

System might detect doctored images and videos for the military

August 24 2016, by Emil Venere

Purdue University is leading part of an international effort to develop a system for the military that would detect doctored images and video and determine specifically how they were manipulated.

"This team has some of the most senior and skilled people out there in the field, some of whom helped to create the area of media forensics," said Edward Delp, Purdue's Charles William Harrison Distinguished Professor of Electrical and Computer Engineering.

The project is funded over four years with a \$4.4 million grant from the U.S. Defense Advanced Research Projects Agency (DARPA). The research also involves the University of Notre Dame, New York University, University of Southern California, University of Siena in Italy, Politecnico di Milano in Italy, and University of Campinas, in Brazil.

The Purdue-led technology-development team is one of several teams assigned to different parts of the overall project.

"It's a very ambitious program," said Delp, the team's principal investigator and director of Purdue's Video and Image Processing Laboratory, or VIPER Lab. "We have plenty of work to do in four years. One of the things we are doing is bringing to bear a lot of important tools from signal and [image processing](#), computer vision and machine learning."

A huge volume of images and video of potential intelligence value are uploaded daily to the Internet. However, visual media are easily manipulated using software tools that are readily available to the public.

"Now there is an unfair advantage to the manipulator," Delp said. "It's similar to an arms race in the sense that as better algorithms are able to detect doctored media, people are able to change how they do the manipulation. Many open-source images and videos are of potential use to the [intelligence community](#), but how do you know those images can be trusted?"

The team's co-principal investigators are Walter Scheirer, Kevin W. Bowyer, and Patrick J. Flynn from the University of Notre Dame; Anderson Rocha from the University of Campinas in Brazil; C.C. Jay Kuo from the University of Southern California; Paolo Bestagini and Stefano Tubaro at Politecnico di Milano in Italy; Mauro Barni at the University of Siena in Italy; and Nasir Memon at New York University.

"The diverse, interdisciplinary team of researchers that DARPA has assembled is remarkable," Memon said. "This is truly an all-star team from industry and academia."

The researchers will strive to create an "end-to-end" system capable of handling the massive volume of media uploaded regularly to the Internet.

"A key aspect of this project is its focus on gleaning useful information from massive troves of data by means of data-driven techniques instead of just developing small laboratory solutions for a handful of cases," Scheirer said.

Although "deep learning" has been widely used in computer vision, Kuo and Barni stressed the importance of its application to media forensics.

"Developing techniques that can withstand the attempts of an informed adversary to deceive the forensic analysis is a very challenging task for which no satisfactory solutions have been proposed so far," Barni said.

The system will require specialized machine-learning computers and will be designed to automatically perform processes needed to verify authenticity for millions of videos and images.

"You would like to be able to have a system that will take the images, perform a series of tests to see whether they are authentic and then produce a result," Delp said. "Right now you have little pieces that perform different aspects of this task, but plugging them all together and integrating them into a single system is a real problem."

Bestagini said the techniques to be developed in the research will be available to anyone in the field of media forensics, not solely to the intelligence community. Such a system could have potential commercial applications, representing a tool for news and social media platforms to authenticate images and video before posting them.

"Many tools currently available cannot be used for the tens of millions of images that are out there on the Net," Delp said. "They take too long to run and just don't scale up to this huge volume. I think the biggest challenge is going to be the scalability, to go from a sort of theoretical academic tool to something that can actually be used."

Rocha and Tubaro said the aim is not only to verify whether a particular digital object has been tampered with, but also to learn key aspects related to its digital lineage over time, a field known as "multimedia phylogeny."

Provided by Purdue University

Citation: System might detect doctored images and videos for the military (2016, August 24)
retrieved 19 April 2024 from
<https://phys.org/news/2016-08-doctored-images-videos-military.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.