Electrical engineer cracks code to detect media tampering

April 1 2009

NJIT Professor of Electrical and Computer Engineering Yun-Qing Shi (left) discusses a techical problem with his graduate student. Credit: Guy Chan for NJIT

(PhysOrg.com) -- An NJIT electrical engineer has cracked the code that will enable researchers around the world to detect tampering with electronic images.

"Using our program, we can usually inspect a photograph on a computer screen and know that someone has changed it," said Yun-Qing Shi, a professor of electrical and computer engineering. "We still cannot say, nor can anyone else, where in the media the image has been changed. But we will get there."

Earlier this year, "System and Method of Steganalysis," developed by

Shi and his collaborator Guorong Xuan received a U.S. patent. The research has already been licensed. Since 2003, Shi has received four other patents in this area and awaits news of more than two dozen pending patents. Steganalysis is a method of determining whether data has been hidden in a digital medium.

Image tampering came to the world's attention following changes to two widely-recognized images-- a Los Angeles Times photo of the Iraqi War in 2003 and a BBC News image of the Israeli air strike against Beirut in 2006. Since then, Shi, an expert in information assurance and digital data forensics who lectures worldwide, has made it his business to highlight new and better ways to detect tampering with electronic images.

"In our digital age," said Shi, "digital media has been massively produced, easily manipulated, and swiftly transmitted to almost anywhere in the world at any time. While the great convenience has been appreciated, information assurance has become an urgent and critical issue faced by the digital world."

In many applications, data hiding, cryptography or a combination of both, will not reveal a problem. Rather, the science of digital data forensics, which gathers evidence of data composition, origin, and history, is necessary. Although this research field remains in its infancy, it is attracting increasing attention from the multimedia-security research community.

Shi lectures often about safety features multi-media users should put in place when posting any kind of media on the Internet. A common safety feature is simply being active: This means taking the time to add or hide secret codes in the original image or media. Codes might be as simple as crediting the photographer or adding a publication date and location.

A digital signature also works. "The signature is generated electronically and then one of many available methods can be employed to hide it," Shi said. Such a tact enables the user to verify the authenticity of a photo by extracting the embedded signature, then comparing it to other signatures possibly written over it.

Of course in most circumstances, most people don't have the time nor technical knowledge to embed a signature or sign their medium. How can an expert like Shi know if the image has been touched? "Thanks to our new patents if a user hasn't embedded identifying information, we will still be able to detect a forged image," said Shi. What our research can't yet determine is where the image has been touched. That's why our research is still ongoing."

Source: New Jersey Institute of Technology

Citation: Electrical engineer cracks code to detect media tampering (2009, April 1) retrieved 10 April 2024 from https://phys.org/news/2009-04-electrical-code-media-tampering.html