Notre Dame computer vision experts develop 'questionable observer detector'

October 11 2011

It's become a standard plot device of television detective shows: criminals always return to the scene of the crime. And law enforcement officials believe that perpetrators of certain crimes, mostly notably arson, do indeed have an inclination to witness their handiwork. Also, U.S. military in the Middle East feel that IED bomb makers return to see the results of their work in order to evolve their designs.

Now a team of University of Notre Dame biometrics experts are developing a crime-fighting tool that can help law enforcement officials identify suspicious individuals at crime scenes.

Kevin Bowyer and Patrick Flynn of Notre Dame's Computer Science and Engineering Department have been researching the feasibility of image-based biometrics since 2001, including first-of-their-kind comparisons of face photographs, face thermograms, 3-D face images, iris images, videos of human gait, and even ear and hand shapes.

While attending a meeting in Washington, D.C, Bowyer listened as military and national security experts discussed the need for a tool to help identify IED bombers in the Middle East.

He decided to join forces with Flynn and Jeremiah Barr, a doctoral student in computer science and engineering, to tackle the challenge he heard expressed at the Washington meeting. The researchers developed a "Questionable Observer Detector (QuOD)" to identify individuals who repeatedly appear in video taken of bystanders at crime scenes.

The challenge was especially daunting because the researchers lacked a data base to compare faces against. Also, many times crime scene videos are shot by witnesses using handheld videos and are often of poor quality. Additionally, many criminals try to disguise their appearance in various ways.

In response, the Notre Dame team focused on an automatic facial recognition tool that didn't need to match people against an existing database of known identities. Instead, Bowyer, Flynn and Barr create "face tracks" for all individuals appearing in a video and repeat the process for all available video clips. The face tracks are compared to determine if any faces from different video clips look similar enough to match each other. When the technology spots a match, it adds it to a group of video appearances featuring just that person. In this way, it attempts to cluster together the pieces of different video clips that represent the same person.

An individual is considered suspicious if he or she appears too frequently in the set of videos. The "too many" number is determined by law enforcement officials based on the number of crimes and videos available.

Although the technology shows great promise, Bowyer, Flynn and Barr admit they still have serious technical challenges they are working to overcome. Optimum facial recognition technology requires high quality lighting and video resolution, which is often unavailable at crime scenes. Also, people may not be looking directly at the camera in video of crowds of bystanders. And the identification of a questionable observer becomes more computationally demanding in cases where there a large number of videos to be analyzed.

The researchers are confident, however, that these challenges can be overcome and are continuing to work to improve their system. They are

also confident that civil liberties concerns are minimized and positive social benefit is invovled, given that the tool helps officials identify individuals by their actual presence at multiple crime scenes rather than by suspicion.

Provided by University of Notre Dame