taras' supervisor at the Australian Centre for Robotics. "We go one level beyond to the electronics

themselves, enabling a greater level of protection."

The researchers tried to hack their approach but were unable to reconstruct the images in any recognizable format. They have opened this task to the research community at large, challenging others to hack their method.

"If these images were to be accessed by a third party, they would not be able to make much of them, and privacy would be preserved," said Taras.

Dr. Dansereau said privacy was increasingly becoming a concern as more devices today come with built-in cameras, and with the possible increase in new technologies in the near future like parcel drones, which travel into residential areas to make deliveries.

"You wouldn't want images taken inside your home by your robot vacuum cleaner leaked on the dark web, nor would you want a delivery drone to map out your backyard. It is too risky to allow services linked to the web to capture and hold onto this information," said Dr. Dansereau.

The approach could also be used to make devices that work in places where privacy and security are a concern, such as warehouses, hospitals, factories, schools and airports.

The researchers hope to next build physical camera prototypes to demonstrate the approach in practice.

"Current robotic vision technology tends to ignore the legitimate privacy concerns of end-users. This is a short-sighted strategy that slows down or even prevents the adoption of robotics in many applications of societal and economic importance. Our new sensor design takes privacy very seriously, and I hope to see it taken up by industry and used in many

applications," said Professor Niko Suenderhauf, Deputy Director of the QCR, who advised on the project.

Professor Peter Corke, Distinguished Professor Emeritus and Adjunct Professor at the QCR who also advised on the project said, "Cameras are the robot equivalent of a person's eyes, invaluable for understanding the world, knowing what is what and where it is. What we don't want is the pictures from those cameras to leave the robot's body, to inadvertently reveal private or intimate details about people or things in the robot's environment."

The research, "Inherently privacy-preserving vision for trustworthy autonomous systems: Needs and solutions," was published by the *Journal of Responsible Technology*.

More information: Adam K. Taras et al, Inherently privacy-preserving vision for trustworthy autonomous systems: Needs and solutions, *Journal of Responsible Technology* (2024). DOI: 10.1016/j.jrt.2024.100079

Provided by University of Sydney