Android add-on monitors eyewitness mobile media reports

November 3 2011

On-the-ground photos from the next political uprising may come with added authenticity tags.

Duke University computer scientists have developed a new feature, called YouProve, which can be integrated into the Android operating system to monitor images and audio captured with mobile devices.

YouProve tracks changes that individuals make to files in third-party applications by recording edits that significantly alter the meaning of media, such as blurring a face in an image or inserting extra content. It also records changes that preserve the original meaning, such as reducing an image's resolution.

"With the Arab Spring and the Iranian protests in 2009, we relied on citizen journalists for information," said Landon Cox, a computer scientist at Duke who helped develop YouProve. "But as crowd-sourced content plays an increasingly important role in world affairs, falsified media could have severe consequences. It's important that we make sure the information we are getting is accurate."

Cox and Duke students Peter Gilbert, Henry Qin, Kyungmin Lee and DJ Sharkey collaborated with Jaeyeon Jung of Microsoft Research and Anmol Sheth of Technicolor Research to design YouProve.

The team altered the Android operating system so that it keeps copies of images or audio clips that are opened in apps, such as Facebook,

Photoshop Express for Android or Garageband, and then tracks what the app does with the data.

If the app writes a modified version of the media to a file on a phone or over a wireless network, YouProve uses advanced audio and image analysis algorithms to compare the original data to the modified one. The software then produces a non-forgeable "fidelity certificate," summarizing the degree to which various regions of the media are preserved, compared to the original data.

With the user's consent, YouProve posts the fidelity certificate along with the edited media on the Internet. Services such as CNN iReports or Al Jazeera's Sharek and individuals can check a photo's authenticity, for example, by opening the file in YouProve's Photo Analysis Visualizer, which produces a "heat map" showing the degree to which the media has been edited compared to the original.

In tests, YouProve correctly identified edited regions of photos or audio clips with 99 percent accuracy. The software monitored media files for compression, cropping and blurring, and completed its analyses in less than 70 seconds.

The analysis does not interrupt individuals' simultaneous use of other applications on the phone, Cox said. He and his collaborators presented the results on YouProve on Nov. 3 at the Association for Computing Machinery Conference on Embedded Networked Sensor Systems in Seattle.

Cox said YouProve uses emerging tamper-resistant, "trusted" hardware on mobile devices to produce the fidelity certificates. This hardware guarantees that the certificates are generated securely and cannot be fabricated. The hardware is a standard feature on personal computers and new smartphones, though it remains largely unused on both

platforms.

To deploy YouProve on smartphones and other devices, however, manufacturers will need to make their devices' trusted hardware accessible to the emerging software. Cox said he is optimistic this will happen in the near future.

More information: sensys.acm.org/2011/index.html

Provided by Duke University