Safety Operations Supporting the Security of Urban Locations

HIROAKI Toshihiko

Abstract

New types of criminal activity such as home-grown terrorism are becoming difficult to prevent by the traditional monitoring methods that focus on a visual black list matching. In the future it is expected that the utilization of various AI technologies as well as white list matching will make it possible to detect the unsuspected anomalies that are hard to discover or predict by human endeavor alone. Thereby it will be possible to adopt measures that will even be able to deal with new types of crime. The system design is also anticipated to shift from crime prevention market to normal operation management market, so that even greater value can be created. This paper outlines the viewpoint of NEC regarding surveillance solutions in support of the safety and security of urban locations and discusses progress in creating technologies that will provide support for them.

Keywords
video surveillance, public safety, sensing, visualization, recognition technology, artificial intelligence (AI), data mining, crime/terrorism prevention

1. Introduction

The trend in concentrations of populations of urban areas has been increasing in a global context for a long time. The ratio of populations living in urban areas now exceeds 70%, and some experts predict that the ratio could reach as high as 90% by 2050. As the creation of infrastructures is not able to catch up with such rapid urbanization, various social issues such as traffic congestion are currently in question and the increase in urban-type crimes is another such problem.

The urban areas attract diverse groups that tend to come from rural areas and foreign countries. If other factors such as the income gaps and poverty are added, the sense of belonging and being colleagues tend to be very sparse in such areas. As a result, community support and the self-governance of entire local areas have become difficult and mutual concern for each other's wellbeing is less practiced. Due to such trends, it is now considered that the psychological barrier of criminal activity has been lowered. From the criminal viewpoint the urban areas offer advantageous locations for their crimes because of the concentration of population that facilitates finding targets more easily and the effects of conflict including terrorism are high.

Countermeasures designed to combat the increasing crime rate include improvements in the field of security and in the police forces. However, the financial situation of local governments makes it difficult to increase police force numbers by large amounts. As a solution to this problem, interest in the use of IT in surveillance and security has been growing. A typical example is the introduction of surveillance systems based on video cameras. In London, which is well known as a representative example of this trend, surveillance video cameras are installed in many locations around the city, and monitored video data are sent and centralized to the surveillance center. The surveillance experts at the centers can then intensively monitor the data in order to detect anomalies and to quickly adopt suitable countermeasures. At present, more than 600,000 cameras are installed in London (the number is estimated to be between five and six millions in the entire UK), reportedly contributing significantly to the investigation and prevention of crimes[1)].

Nevertheless, the threats caused by new types of crime are casting a shadow on the realization of safe and secure

urban life styles. These crimes are hard to deal with using the traditional surveillance systems, which cover only limited areas and depend on monitoring by humans. Their negative impact on society are not merely threats to the urban areas but should be positioned rather as threats to the entire nation. In order to deal with them effectively, it is essential to establish a mechanism that can provide prompt and finely tuned surveillance and alarm systems over wider areas with collaboration across the barriers posed by organizations, institutions and nations.

2. New Types of Threats

A recent problem in society is that some younger generation groups that have negligible relations with the wider community and come to have feelings of social alienation, have had contact with the extremist ideas of terrorist organizations, etc. They proceed under such influences to participate in violent crimes, including terrorist attacks. For example, as can be seen by the incident of the 2013 Boston Marathon in the USA, new forms of terrorism are emerging, such as "home-grown terrorism" by which a person performs a terrorist attack on persons of the same nation. The "lone wolf terrorism" by which an individual who does not belong to any organization perform a large-scale terrorist attack alone[2] also occurs. These kinds of crime are expected to continue to grow and on a global scale, backed by further growth of the Internet in the future.

What makes it difficult to take countermeasures against such new forms of terrorism is that persons who do not give the impression having criminal tendencies are often selected as the executors. If the executor is a first-time offender or a young child, the terrorist attacks can no longer be prevented by the traditional method of limiting the suspects by registering persons of interest in a blacklist and focusing on discovering such persons.

In addition, contact between the crime planner and the terrorist organization is hard to detect when it is done via the Internet. This makes it necessary for crime prevention to exercise patrolling by estimating the potential of crime based on detection of weapons and bomb preparation activities or suspicious behavior evoking crimes. However, such activities are still hard to discover and to be isolated as abnormal activities because they are often concealed under the more normal activities of people generally.

The activities of terrorist organizations are also becoming more sophisticated. For instance, in the terrorist attack on a hotel in Jakarta, Indonesia, in July 2009, it was found that the terrorists were disguised as florists who had brought the bomb through the staff entrance in advance. This was despite the fact that the hotel applied strict inspection of baggage using metal detectors at the front entrance[3].

To cope with the threats of new types of crime that are diversifying and extending into new areas as seen above it is becoming necessary to adopt advanced, flexible measures by imposing continuous surveillance and to a wider extent than hitherto in order to improve on conventional knowledge and assessments. On the other hand, considering the actual circumstances that the time and place of crimes are unknown before they occur, it is impossible to allocate unlimited costs for financing the countermeasures. Adequate consideration of the effectiveness and economy are required in order to implement new crime prevention measures.

3. Threat Countermeasures

3.1 Use of a White List

As discussed above, the traditional countermeasure generally taken against crimes has been to compile a blacklist of persons with criminal records and those suspected to belong to criminal organizations. To then discover the corresponding person early, track him or her and observe behavior in order to hinder planning or execution of a crime. As the number of persons registered in the blacklist are quite small compared to the number of unsuspected people, the surveillance based on blacklist matching at a country entrance or other screening facility has also been an extremely effective measure from the viewpoint of efficacy.

Nevertheless, some types of terrorism that cannot be prevented by blacklist matching, such as the home grown terrorist, basically require a completely new method, which is the exhaustive surveillance that can evaluate the suspicious behavior of a large and indeterminate number of persons. An example of such a method is to adopt measures based on a whitelist.

A whitelist refers to a list of persons that have proven identities and are judged to present no threat. If the whitelist listees who are the majority of persons can be identified early and be eliminated from the tracking targets, more IT resources can be assigned in observing and analyzing persons not registered in the whitelist (gray list listees). The judgment accuracy for the potential of crime may then be improved by applying finely tuned monitoring of behaviors (**Fig. 1**).

One of the simplest examples of whitelisting is to screen the targeted persons in advance and to grant a certain means of authentication (such as ID cards) to the persons passing the screening. Such persons are re-

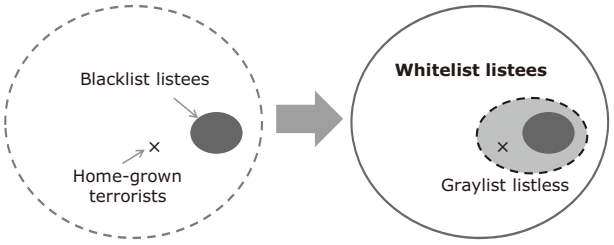

Fig. 1 From blacklist matching to whitelist matching.

quired to carry these authentication means safely (they should not be lost or stolen) and it will be registered in a list. This list can be used as a whitelist. An entrance facility that employs such a method in order to authenticate all entering persons with cards can also be regarded as a kind of whitelist type measure.

If biometrics (fingerprint or face recognition) can be applied in place of ID cards and a walk-through authentication that does not need stoppage of visitors can be combined, the active authentication procedure that forces visitors to carry ID cards at all times and to pass them over the reader at every entry and exit will not be necessary. In general, installation of authentication gates hampers the flow of people and tends to cause congestion, and the cost of installation is also high. Therefore, to take a whitelist type measure in a place with high human traffic it is desirable to implement a walk-through type authentication that does not need the installation of gates or hamper the human flow.

However, implementation of whitelist matching requires the capability of fast accurate personal authentication of whitelist listees who are much more numerous than blacklist listees. It is also essential to manage information that could lead to specification of individuals strictly by taking full consideration of the privacy issue, and to obtain the public understanding of whitelist-based crime and terrorism countermeasures by returning individual benefits to them.

In case more effective safety measures are required in addition to the whitelist type measure, the behaviors of everyone including the whitelist listees should be observed and any suspiciousness should be evaluated. As such a case does not presuppose carrying out an accurate personal authentication as described above, it is necessary to consider even the impersonation by spoofing or theft of ID cards. However, since observing the behaviors of all of the targets for a long period has a huge processing load, the procedure is not suitable for large-scale surveillance. In practice, it becomes necessary to limit the targets to only a small number of persons or to decrease the surveillance items of whitelist listees only to the most critical items.

3.2 Prediction and Precognition of Crimes

In the sci-fi movie "Minority Report" released in 2002[4], the administered society of the near future is depicted in a quite interesting way. The movie shows a society that has succeeded in preventing murder cases completely by establishing a system that identifies future murderers by using three psychics who have crime prediction capabilities and arrests the future murderers before they can actually kill their victims. It distinguishes the premeditated murders from the emotionally driven sudden murders, defining that the latter cannot be predicted until immediately before the occurrence.

In the real world, sudden incidents are also hard to predict. However, prediction of crimes is expected to be possible to a certain degree when behaviors and events that have a high probability of leading to crime plans or actual crimes or that can be interpreted as signs of such behavior can be identified. Therefore, when considering the use of IT for the prediction and prevention of crimes, the primary aim is to discover early on the specific behaviors and events that can be regarded as "signs".

Firstly, crimes with a premeditated nature can be detected in various stages. In the case of terrorist attacks, for example, it can be detected at the preparation stage, procurement of explosive materials, at the transport reservation stage, preparing temporary means of transport for crime execution, and at the crime scene previewing activities stage. In addition, purchase of objects for use as weapons, contacts with criminal organizations and viewing crime based material on the Internet can also be clues for crime sign detection. Knowledge of these typical preparatory activities and interests leading up to crimes helps in establishing a kind of crime model and enables the prediction of crimes based on such a model. Also, international conferences attended by important persons, big sports events and festivals often become the targets of terrorism. The priority should initially be put on the development of a technology that features measures to be taken at such key events. Such a strategy would support dynamic, rapid control and deployment of security resources and police activities at the event location and at its surroundings.

On the other hand, crimes that are not of a premeditated nature are hard to predict their occurrence. Crimes that are committed suddenly or with completely new modus operandi are not accumulated as previous data and consequently it is hard to develop suitable crime models. The impossibility of predicting or identifying the locations of crime occurrences means that crime prevention measures must be capable of monitoring an area as effectively as possible and of detecting any anomaly promptly. For this

purpose, we aim at monitoring multiple sites by utilizing IT methods to capture the occurrence of any new anomalies as well as any noticeable changes that might lead to anomalies. We will thereby be able to make correct predictions and judgments of the potential that these newly detected anomalies might develop into actual crimes.

What is important in this task is that the surveillance system needs to be capable of detecting a "sense of strangeness" at a level close to that which humans are capable of. The "sense of strangeness" refers to cognition of a situation slightly deviated from the usual or normal condition, or the recognition of an abnormal, uncomfortable or suspicious feeling based on it. In other words, the issue lies in how to define the scope of a "normal condition" based on the accumulation of the usual observations and to decide the degree of deviation from the normal condition that is to be judged as an "anomaly" for which an alert is issued. This can be rephrased as building a model that enables a correct judgment of the normality of an environment and the identification of anomalies that happen less frequently or that are completely new based on the model produced. This is an important concept in the detection of less-frequent events such as crimes. It is considered that technology such as "invariant analysis"[5] is applicable to the judgment of abnormality, and application of such a technology may also be possible to support the prediction and precognition of crimes in general.

The idea described above is backed by the fact that the machine learning technology essentially necessitates a large amount of learning data. It is more advantageous to be based on normal events, from which it is easy to obtain learning data, rather than on abnormal events, for which it is hard to obtain learning data. To build a system that performs automated observations of actual environments and determines whether they are normal or abnormal, it is in general required to use a machine learning technology. However, sincea satisfactory amount of learning data cannot be reserved for crimes with low occurrence frequencies, the detection accuracy of crimes may not be able to increase. It may seem to be possible to generate learning data by simulation synthesis, but the simulation of all of the possibilities related to crime itself is a hard one to achieve. Rather, it may be a more rational approach to determine the normal condition and to detect any deviation from it.

4. Considerations for Economy

4.1 System Design Emphasizing Management under Normal Conditions

Traditionally, safety orientated surveillance systems have been designed by focusing on the detection of anomalies. This has tended to make them inseparably associated with the thorny problem of how to detect "abnormal" events that hardly ever occur predictably and how to evaluate their detection accuracies correctly. However, even in a crime-ridden area, the normal period without crimes should be longer than a period for which crimes are recorded. It is often more important in the field to manage persons and things correctly for improving the efficiency of original work rather than to detect crimes and anomalies. In addition, since an anomaly is an event that is the reverse of normality, as discussed above, the potential of detecting anomalies accurately would increase if it was possible to identify normal status accurately.

Also, from the viewpoint of the return of investments spent on the system, it is not effective to design the targets and functions of the system by limiting them to only anomalies while no one knows when such events will actually happen. It is more advantageous considering the return on investment to design the system by setting its functioning in the normal condition as the main target while also providing the capability of handling emergent events (**Fig. 2**). For example, a system for the management of employees can also be used for determining people other than employees. It can serve thus for the prevention of the intrusion of outside persons. A system that can manage all of the objects in an environment can also easily detect the non-registered articles as foreign entities. It is the same with a safety system intended to ensure the security of an entire city. The system design is expected to achieve the integrated coexistence of the functions that aim at the effective management and control in the normal condition of a city and of the functions aiming at the prevention of crimes and terrorist activity that occur less frequently.

However, since the direct beneficiaries and administra-

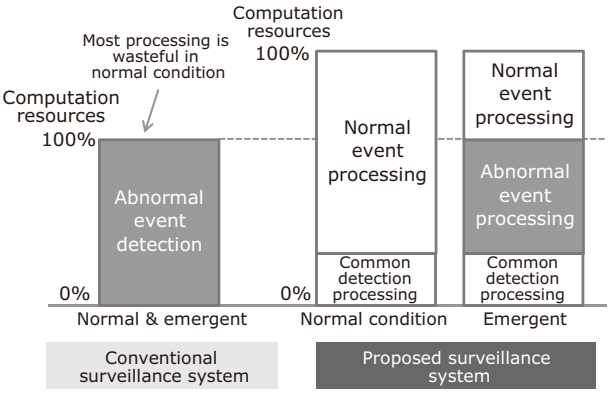

Fig. 2 System design focusing on operation under normal conditions.

tors differ between the systems for normal conditions and those for emergent conditions, the implementation of a system integrating the functions for both of these conditions involves many difficulties. Therefore, coordination between the persons occupied in the system is crucial. Particularly, information sharing across different institutions or corporations tends to produce various issues. So the system is required to provide a mechanism ensuring the proper coexistence of safety and convenience.

4.2 Management of an Entire City

To handle new types of threats such as home-grown terrorism and lone-wolf events, it is desirable to implement a surveillance system that can detect the signs of crime early by covering the main cities and key facilities. Traffic infrastructures such as roads and railways should also be covered at a level involving the entire city or nationally.

Nevertheless, if it is attempted to build such a system mainly composed of fixed-location sensors with predefined installation locations, a very large number of sensors must be installed in various locations to ensure the scope of sensing and huge installation costs are required. It is therefore more effective to create a mechanism that can cover a wider area effectively by combining fixed and mobile sensors. Mobile sensors can be implemented by installing sensors and other means of communication on automobiles and drones, but the use of sensors in mobile terminals including smartphones is also worth consideration.

Existing fixed-location sensors are also able to monitor wider areas if organizations collaborate to create a mechanism for sharing the surveillance information. But, for this purpose, various recognition and analysis technologies should be used to enable the optimum abstraction of data possessed by each organization. In this way the information required for surveillance can be shared. An example of such a procedure is a system that employs a recognition technology that converts into metadata the sensing data acquired from all organizations as structures in common and with the same degree of abstraction. Therefore, the converted data can be shared instead of sharing the original data as has been done previously (**Fig. 3**).

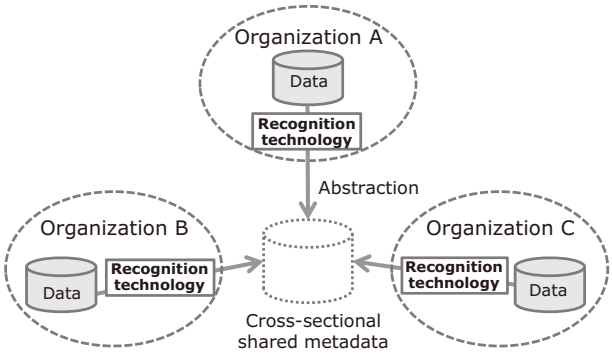

Fig. 3 Example of cross-sectional sharing of surveillance data.

5. Conclusion

In the above, we have outlined the vision of NEC with regard to surveillance solutions to support the safety and security of urban locations and we discussed the anticipated future progress of technologies and systems to support such solutions. The conventional surveillance systems that focused on visual blacklist matching have difficulty in pre-empting the new types of crime that are often committed by first-time offenders. In the future systems must be capable of dealing with the new types of crime that have been difficult to discover or predict by human effort alone. This will be achieved by applying whitelist matching that presupposes the use of abundant computation resources as well as various AI technologies. The system design concept is also expected to shift from emphasis on crime prevention to the management field under normal conditions so that systems that can create higher value will be implemented.

At NEC, we are determined to advance the development of these new technologies, systems and solutions that can support the safety and security of cities and nations worldwide and which are based on our corporate vision.

Reference

1) BBC, 5.9 million CCTV cameras in UK
http://www.bbc.co.uk/newsround/23279409
2) Wikipedia, Domestic terrorism
https://en.wikipedia.org/wiki/Domestic_terrorism
3) Wikipedia, 2009 Jakarta bombings
https://en.wikipedia.org/wiki/2009_Jakarta_bombings
4) Twentieth Century Fox Film Corporation
http://www.foxmovies.com/movies/minority-report
5) NEC, MasterScope Invariant Analyzer
http://www.nec.com/en/global/prod/masterscope/invariantanalyzer/

Authors' Profiles

HIROAKI Toshihiko
Deputy General Manager
Data Science Research Laboratories

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.11 No.1 AI & Social Value Creation - The World of "NEC the WISE" -

Vol.11 No.1
December 2016

Special Issue TOP