

Conclusion

The terrorist attacks of 9/11 as well as the Boston marathon incident that happened more recently raised the public awareness of security issues as well as tremendously increased the importance of intelligent automated video surveillance systems applied in public, commercial, law enforcement, and military domains.

Computerized video processing and analysis implemented in a variety of fields, such as governmental institutions, various businesses, municipalities, agencies, educational institutions, mass transportation centers, financial institutions, utility plants, medical centers and industries, is typically associated with analysis of video streams captured by surveillance systems. It performs video real-time analysis for immediate detection of events of interest as well as analyzes pre-recorded video for the purpose of extracting events and data that is known as forensic analysis.

As the use of video surveillance systems becomes more widespread and the quantity of recorded video increases, the need to go through recorded video data and extract specific segments and events of interest is growing. Very often in such cases, time is of the essence, and such review must be undertaken efficiently and rapidly. When done manually by human operators this represents a very time consuming, inefficient, and tedious task. Considering various research studies and real-life incidents indicate that an average human operator employed in an analog video surveillance system, tasked to observe video screens, cannot remain alert and attentive for more than 20 minutes and that the operator's ability to monitor the video and effectively respond to events is significantly compromised with time, operators show to be a costly resource with limited alertness and attention. This makes intelligent automated video surveillance systems to automatically monitor cameras and alert for events of interest very attractive and popular.

The benefit from a video surveillance system is significantly increased when it is accompanied by intelligent video analysis. Intelligent automated video surveillance systems make practical and effective use of the surveillance systems. The application domains of the intelligent automated video surveillance systems are numerous: security applications and intrusion management where it ensures perimeter control for sensitive or restricted areas such as permit parking and limited-access buildings where security officers are alerted to automatically detect and track burglary or to a suspicious individual loitering in the parking lot; urban surveillance applications where it measures traffic flow, detects accidents on highways, monitors pedestrian congestion in public spaces; crowd management where it compiles consumer demographics in shopping malls and amusement parks, monitors for the build-up of crowds in public areas based on occupancy measurements, ensuring that customers are not impacted by uncomfortable and potentially unsafe crowds; industry applications where it performs quality control or count the number of products on the production lines; various military applications include patrolling national borders, measuring the flow of refugees in troubled areas, providing secure perimeters around bases and embassies, battlefield surveillance applications, real-time moving object detection and tracking from stationary and moving camera platforms, recognition of objects like humans and different types of vehicles, human gait analysis, human activity recognition, vehicle tracking and counting, airborne surveillance, etc.

Numerous advantages of automated intelligent video surveillance systems caused an increased number of cities, schools, districts, workplaces, apartment buildings, garages, stores, banks, restaurants, and public housing to apply surveillance systems to monitor movement, detect illegal activity, and protect the public. The survey conducted in 1997 showed that only 13 city police departments in the US used CCTV video surveillance systems, primarily to monitor pedestrian traffic and to catch cars running red lights. After 9/11, this number significantly increased. Every city in America now has its share of private surveillance cameras that monitor public areas such as sidewalks, parking lots, freeways, and traffic lights, many of which are integrated with the Internet so that real-time video of people in public places can be observed online. Thousands of Web cameras in every corner of the world distribute images of street scenes, famous landmarks, and allow the Internet observer to control who, what, and how closely the target subject is observed.

Besides the US, many countries employ public video surveillance to monitor population movements in order to prevent crime and potential terrorism like Singapore, Canada, the US, Australia, China, UK, and other European countries that installed thousands of cameras in public settings. The United Kingdom is by far the international leading country in the matter of applied CCTV video surveillance as according to one source the average Briton is photographed by 300 separate cameras in a single day.

All the advantages of the video surveillance systems raise other questions and concerns that are conflicting with its beneficial side like: privacy issues, its philosophical or theoretical considerations, policy issues related to video surveillance, its social and legal dimensions, cost, rate of return of investment, quality assurance, etc. (Nieto, Johnston-Dodds, & Simmons, 2002; Bharucha, London, Barnard, Wactlar, Dew, & Reynolds, 2006; Collins, et al., 2000; Scherr, 2007).

An intelligent automated video surveillance system is tireless and permanently records everything without ever getting distracted. Recorded digital videos and images are permanently stored and can be viewed at any time, from any place, as many times as desired. The arising problem is that this data can be modified and used beyond the original intent of either the image collector or the subject. This is why the public, some government officials, and various organizations are increasingly concerned about protecting individual privacy.

For three decades, until the late 1990s, continuous video surveillance was mainly considered by courts and legislators to be a form of “passive” surveillance, which was not considered to be an intrusion upon an individual’s privacy and did not present a significant legal obstacle. Within the last years, the rapid increase in the application of intelligent video surveillance systems have significantly impacted the appropriate use of video and related surveillance technologies and their implications for civil liberties and privacy rights.

The speed at which video surveillance systems evolve challenges the ability of judicial and legislative system to enact and enforce policies that protect the public’s security and right to privacy. The newly opened questions that are inevitably imposed are global use of emerging surveillance technologies, law enforcement, national security interests, and the privacy rights of citizens. Apart from being defined as the “right to be let alone,” the legal concept of privacy encompasses three categories: physical privacy, informational privacy, and decisional privacy, which are all tackled by video surveillance systems.

According to some polls, American citizens are willing to give up some privacy for better security but at the same time are concerned about the possibility that information obtained from video surveillance could be abused by government agencies, employers, or businesses, as well as about the potential false identification caused by computer errors.

The ethical implications of surveillance technologies on the privacy of citizens and the pragmatic approach to the central ethical concern about privacy and confidentiality protections and relevant issues of the informed consent process as well as the question about setting the appropriate balance between law enforcement, national security, and civil liberties are far beyond the scope of this book and are left to be addressed by professionals in those fields like sociologists, legislators, lawyers, philosophers, psychologists, etc.

The book, *Video Surveillance Techniques and Technologies*, offers various original methods and algorithms that automatically analyze video with the goal to detect, track, and identify moving objects based on sequence of images. It also includes biometric algorithms for anthropometric measurements, military aircraft radar ISAR image analysis, and iris recognition. The book is primarily aimed for graduate students and professionals in the field of signal and image processing applied in static/moving object detection, tracking, and identification, but I hope that others who are also in the field of video surveillance and security can profit from its content as well. The targeted readers' group can benefit from its educational and informational content, and the wider audience can perceive and get the idea through this book about the algorithms and intelligent software that represents the main core of intelligent automated video surveillance systems.

The main value of this book lies in its practical implementation in numerous domains and wide spectra of applications like video surveillance, homeland security, military applications, healthcare, quality control, industry, safety, etc. The described mathematical algorithms are employed in security video surveillance systems with wide variety of applications, some of them having very high priority and importance: homeland security and national defense. These algorithms could be further extended to perform other functionalities like identification, behavior analysis, or other forms of situation-awareness, which is the scope of my future research.

Vesna Zeljkovic

New York Institute of Technology, Nanjing Campus, China

REFERENCES

- Bharucha, A. J., London, A. J., Barnard, D., Wactlar, H., Dew, M. A., & Reynolds, C. F. III. (2006). Ethical considerations in the conduct of electronic surveillance research. *The Journal of Law, Medicine & Ethics*. doi:10.1111/j.1748-720X.2006.00075.x PMID:17144185
- Collins, R. T., Lipton, A. J., Kanade, T., Fujiyoshi, H., Duggins, D., & Tsin, Y. ...Wixson, L. (2000). A system for video surveillance and monitoring (CMU-RI-TR-00-12). Pittsburgh, PA: The Robotics Institute, Carnegie Mellon University.
- Nieto, M., Johnston-Dodds, K., & Simmons, C. W. (2002). *Public and private applications of video surveillance and biometric technologies*. Berkeley, CA: California Research Bureau, California State Library.
- Scherr, C. (2007). You better watch out, you better not frown, new video surveillance techniques are already in town (and other public spaces). *I/S: A Journal of Law and Policy for the Information Society*.