Dr. Rustom Kanga, *CEO*
iOmniscient Corporation

What is the IQ Rating of your Security System?

Dr. Kanga is the founder and CEO of iOmniscient Corporation, one of the leading suppliers of Intelligent Surveillance systems worldwide. In this, the first of several articles on Intelligent Surveillance, Dr. Kanga discusses a way to understand how smart your own security system is

Studies have shown that an operator watching 2 monitors misses 45% of the action after 10 minutes and after 22 minutes, he misses 95% of the action. This is in a relatively empty scene. In a busy scene it takes even less time for an operator to miss action on a screen. What are the chances that an operator watching hundreds and sometimes thousands of cameras would observe anything of use?

Organizations focused on security have realized that the very large sums of money that they have spent on cameras and control rooms provide them with little real security. The video recorders they have installed are useful after an event but have little value in preventing an incident.

Hence there has now been the growing realization that for organizations to get value from their security systems they need to add "intelligence" such that the operator will be told when an incident happens or even better, *before* it happens. The system should be able to tell him that a person has fallen down on Camera 235 or that a bag appears to have been abandoned for more than 10 minutes on Camera 650.

Now that astute users of security are recognizing that without intelligence their investments in security equipment are underutilized at best and are, at worst, useless, there is a burgeoning industry of providers of such intelligence. Suppliers who provide nothing more than simple features such as database access or motion detection, tout themselves as providing intelligence, causing significant confusion in the minds of the users. How can one tell the difference amongst hundreds and even thousands of suppliers who all purport to add intelligence to security systems?

At iOmniscient, as suppliers of Intelligent Surveillance we had the same problem. We had products which were extremely intelligent – being able to do things that humans could not do and others which were relatively simple involving trivial programming using techniques that are practiced in many universities and available in the public domain. And since the company's products covered the whole range of capabilities in the Intelligent Surveillance field we came up with an Intelligence Rating system for our own products which can of course be used more universally by users to define the intelligence of their own systems.

Categorization of 'Intelligent' Technologies

To start with there are two major classes of Intelligent Technologies - those involving Detection and those

IQ-115
Loitering

IQ-120
Counting in a Crowd

involving Identification. Detection involves observing a scene and understanding what is happening in the scene (e.g., if someone has jumped over a fence). Identification involves knowing the identity of the person (i.e., knowing that Jack Smith is the person who jumped over the fence). Note that both Detection and Identification can be used for objects other than humans. Identification for instance can be extended to vehicles using number plate recognition systems. The focus in this article is on Detection Systems.

Detection Technologies

The measurement of human IQ is based on a normalized system. The average person in the population has an IQ rating of 100. That means 50% of the population has a rating higher than 100 and the remainder has a rating below that. A similar rating system was used on "intelligent" security products. Those algorithms involving enormous complexity mimicking the human brain were classified as requiring a high IQ while other techniques that were simple to implement were deemed to have a low IQ rating.

The products were rated as having an IQ from as low as 10 to as high as 180. As one would expect in looking at the market there are many suppliers who offer the lower IQ capabilities. As the IQ rating increases the number of players in the market decreases rapidly.

At the lowest level of the scale the algorithms are based on Video Motion Detection (VMD). VMD in its simplest form consists of comparing the pixels on one image with those on the next. If there is a difference this means that there was some change in the scene usually interpreted as motion. Such systems rated at around IQ 20 are widely available but of course as the IQ rating implies they are of little value as they are prone to false alarms. Not every pixel change is due to motion. Light variations, reflections on water, shadows and a host of other changes cause the change in pixels making such systems useful only to those who want to claim their systems have intelligence while not expecting them to do anything practical.

At the next level of sophistication, systems can be set up to group the pixel changes between images as 'blobs' and to then track the movement of the blobs across the screen (IQ 60 to 100). The characteristics of the blobs (such as size or shape) can also be analyzed and the system can therefore differentiate between people and small animals or between cars and trucks. Even within an IQ level there can be many variations in technology. It is quite simple to track a single person in a relatively empty scene. As the scene gets more crowded the algorithm has to cope with blobs that merge and split. Tracking a particular person through a crowded scene can be a very complex task and not all companies who can supply a technology with this rating can necessarily cope with such scenes effectively.

Using this level of technology it is also possible to detect left objects ***in a relatively empty scene*** as this just involves noting when a blob has split and where one part of the old blob remains stationary.

The next level of capability (IQ 110) involves being able to clearly define the item that is being tracked (say people) and to be able to count them accurately. As with IQ 100 there can be wide variations in how well suppliers do counting. It depends on their ability to cope with blobs that split and merge. A good algorithm that has been professionally set up can be very accurate and iOmniscient's counting product was recently audited as providing 99.91% - higher than was possible with a human.

Once blobs have been tracked and counted, the next level of sophistication involves understanding what the blobs are actually doing. This is Behaviour Analysis. At this level of technology one can detect behaviours such as slips

and falls. Behaviour can be culturally dependent and hence not all behaviours are easy to detect using a computer system. For instance, I observed a system designed to detect fighting. It worked well in the UK. However it collapsed in Italy as it easily mistook two exuberant Italians meeting after a long separation as fighting. At this level there are less than a handful of companies that can offer a comprehensive set of good behaviour detection algorithms.

As one gets to IQ 120 the technology moves from detecting and observing individuals to operating in crowded environments. Crowd Management at this level can provide capabilities such as determining how many people are in a very crowded scene at a given time (as opposed to counting individuals passing through a gate).

Finally one gets to IQ 140 which allows the detection of abandoned objects (or removed objects) in a crowded scene*. This is useful in an environment such as an airport where luggage may be left unattended or in museums or warehouses where items may be stolen. Such systems have to cope with very long detection times. If the detection time is too low there would be thousands of nuisance alarms from passengers placing their bags down momentarily.

And with the long detection times the system has to cope with significant obscuration (where the object is obscured for a significant period of time by passersby).

Finally at IQ 180 the system has the capability to do everything that can be done at IQ 140 but it does it even when the object may be invisible to the human eye because the object is tiny and with little contrast.

Often systems will do one or the other of these detections on a camera scene. A system that can do all of them at the same time has been defined as IQ Infinity.

General characteristics that all systems must have

All systems, no matter what their intelligence level, need to have certain core characteristics. Several of these features are architectural though some do require a level of intelligence. Architectural characteristics include openness (the ability to take inputs from any camera, operate on any computer and interface with any video recording system) scalability (the ability to grow from a single camera to thousands of cameras) and distribution (the ability to place the intelligence either centrally or remotely in a network.

Intelligence characteristics include the ability to avoid nuisance alarms caused by extraneous factors such as light changes, water reflections or shadows, the ability to understand perspective and the ability to know if all the cameras can see properly and are operational (specially if the system is prone to sabotage, vandalism or just bad weather). At iOmniscient we spent a significant amount of time on just this aspect of the technology building a Nuisance Alarm Minimization System (NAMS) which used artificial intelligence to understand the cause of the alarm and hence automatically eliminate the false ones.

A very significant general characteristic of a system that would differentiate a smart system from one that is less so is the ability to 'Jump to

IQ-140
Abandoned Object in a Crowd

Event.' Most systems have the ability to set a 'pre-alarm' time and to go back a short period before the alarm. But what if one is looking at a crowded airport and sees 10 suspicious bags. A sophisticated 'Jump to Event' system can allow the user to focus on any one of those bags and with a single click of a button, see when it was brought in and by whom – even if it happened several hours before.

Moving beyond Intelligence of the Camera to Intelligence of the Network

Most systems today provide intelligence based on the view of a single camera. For instance the system can tell if a person enters a scene or leaves a bag based on a single camera view. The technology has now moved beyond that to using the intelligence gained from multiple cameras within a network to make higher level decisions. An example of this is for theme parks or airports where they may have long queues that extend beyond the view of a single camera. By collecting information from multiple cameras one can calculate the average waiting time for people in the queue.

So, what is the IQ of your system?

As users, one needs to ask oneself as to what their system is required to do. Are you, as a user, happy to have a system that is only useful after the fact to review disasters or do you prefer to have one that can help you to pre-empt them. What types of events are important to you? Can your system help you to avoid these events or in the worst case tell you instantly if one occurs. The IQ Rating system described will help you to assess the level of intelligence your system has and allows you to determine what you need.

iOmniscient Corporation has international patents on the technology that allows Non Motion Detection in crowded environments. Hence technologies at this level and above are only available from iOmniscient or its licensees. ■

Mexico City implements Intelligence

Mexico City International Airport (AICM) has just chosen to install iOmniscient's IQ Series of products to ensure it has the world's best security in its new, ultra-modern terminal. The airport is the busiest in Latin America with over 24 million passengers passing through it each year.

The requirement for the Mexican Airport is IQ-Infinity, the top of the line product in terms of intelligence. By implementing IQ-Infinity, the Mexico City Airport joins the growing list of airports in North America, Europe, Asia and Australia that have already implemented this technology.

"Based on our vast airport experience, one of the most useful features for the airport will be the system's artificial intelligence based Nuisance Alarm Minimization System (NAMS)," said Ivy Li, MD for iOmniscient's operations in the Americas.

"The key in any CCTV based system is not in just what is detected but also in knowing what to ignore so that one does not have thousands of false alarms each day."

"We were looking for a solution that would be modular, effective in areas where large crowds and heavy traffic are common, and would not be limited to a specific video management system," said Gonzalo Martinez Ulloa, CIO for Mexico's Airport Administration Agency (ASA) which is responsible for design and implementation of the technology infrastructure at the airport.