IJIS Institute

ADVANCES IN DIGITAL VIDEO: GETTING THE MOST VALUE FROM VIDEO INFORMATION

IJIS Institute

Emerging Technologies Committee White Paper

December 2011

Principal Contributors

Mike Reade, IBM Corporation – Author

Matthew D'Alessandro, Motorola Solutions Inc. – Committee Chair

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following additional contributors and their sponsoring companies for supporting the creation of this document:

John Crouse, Policy Studies, Inc. – Committee Vice Chair

Ralph Bell, Motorola Solutions, Inc. – Editor

The IJIS Institute would also like to thank the U.S. Department of Justice (DOJ) Office of Justice Programs (OJP) Bureau of Justice Assistance (BJA) for their comments and feedback.

This project was supported by **Grant No. 2010-DJ-BX-K083** awarded by the *Bureau of Justice Assistance*. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

CONTENTS

LIST OF ILLUSTRATIONS

INTRODUCTION

The use of video in the public safety and justice realm has taken on greater significance over the past decade, due primarily to advancements enabled by digital video and its gradual replacement of analog video over this period. Video captured in, or converted to, a digital format has enabled many new capabilities that affect the cost and ease of storage, sharing of inter- and intra-agency video information, integration with other systems and data sources, and analysis used to extract meaning from large volumes of video data. This paper briefly describes the advancement in each of these areas as applied to the many domains (lines of business) within the justice and public safety enterprise, but with a deliberate focus on law enforcement as the front-line producer and consumer of video information. In addition, emerging video technologies and applications will be presented, along with an overview of the evolving standards applied to this relatively new source of valuable crime fighting information.

OVERVIEW

The evolution from analog to digital networked video has helped bring video into common use throughout justice and public safety. Once regarded as a tool for law enforcement or security officers to observe behavior or for post-incident analysis, digital video information of today has proven to be more useful before, during and after a reported incident or response.

As the use of video information has increased, there has been a concomitant trend toward declining video technology cost. Partly based on this, there has been an increase in the installation of cameras without due consideration of how video capture can serve broader goals beyond traditional surveillance purposes. In fact, skilled public safety personnel who monitor up to hundreds of video cameras have shown to be somewhat ineffective in improving public safety. Even the most highly trained and motivated professional can fail to notice activity that might warrant attention after as little as twenty minutes.

Notwithstanding the negative perception conjured up by the term “surveillance” by privacy advocates, and the public at large, it is important to consider the value of video information beyond this traditional use simply because it can be a less than optimal use waste of limited resources when broadly applied. When networked, shared and analyzed, video provides its greatest value when additional uses are considered:

- Live video can provide *situational awareness* for operations or conditions that are developing.
- Video can provide tactical information to compliment other communications during a response.
- Quality video can provide valuable information to assist investigations.
- Properly managed video can provide evidence to support prosecution, to increase conviction rates, and to reduce litigation claims.
- Video capture for patrol cars, interview rooms, court proceedings, corrections, and more can provide an additional layer of safety and security for public

safety personnel, while also reducing instances of false claims and litigation.

- Video applications for remote or virtual arraignments and depositions can reduce costs while reducing the inherent risk of transporting suspects and inmates.

- When integrated with other systems and sensors, correlated data can provide enhanced awareness, and can improve command and control.

- By applying advanced analytics, accumulated video data can assist in determining patterns or trends for enhanced decision-making and training.

Consideration to these applications should be given when appropriate to guide decisions about the many facets of a digital video network design.

BASIC SYSTEM COMPONENTS

The basic components of a video system include:

- **Camera** – the video "sensors" or capture devices. Audio can also be captured either within the camera or via a separate device (microphone).

- **Encoder** – converts camera output to digital format if cameras are analog. The majority of cameras deployed and still being sold today are analog.

- **Network** – enables the transfer of captured video to its eventual consumer. Both wired and wireless networks are prevalent today, with hybrid networks offering the advantages of both.

- **Storage** – a video repository that can be centralized or distributed on disk media (i.e. server based drives, Digital Video Recorders [DVRs], Network Video Recorders [NVRs]), digital tape media, or a hybrid.

- **Video Management Software (VMS)** – provides core management functions, such as camera control (i.e. pan, tilt, zoom), live viewing and playback.

To further enhance the value of video information, analysis can be enabled by software that identifies elements of video to be brought to the attention of the user. Basic analytics are often incorporated in the VMS, while more complex analysis capabilities are provided by add-on software applications (often from companies other than those providing the core VMS). Video analytics hold the promise of assisting, observing and identifying important activity in live video, as well as the ability to search video post-capture for elements of interest identified after the fact.

IMPLEMENTATION & STANDARDS CONSIDERATIONS

A variety of organizations are involved in the research and development of digital video and advanced applications, as well as system designs, for public safety use, ranging from traditional physical security equipment manufacturers and system integrators. They include organizations such as Physical Security Interoperability Alliance (PSIA), American Society for Industrial Security (ASIS), International Security Conference (ISC), Public

Safety Communications Research (PSCR), as well as public safety IT-related groups, such as the now defunct Law Enforcement Information Technology Standards Council (LEITSC). In addition, due to the opportunities presented by the movement from analog to digital information, technology companies such as IBM, Siemens, Cisco Systems, Inc., Motorola Solutions, Inc., and many others have joined traditional physical security vendors in developing video solutions for the public safety and justice markets.

According to PSIA, some de facto standards are emerging—for example, 'H.264' is the standard for video compression of high density video over internet protocol (IP) networks. More importantly, interoperable communication specifications, which are increasingly needed in the industry, are beginning to surface. The Security Industry Association (SIA) has been working on the Open Systems Interoperability and Performance Standard (OSIPS) framework for a number of years. This framework is moving towards establishing open, non-proprietary standards in this area.

The Open Network Video Interface Forum (ONVIF) is another organization currently addressing the digital video market from the standpoint of video, while PSIA promotes the interoperability of IP-enabled security devices across all segments of the security industry, including video, access control, analytics, and software.

Open communication specifications are important for reasons vital to public safety users. Interoperable communication specifications enable disparate networked security products, such as video surveillance and intrusion detection, to communicate more readily than in the past. This communication capability will enable the ability to share forensic data more readily by speeding up investigations and enabling information sharing across the public safety and justice spectrum.

Digital video enabled public safety applications represent a fraction of the overall physical security industry marketplace. This small representation presents a challenge to those developing products and standards that serve the needs of government agencies. While some security industry specialists have created a niche in developing and implementing video systems for public safety, there has not been much movement toward developing products in support of public safety information sharing standards, such as the National Information Exchange Model (NIEM). The IJIS Institute has not yet taken a position on the development and adoption of standards for video information sharing; however, groups like SAFECOM (The Wireless Public Safety Interoperable Communications Program) and PSCR have published some helpful guidance.

When researching options for implementing new video networks or upgrading existing analog systems, public safety agencies would be well advised to work with integrators that have experience in the design and implementation of municipal networks and public safety systems. Many traditional physical security integrators, while well versed in the latest component technologies (such as high-resolution cameras and analytics software), may not have the experience and knowledge necessary to deal with the complexities and challenges presented by factors unique to law enforcement and municipal government systems.

These factors include:

- Law enforcement information security requirements, such as requiring video encryption, digital watermarking, and secure communications;
- City-wide networks with hybrid wired and wireless topologies and harsh outdoor environments;
- Privacy protection requirements;
- Prevalence of mobile and ruggedized components;

- Access control and chain of custody audit capability;
- Event based *ad hoc* deployments;
- Integration and information sharing between systems with different owners, including both public and private; and,
- Integration of disparate video systems, cameras and sensor inputs.

There are many commercial off-the-shelf (COTS) products available from a wide variety of manufacturers to create an end-to-end networked digital video solution. There are even some open-source components that can extend the functionality of the system, such as video players and browser-based viewers that can enable more users of the system at little cost.

The investment required to implement networked digital video depends on several factors that include delivering a range of required functionality to varied users or stakeholders in the system. It is important that the needs of each stakeholder group, from law enforcement and first responders, to the courts and beyond, be evaluated and addressed if the system is to deliver on the promise of what video information may offer across the spectrum of public safety and justice.

While several basic component costs of a video network (such as cameras, network and storage hardware), are stable or declining, the total cost of implementing and maintaining these systems need to be carefully managed to avoid additional costs that could occur when vast amounts of video data are stored for extended periods of time, and when increasingly more cameras are tied into the network. To control storage costs, consideration must be given to only store information needed to serve the stakeholders, and to store it for only as long as necessary to meet local, state or Federal statutes for the storage of records or evidence.

When designing and building the network used to transport video from its capture (the "edge") to its intended users, and, ultimately, to storage, other uses for the network to improve connectivity and communications should be considered for cost-justification purposes. Enabling other mobility applications, like hand-held information query and sharing tools, can also justify these network investments as broad infrastructure improvements that benefit more public safety and other users.

Video camera technology itself has seen many improvements in recent years. The incorporation of the same technology we have become accustomed to in consumer products—for example, multi-megapixel resolution and High Definition (HD) quality—presents new opportunities for reassessing camera quantities and placement. A multi-megapixel camera provides a much more enhanced quality of video, which allows for improved clarity when zooming in on a particular activity of interest. This enhancement has led to the ability to utilize a single camera for viewing a very wide area instead of multiple cameras covering the same area; however, there is risk in broadly adopting this approach without understanding the potential impact with regard to viewing angles, obstructing objects, and the effectiveness of analytics applications in this environment.

Extremely high definition cameras and cameras with multi-megapixel resolution are more costly, consume larger amounts of network bandwidth, and do not always allow for the same flexibility that several less expensive cameras may provide. It is important to individually evaluate each scenario and potential use cases.

Video analytics, while not a required component of any system, can deliver new capabilities to a digital video network, with proper understanding of its capabilities and limitations. Once portrayed as somewhat of a panacea, video analytics providers are

becoming more realistic about its strengths and drawbacks. Still considered an emerging field, video analytics can assist human observation by providing alerts to defined events, such as motion detection, crossing a "virtual tripwire," or more sophisticated activity such as gathering crowds, directional motion, or objects removed or left behind. Simple video analytics can be placed in edge devices (either in or connected to the camera), while more complex analysis is typically performed by more powerful computer processor's within the system's servers and storage equipment.

FIGURE 1. VIDEO FRAME ALERT FOR SIMPLE MOTION DETECTION

FIGURE 2. VIDEO FRAME DEPICTING "VIRTUAL TRIPWIRE" AND MONITORING DIRECTION OF MOTION

More complex alerts are also available—for example: monitoring for abandoned objects to assist in identifying suspicious packages left behind by a person; person threshold counting to identify the congregation of people that may warrant interest; and, even the ability to identify potentially threatening or violent behavior in prison environments. One of the newer applications is attempting to accurately identify drug dealing behavior on 'the street'.

Each of these alert types must be carefully configured during system implementation, requiring each camera's purpose to be defined and the viewing environment considered. This typically involves testing for several days under changing environmental conditions and accommodating for varying light levels, glare or reflections, clouds, etc.

The alerts are defined and designed for each camera, and any camera movement or change to the viewed area will most likely affect its effectiveness. An exception to this concern would be simple motion detection alerts; however, even that simple analysis can produce false alarms due to minor movement (*e.g.* wind blowing trees) if thresholds are not properly set.

The latest developments in video analytics also address the challenge of finding video events that may not have been recognized as threats when initially recorded, and do not trigger an alert, but nonetheless require identifying and locating recorded video for investigations, prosecution, pattern and trend recognition, or many other uses. These events can take many hours, days or weeks to manually locate. This function can reduce that search time to seconds or minutes. Such was the case in London following the mass transit bombings when manual analysis took many days.

While the technology does not exist today to search for very specific items (*e.g.* Ford vs. Chevrolet or male vs. female), there have been significant advances in recognizing elements such as color, shape/size, direction, speed of movement, building face catalogs, and tracking and accumulating knowledge of activity "hotspots," among many other things.

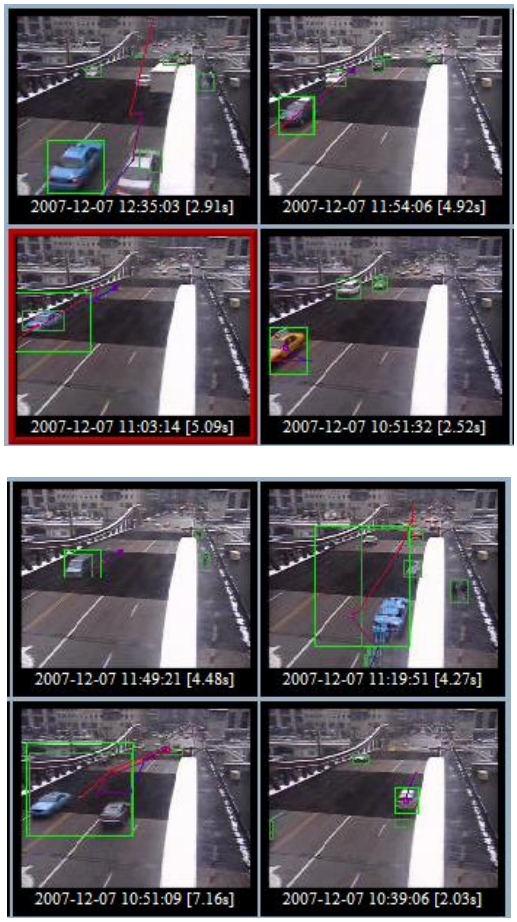

FIGURE 3. VIDEO FRAME SHOWING RESULTS FROM SEARCH FOR "BLUE CAR"

Additional pitfalls associated with video analytics are described in the section below, Summary of Strengths, Weaknesses and Challenges.

The continued justification for investment and funding in these systems has proven to be one of the greater challengers to the sustainability of networked video projects in many cities.

From the initial capital outlay needed for the network, to the camera and IT infrastructure needed for the launch of a video project, to the maintenance and growth of systems as more cameras and user access are requested, it is often difficult for public safety agencies to secure the appropriate budget given the fiscal constraints of today, let alone try to identify new funding to fully support these projects. This challenge could be reduced if soft and hard benefits were properly presented to the many audiences that influence the approval of funding, and, ultimately, the acceptance of networked video as a real benefit to public safety.

Messages that convey evidence-based successes (*e.g.* when video enables arrests, supports prosecution, or protects against false accusations) of a network video project should be tailored to city or county elected officials, executive decision-makers, and other stakeholders. Likewise, communication should be made with the justice system beyond law enforcement, and should include Federal funding agencies, other grant sources, and the community that stands to benefit the most from improvements in public safety: the citizens and businesses that thrive in a much safer and more secure environment.

Currently, there is no national mandate, institutionalized recommendation or methodology to capture statistics on incidents reported, crimes cleared, or the convictions obtained where live or stored video has played an assisting role; however, we see frequent reports in the media and from various watchdog groups that appear to question or challenge the contribution that video has made in reducing and/or solving crime. With no requirement to document successful video usage, nor the tracking mechanism set in place to aggregate statistics on the role that video information has played, challenges in funding and public perception issues will always remain. The law enforcement agency that plans for the future and understands the value of networked video should establish its own means to report the benefits and positive outcomes of effective video capture and management in order to ensure the long-term sustainability of its video program.

SUMMARY OF STRENGTHS, WEAKNESSES & CHALLENGES

Strengths

- Properly planned, designed and implemented, a video network can serve many stakeholders across the public safety and justice spectrum, from first responders to investigators to prosecutors.
- Strategic use of municipal video can provide an increased feeling of community safety, and can reduce reported criminal activity.

Weaknesses

- Balancing costs with requirements often results in trade-offs that weaken the effectiveness of a system and the information it provides (*e.g.* installing a single, wide-angle camera high above a viewing area to cover that area with one camera to save costs may prove inadequate if the need to read a license plate or identify facial characteristics arises).

Challenges

- Avoid proprietary video management software (codec) that does not allow any stored video to be viewed and shared with a standard COTS or open source player, such as Microsoft Media Player.
- Ensure proper security controls of the entire system, as you would with any IT application, from video capture through the network (via encryption) to viewing and storage (through access controls) to tamper protection (via digital watermarking). This is important for several reasons:
  - Protecting individual privacy, and the justice enterprise, from first responders to investigators to prosecutors.
    - Ensuring law enforcement sensitive information doesn't get "leaked" to unintended parties [*i.e.* social media (*e.g.* You Tube, Facebook, etc.) or news media); and,
    - Properly documenting strict chain of custody for court-admissible evidence.
- Video can be an effective force multiplier.
- Recorded, indexed and cataloged video information can support higher conviction rates and increase security of agency staff.
- Understanding the limitations of video analytics:
  - Real-time alerts or alarms require predefined criteria on what constitutes a threat; false alarms can undermine the desired attention given by personnel.
  - Many factors need to be considered in improving accuracy and to achieve the benefits of alerts, including camera placement, background motion, changing light conditions, and others.
  - Consider applications for real-time vs. post-capture analysis, and the desired use cases for each stakeholder group when deciding on video analytics "at the edge" (in/near the camera) or server-based processing.

CONCLUSION

This paper presents only an overview of the many elements and factors that will determine successful justice and public safety networked video projects. Several topics mentioned in this paper are worthy of lengthy discussion in their own right. For those interested in video solutions, it is recommended you engage independent, experienced consultants and establish a working group that includes the various stakeholders, identifies requirements, establishes critical success factors, and evaluates technologies that will enable the achievement of success.

Networked digital video can be a valuable tool for law enforcement and the broader criminal justice domains. Beyond traditional surveillance uses, video information can enable and support many critical public safety functions including investigations, situational awareness and response, risk management, and more. Each of these uses, and the unique needs of each user group that will benefit from them, should be considered in the design and implementation of networked video systems to maximize the benefits derived and to ensure a successful and sustainable video project.

ABOUT THE IJIS INSTITUTE

The IJIS Institute unites the private and public sectors to improve critical information sharing for those who provide public safety and administer justice in our communities. The IJIS Institute provides training, technology assistance, national scope issue management, and program management services to help government fully realize the power of information sharing.

Founded in 2001 as a 501(c)(3) nonprofit corporation with national headquarters on The George Washington University Virginia Science and Technology Campus in Ashburn, Virginia, the IJIS Institute has grown to nearly 200 member and affiliate companies across the United States.

The IJIS Institute does its valuable work through the contributions of its member companies. The IJIS Institute thanks the Emerging Technologies Committee for their work on this document.

The IJIS Institute also thanks the many companies who have joined as members that contribute to the work of the Institute and share in the commitment to improving justice, public safety, and homeland security information sharing.

LINKS TO MORE INFORMATION

DHS Video Quality in Public Safety (VQiPS)
http://www.safecomprogram.gov/SAFECOM/currentprojects/videoquality/

FBI Caught on Video link
http://www.youtube.com/watch?v=u5Oj2FDwLXs

The IACP In-Car Video Technical Assistance website
http://www.theiacp.org/PublicationsGuides/Projects/InCarCameraTechnicalAssistance/tabid/305/Default.aspx

The IACP Forensic Video project
http://www.theiacp.org/PublicationsGuides/Projects/RegionalForensicVideoAnalysisProject/tabid/309/Default.aspx

The IJIS Institute
http://www.ijis.org

National Center for State Courts video technologies resource guide
http://www.ncsc.org/topics/technology/video-technologies/resource-guide.aspx

Open Network Video Interface Forum website
http://www.onvif.org/

Physical Security Interoperability Alliance website
http://www.psialliance.org/

Public Safety Video Quality – U.S. Department of Commerce – Public Safety Communications Research project
http://www.pscr.gov/projects/video_quality/video_about.php

SAFECOM Video Quality in Public Safety Working Group
http://www.safecomprogram.gov/SAFECOM/currentprojects/videoquality/videoquality.htm