Keynote: Intelligent Video as a Force Multiplier for Crime Detection and Prevention
Dr Alan J. Lipton
ObjectVideo, USA

ABSTRACT

Four of the main crime detection and prevention functions of law enforcement personnel are: physical deterrence; monitoring public areas; responding to crimes; and forensic analysis to “pick up the pieces”. An acknowledged challenge is the lack of manpower to be effective at these functions. Law enforcement agencies everywhere are embracing new technologies as “force multipliers” to make their existing labour force more effective. One valuable force multiplier technology is intelligent video surveillance (IVS) – computer software that can detect threats, crimes, or events of interest in surveillance video and automatically generate and distribute alerts for those events. This technology exists today and is experiencing commercial success in law enforcement applications world-wide. However, to fully exploit the benefits of such technologies, four specific factors need to converge: more specific IVS applications must be created to solve law enforcement challenges; IVS technology must enable smart devices that can be rapidly and ubiquitously deployed; these devices must proliferate based on applications and infrastructure outside of law enforcement; and law enforcement agencies must adopt new processes and policies to exploit them. This paper discusses these factors and provides examples of successful law enforcement agencies that have adopted and adapted IVS technology.

INTRODUCTION

In the modern world, police departments are beset with new challenges. Terrorist and criminal acts are more insidious and more audacious; urban expansion leads to increase in criminal activities; and criminals have access to more advanced technology and weaponry. At the same time, law enforcement budgets have not kept pace and law enforcement agencies are not expanding their membership. This means they are being asked to do “more with less”. The greatest tool that modern law enforcement has to lean on is technology. New products and technologies are emerging that can automate much of the drudgery of police work allowing police personnel to do the things they do best: providing a visible, ever-present deterrent; and being ready to respond when criminal or emergency events occur.

Video is seen as an effective force multiplication tool as it provides set of remote “eyeballs” into more areas than are practical to monitor directly. The United Kingdom leads the world in deployment of video cameras and video transmission infrastructure for the purposes of public safety, while the rest of the world is struggling to catch up. There are thousands of cameras located all around the public spaces of London – but without people to monitor those cameras they are useless for real-time crime detection and prevention, used only “after the fact” to pick up the pieces. In fact, the proliferation of video infrastructure has acted as a “force divider”, requiring humans to monitor large numbers of video feeds in real time, and generating huge volumes of video data that must be manually “mined” for activities of interest in the event of criminal activity. A U.S. example of this was the investigation into the DC Sniper shootings. Thousands of hours of video from car parks, petrol stations, and traffic cameras were examined looking for John Allen Muhammad and John Lee Malvo’s “white van” – when it turned out they were driving a blue car!

A technology that has recently arrived from the military world is Intelligent Video Surveillance (IVS). IVS allows computers to monitor video feeds in real time to detect activities of interest to law enforcement professionals and then transmit “alerts” to personnel in the form of network data packets over wireless communications infrastructure.

This technology has potential to be a real, effective force multiplier for law enforcement agencies in several ways. Most obviously, computer software can monitor video feeds and direct human attention only to areas needing further scrutiny – freeing up human crime-fighters to be out on the street where they can be of most use. They are more visible and therefore more likely to be a deterrent. They are also more distributed and thus more likely to be able to respond to criminal events. This “alert based” approach means that responders can remain in the field, yet still be in possession of all the contextual information they need to respond effectively to an event. Finally, there are also IVS tools that can relieve the drudgery of “after the fact” video analysis – tools that can mine video archives at high speed to extract useful events.

However, early adopter experience leads to the conclusion that there are several factors that must converge before use of IVS technology can be widely accepted in law enforcement applications. These factors are:

- Creation of specific IVS applications to support law enforcement missions.
- Delivery of IVS applications in small form-factor, low price-point formats to enable ubiquitous proliferation of the technology
- Deployment of IVS-capable devices and infrastructure based on non law enforcement applications
IVS APPLICATIONS FOR LAW ENFORCEMENT

The key technology in Intelligent Video Surveillance (IVS) \[1,2,3,4,5,6\] is called Computer Vision. This is a specialized branch of mainstream artificial intelligence research involving teaching machines to understand what they “see” through a camera. Traditionally, computer vision has had limited success in real-world commercial applications. Previously the best available automated video surveillance capability used a simplistic technology called Video Motion Detection (VMD) that is notorious for false alarms in realistic operational environments (see Figure 1). Recent advances in technology and computational power, along with the move of key talent from academia into industry have allowed computer vision to migrate from the lab into commercial video surveillance products.

Figure 1 (a) The source image - everything is moving. (b) IVS accurately detects the object

ObjectVideo is one company that has successfully expanded and commercialized some government funded computer vision research technology. This technology is used as the basis of an IVS product called ObjectVideo VEW that monitors video streams in real-time and detects activities that have been prescribed as interesting or suspicious.

Figure 2 Examples of ObjectVideo VEW applications for Law Enforcement

ObjectVideo’s solution watches video streams and extracts descriptions of all relevant objects. It employs sophisticated algorithms for extraction, detection \[1\] and tracking of all relevant objects in the camera’s view. It also provides algorithms for classification \[8\] of objects into specific types \[1\]. Figure 2 illustrates some examples of ObjectVideo applications with direct relevance to law enforcement missions. ObjectVideo technology can be used to detect vandalism, theft, property intrusion, suspicious packages, suspicious loitering, suspicious rendezvous and many other activities.

ObjectVideo Forensics

In addition to this real-time detection capability, ObjectVideo has an after-the-fact analysis tool called ObjectVideo Forensics\[9\] that applies the same level of analytical intelligence to archived information. Users create queries that are applied to archives of video and their associated meta-data. The analysis is performed on the meta-data only, so the results are extracted hundreds of times faster than real-time.

This capability offers three important advantages for law enforcement personnel: automated searching through video data is significantly faster than a human could achieve (which is important for time-critical applications); the human operator doesn’t have to physically monitor the search taking place, so they can effectively multi-task; and search parameters can be modified at any time, so the search can be repeated without using large amounts of human labour.

EMBEDDING IVS

Early versions of IVS products required large, centralized PC-based computing infrastructure. This is acceptable for a certain class of user, e.g. in mission-critical, homeland security or military applications, price and form-factor are no object. However, law enforcement operations are more budget-conscious and also more tactical in nature. An ideal IVS configuration for law enforcement would have cameras on every possible building, street, street-corner, public space, and police vehicle – all enabled with IVS technology to notify law enforcement personnel when events of interest are happening. To achieve this, IVS technology infrastructure must be reduced to the point where it can be deployed with every video camera -- without requiring a huge footprint and without placing too high a cost on the budget.

---

\[1\] The basic product classifies objects into “human” and “vehicle” classes, however the product also provides a simple mechanism for custom classification algorithms to be developed for customers with more specific needs such as to distinguish humans from animals, or trucks from aircraft.
Fortunately, two things have happened that facilitate this transition: the surveillance industry is shifting from an analogue to a digital paradigm; and IP-based devices (cameras, network video recorders, routers, and video servers) are becoming “compute platforms” designed to treat video – and other – data as digital network information rather than analogue signals.

The first trend is piggybacking on the explosion of IP infrastructure available today – and the promises of tomorrow. Wireless communications in the form of cellular technologies such as GSM and GPRS, and wireless network technologies such as WiFi and WiMax make it possible to create city-spanning IP-networks to transport video and other data to any point within a metropolis in real-time.

The second trend is a direct result of the first. As cameras and video management systems increasingly have to deal with video as a digital product, they require significant on-board compute power. They need to be able to perform video encoding, streaming, and decoding; image enhancement; camera control; and integration with other sensors and data sources. The time is right to treat IVS as simply another software application that can run on a video camera’s on-board compute-platform.

One of the most common approaches to adding compute power to a video device is through a digital signal processor (DSP). These are powerful programmable devices that, in many cases, are specifically designed for video and other digital media applications. One common example is the DM642 DSP from Texas Instruments. This is one of the most powerful DSPs for video applications.

ObjectVideo is one of the first companies to embrace the On-Board model for IVS applications. IVS technology has been ported from the expensive PC platform to the flexible TI DSP environment and will soon be available as a “feature” of commercial off-the-shelf (COTS) video cameras, video servers, and network video recorders (NVRs). The architecture of this solution is shown in Figure 3. This technology embedding has two important implications for law enforcement personnel. Firstly, the technology becomes small, low-power, mobile, and tactical. It can be embedded in a police vehicle or rapidly deployed to perform stake-out operations. And secondly, the price point for the technology is greatly reduced as it becomes an add-on feature of a video camera.

DEPOLYMENT OF IVS INFRASTRUCTURE – MULTI-PURPOSE CAMERA NETWORKS

Even with the price point and form factor of IVS technology dropping to consumer levels, police departments do not have the budgets to build the type of extensive surveillance network infrastructure that they would like. It’s too expensive and takes too much time to place a camera on every street corner, in every car park, at every petrol station, and so on. In addition, the expense of building an IP network to support all those cameras would be prohibitive. A faster and more effective way to achieve this goal is for Police departments to piggyback off camera networks emplaced by other organizations (both private and government) for their own purposes.

Fortunately, the nature of IVS technology allows it to be multi-purposed. A single network of video cameras can be used for many different applications, and IVS software can be architected in such a way as to shield one set of users from another. One of the key components of (at least ObjectVideo’s) IVS technology is the use of meta-data. Meta-data is a low level (textual) description of everything that is happening in a video scene. It contains the locations, classifications, trajectories, and interactions of every object in view of the camera (see Figure 4). ObjectVideo’s IVS technology exploits meta-data in a powerful way. The video analysis is broken up into two pieces: extracting meta-data; and using meta-data to determine when events of interest occur. This is powerful because it allows these two analytical pieces to be separated and distributed throughout an IP network. Consequently, multiple back-end software applications at different physical locations can mine the same real-time video data for different activities.
“Watches” Video  
Analyses Video
Separates Objects from Environment
Describes Objects and Activities (metadata)

**Figure 4 Extracting Meta-Data from Video**

The benefit of this approach from a law enforcement perspective is that private companies and government agencies alike will build IVS-enabled video surveillance networks for their own purposes that can be used by police departments for crime detection and prevention without sharing sensitive data.

Figure 5 shows an example. A retail chain deploys an IVS-enabled video network in its shops to perform several internal applications. The cameras are equipped with IVS software to analyse the video, extract object and activity descriptions and broadcast meta-data across their IP-network. The Loss Prevention group has a local back-end application looking for employee theft activities. The Risk Management group has an application looking for people slipping or falling, or speeding vehicles in the car park. The Business Intelligence (or marketing) groups have applications watching the flow of people through the shop, their dwell time at particular displays, the lengths of queues, and the effectiveness of their marketing efforts. None of these groups is sharing its data with the others – but they are all receiving the same, common, totally generic meta-data from the camera network. Similarly, a local police department may be given access to this network and may be able to “listen” to the broadcast meta-data from the shop cameras. They could then have back-end applications looking for vandalism, theft, or public unrest.

![Figure 5 Using meta-data to create a multi-purpose camera network](image)

Already we are seeing large camera networks deployed by governments and industry – and many of these networks have a view over public areas. Traffic management systems are watching the roads and intersections; retail cameras are watching car parks and public roads; public transport cameras are watching railway platforms and bus stops; and so on. The main challenge for police departments derive useful information from all these camera networks is the lack of standards. Camera networks and IVS applications all have different proprietary methods for representing and transmitting data. It requires a dedicated push from user groups such as police departments to force vendors to standardise their data formats so that they can gain the maximum public benefit from these networks.

Of course, other ever-present challenges are individual privacy and data security. Now that physical security information is network data, it is subject to the same types of cyber-attack as any other network data. Consequently, network security techniques will have to go hand-in-hand with video sensor proliferation. The story is a little easier where privacy is concerned. IVS technology is a “force for good” in the battle for individual privacy. A large argument against expansive camera networks is that “big brother” might be watching. With IVS, the potential for human abuse of video data is greatly minimised. It is a machine monitoring the video – not a minimum-wage security guard. Attention is only drawn to a particular video view when something potentially significant is occurring. Importantly from a Civil Liberties standpoint, some IVS vendors offer the ability to “obscure” human faces in video streams until such time as a human operator confirms that they have ‘broken’ a rule, maintaining presumption of innocence and customer confidentiality.

**POLICE PROCESSES AND PROCEDURES**

Finally, once IVS enabled camera networks are deployed throughout a metropolis and IVS applications exist to support law enforcement missions, the police will need to change policies and processes to adopt and adapt the new technology. Police will have access to more information than ever before. Information will be available on call through wireless devices and networks. Police operations will have to adapt in three ways: technology adoption; decentralisation; and cooperation.

Obviously, for new technology to be successful it has to be readily adopted by users. Police have to be willing to allow new devices and technologies into their processes. Wireless devices will link police, in real-time, to remote video data, archived video data, and other information sources and data bases. Each police car will become its own command centre capable of seeing the “big picture” collected from thousands of remote sensors and integrated by automated technologies.
Furthermore, with the creation of these mobile command and control centres the requirement to have central dispatch and command centres to integrate information and coordinate action is minimised. Information will be available everywhere, on-demand. And coordination of police activities can be done at the individual unit level rather than requiring a central dispatch function.

Finally, with police departments sharing information with public entities, private entities, and other police departments; new methods of cooperation and coordination will need to be devised. The delineation between a private guard force, a local police authority, a federal police authority, and a military authority will need to be seamless.

CASE STUDIES

Through its work with early adopter customers, ObjectVideo has witnessed law enforcement agencies adopt IVS as a powerful force multiplication technology and thus be able to modify their operations to be significantly more effective.

U.S. Customs and Border Protection

ObjectVideo’s largest customer is the U.S. Customs and Border Protection Agency (CBP) who are part of the Department of Homeland Security (DHS). They have the arduous task of monitoring the “longest stretch of unprotected border in the world” and they had a problem. U.S. Customs controls all of the border crossing points – or ports of entry (POE) in the United States. That means that every time a road crosses the border between the U.S. and Canada or Mexico, there is a Customs presence. Some of these POEs are very remote and are not manned around the clock. When the POEs were unmanned, they would place orange cones in the middle of the road and put up a sign saying “please do not enter the United States”. At that point they would hope that Border Patrol or local law enforcement could monitor these locations (which was not a priority for these other agencies).

To solve the problem, CBP put cameras up at each of these locations and installed IVS software to monitor them. Now, whenever there is a border incursion, the event is detected by the IVS software, transmitted to a central US Customs facility and alerts are dispatched to Border Patrol and local law enforcement agencies on the scene using satellite communications.

As a results of this technology, they have realised three important benefits. Firstly, they are catching many more illegal activities than previously. Secondly, they are enjoying a far more cooperative relationship with Border Patrol units and local law enforcement agencies than they ever have in the past. And finally, they have radically reduced the cost of taking legal action in these illegal immigration cases. They don’t need to waste personnel time scanning through video to find the incursion and they often don’t need to waste personnel time in court appearances because many of the perpetrators, upon seeing imagery of their transgressions, will “plead out” rather than going to court.

Port of Jacksonville, Florida

One of the most technologically advanced customers of ObjectVideo is the Port Authority of the Port of Jacksonville, Florida. Like all U.S. seaports they are faced with government regulation demanding greater security. The challenge they face is that they have a very large physical area, and a fairly small police force. So they decided to adopt technology, and in particular IVS technology, as a force multiplier.

Figure 6 US Customs and Border Protection Using IVS to Protect the US/Canada Border. The individual surrounded by the red box has illegally run across the border. US Customs personnel (blue) are instantly dispatched to apprehend them.

Figure 7 Port of Jacksonville, Florida. Using IVS to empower a Mobile Police Force
The Port Authority set up a wireless video camera network infrastructure and configured each of their police cars with wireless communications and video management software. This enables every police officer to control the video surveillance system (and other critical systems like access control) from his or her vehicle. They can view video, control pan, tilt, zoom (PTZ) cameras, record video, and many other functions from anywhere on the port. The most significant piece of technology is IVS. The system is configured to automatically notify police officers when any one of a number of significant events occurs. These events include perimeter breach, theft, depositing of a suspicious package, illegal vehicular activity (either on the roads or on the waterways), and a number of other applications.

As a result of this wireless security network, they have dispensed with their central dispatch office. There is no central location where security data is monitored and security personnel are dispatched. Each individual police car is its own central monitoring station. The two major benefits of this are: they can completely utilize their personnel without tying some of them to a central location doing dull, routine work; and their personnel are distributed throughout the facility so they have been able to drastically reduce their response time when events of interest do happen. Additionally, the port has made the information generated by the IVS system available to other Law Enforcement entities in the area, integrating them into a now expanded response team working from a common operating picture.

CONCLUSION

Four of the main crime detection and prevention functions of law enforcement personnel are: physical deterrence; monitoring public areas; responding to crimes; and forensic analysis to “pick up the pieces”. An acknowledged challenge is the lack of manpower to be effective at these functions. Law enforcement agencies everywhere are embracing new technologies as “force multipliers” to make their existing labour forces more effective. One valuable force multiplier technology is intelligent video surveillance (IVS) – computer software that can detect threats, crimes, or events of interest in surveillance video and automatically generate and distribute alerts of those events. This technology exists today and is experiencing commercial success in law enforcement applications world-wide. However, to fully exploit the benefits of such technologies, four specific factors need to converge: specific IVS applications must be created to solve law enforcement challenges; IVS technology must enable smart devices that can be rapidly and ubiquitously deployed; these devices must proliferate based on applications and infrastructure outside of law enforcement; and law enforcement agencies must adopt new processes and policies to exploit them.

In this paper, we have discussed these factors and shown examples of how IVS technology, when appropriately applied with the right infrastructure, can act as a strong force multiplier. This technology allows police officers to be more efficient and more effective; improves cooperation with other public and private agencies; and can radically modify how they conduct their missions.

REFERENCES


