Using camera fingerprints to catch cybercriminals

July 18 2018

Credit: Freshscience

A technique that can match images and video to the device that took them, is being used to investigate cybercrimes.

Developed by Dr. Xufeng Lin and his research team at Charles Sturt University, the method exploits the unique traces—often referred to as the camera's fingerprints—which the hardware and software processing components of a digital camera leave behind in every image or video it takes.

"Like the barrel of a gun will leave unique markings on a bullet that passes through it, which can then be used to match the bullet back to the firearm that fired it, we can find something similar in digital images," says Xufeng.

"For example, manufacturing imperfections in the camera's sensor will leave behind a pattern of noise in an image that is unique to that particular device."

Xufeng's team tested their method on a database of 5,400 images taken by 36 different cameras. They found that if a camera's fingerprint could be reliably estimated they were able to match the images to the correct device 95 per cent of the time or better.

They've also developed an algorithm which is able to go through large databases of images and group together images that were taken by the same camera.

So far, their research has been used to help Sussex Police in the UK link child pornography images to an offender's mobile phone.

They've also worked with Interpol, and used their algorithm to analyse 10 million images in the International Child Sexual Exploitation image database to help identify victims on the internet.

"As camera fingerprint techniques like ours improve and get more sophisticated, I believe that they will play an even greater role in fighting

cybercrime," says Xufeng.

Provided by Freshscience