DATA MINING IN VIDEO SURVEILLANCE SYSTEMS: SUSPICIOUS ACTIVITY DETECTION

Mohd Fahadullah

Having loads of information at one's hands only helps if it is possible to sift through it and figure out what can be inferred or learned from it. There are 6 million video cameras mounted in stores across the U.S., according to market researcher J.P. Freeman Co and retailers in U.S. record an estimated 1,000 years of video every day, according to IntelliVid [6]. With such an amount of data available, it is impractical to manually analyze the behavior of all the observed objects in order to quickly and correctly detect unusual patterns. Thus, data mining is getting to play a larger role in automatic video surveillance systems to detect any anomaly in behavior of the subjects. "Rather than have someone watch and review TV for hours on end, retailers are utilizing intelligence behind the video screen," says Joe LaRocca, vice-president for loss prevention at the National Retail Federation trade group [6]. That's why stores are investing in technologies so that they can use video cameras to check out an aisle for any possible suspicious activity and catch the suspects before they get their hands on the job.

One such system called the Video Investigator has been installed by some Macy's, CVS, and Babies 'R' Us stores, whose advanced surveillance software can compare a shopper's movements between video images and recognize unusual activity [6]. Indulge in an activity that is unusual like removing large number of items from a shelf at once or opening a case that's normally kept closed and locked, and the system sends off alerts to the security. These systems can also predict where a shoplifter is likely to hide like at the ends of aisles or behind floor displays etc [6]. "And if someone opens a back door at 2 a.m., the system will record who sneaked in and link it with snapshots of the previous and next persons to use the door. Alerts, complete with images, can be sent to handheld devices, keeping retailers informed 24/7", says Jumbi Edulbehram, vice-president for strategic marketing at IntelliVid Corp., a Cambridge (Mass.) firm that makes the Video Investigator system [6]. Stores are increasingly under assault from organized gangs of professional shoplifters and store managers these days can get all the high-tech help they want. According to a survey by the University of Florida's Center for Studies in Criminology and Law, there was an increase of 37% in average dollar loss per shoplifting, from $622 in 2004 to $855 in 2005 [4]. Stores lost around $30 billion to shoplifting and employee theft in 2005 [6]. And for the same reasons, Wal-Mart stores across America increased the prices of their goods to cover the cost of revenue lost to shoplifting. IBM's Smart Surveillance System (S3) is another such system that can analyze real-time video while it is being digitally recorded and stored over a network [5]. According to National Retail Federation study, retailers were bilked for $1 billion from fraudulent returns and S3 can be used to identify customers who walked into a store entrance without a package but then approached the returns desk with a package.

These surveillance systems with data mining techniques are also being investigated to find out suspicious people who are capable of carrying out terrorist activities. Melbourne based Sentient Software has designed a system to spot potential terrorists, zoom in and track them and then identify them using facial recognition technology [9]. This system watches incoming video footage and learns the normal pattern of behavior for that scene. Then, when any unusual behavior takes place, the system picks out "highlights" to be watched by security guards. IBM's S3 can back-track the path of an object entering a particular area [5]. For example, in a video feed of an airport tarmac, S3 can electronically draw a line around a particular area of the screen and then back-track the path of anyone entering that secure area of interest. It sets off an alarm if the person walking into that secure area did not enter from a predetermined point of entry. One such example is the video surveillance system at Liberty Island's which is fully equipped and capable of running software that analyzes the imagery and automatically alerts human overseers to any suspicious events, though the park doesn't disclose any details [7]. The system can spot when somebody abandons a bag or backpack. It has the ability to discern between ferryboats, which are allowed to approach the island, and private vessels, which are not and it can count bodies, detecting if somebody is trying to stay on the island after closing, or assessing when people are grouped too tightly together, which might indicate a fight or gang activity [7].

There has been a lot of work on the automatic detection and prediction of unusual events, like the BSERVER, developed in the University of Minho and the ADVISOR project [2]. The aim of ADVISOR was to detect vandalism acts, crowding situations and street fights [2]. Another such system is being built at the University of Texas in Austin, US, that can tell the difference between friendly behavior, such as shaking hands, and aggressive actions like punching or pushing [8]. The main idea behind these systems is to detect an anomalous behavior whenever the trajectory of an observed object deviates from the typical learned prototypes. These systems find the probability that the object will follow a path that causes an unusual event, based on its previous trajectories and other properties. These systems use object movements to construct a statistical model of "normal" activity and the movements that are out of the ordinary can then be flagged up. Clearly, this is not a trivial task; it is possible that different kind of objects following a similar trajectory have distinct properties. For example, crossing a garden can be a normal behavior for humans, but an unusual one for vehicles. And the system must also be able to detect situations from combinations of multiple objects and their interactions. Also a person by him or herself may not be suspicious, but when seen together in a group he/she may be. That is, the system has to identify groups of suspicious individuals. Other challenges include the requirement for these systems to work under real-time conditions so that the system can analyze the surveillance data, make decisions and take appropriate actions promptly.

Data mining is widely used in commerce, but it has been controversial in security because of the fears of privacy loss and civil-rights violations. The critical need for applying data mining for surveillance poses serious privacy threats. The challenge here is to carry out privacy preserving surveillance. There are some efforts on blanking the face of a person on surveillance videos so that his/her privacy is maintained. To address privacy concerns, IBM's S3 can redact

things like people's faces and license plates with a black box or blur [5]. The video can then only be un-redacted by an authorized person if, for example, an incident occurs, and the video needs to be searched for a particular time span [5].

Despite this revolution in technology, no one is coming out in open and bragging about their new security systems. No store wants to tip off shoplifters or advertise that they suspect their customers. Another reason no one wants to talk much about surveillance is that they know it sparks concerns about privacy [6]. With so much going around the NSA's call surveillance controversy, no one wants to step out and cause further storm. Systems named here are just few of the innumerable attempts and a lot more of such systems are coming up lately. We might not notice any difference while we hang out at a store or the airport next time but people out there are involved in the super crunching of the highest form and watching us.

REFERENCES

1. J. Y. Lee, and W. Hoff, Activity Identification Utilizing Data Mining Techniques, *IEEE Workshop on Motion and Video Computing* (WMVC'07)
2. D. Duque, H. Santos and P. Cortez, Prediction of Abnormal Behaviors for Intelligent Video Surveillance Systems, *Proceedings of the 2007 IEEE Symposium on Computational Intelligence and Data Mining* (CIDM 2007)
3. H. Zhong, J. Shi, and M. Visontai, Detecting unusual activity in video, *IEEE Workshop on Motion and Video Computing* (WMVC'07)
4. 2001 NATIONAL RETAIL SECURITY SURVEY FLORIDA
5. http://www.news.com/Big-Blue-could-monitor-borders,-shoplifters,-moose/2100-1008_3-6133067.html
6. http://www.businessweek.com/magazine/content/06_37/b4000401.htm?chan=top+news_top+news+index_businessweek+exclusives
7. http://www.popularmechanics.com/technology/military_law/4236865.html
8. http://technology.newscientist.com/article/dn10387-surveillance-system-spots-violent-behaviour.html
9. http://www.news.com.au/adelaidenow/story/0,22606,16712029-911,00.html