MAXIMISING POTENTIAL

Jamie Barnfield *reveals how AI can work with video to transform perimeter security*

Deep learning-based video analytics give operators the tools to better detect, verify and respond appropriately to threats

Driven in part by the pandemic, we've seen rapid innovation across the security industry in the video surveillance market. Users continue to benefit from ever higher megapixel cameras with enhanced IR and true WDR, a vast array of new and specialist models, and compression technologies that deliver better image quality in all lighting conditions and relieve burdens on storage and bandwidth.

Most reputable manufacturers now offer a range of NDAA-compliant kit, which has become a key purchasing consideration outside of the US Governments and industry bodies across the UK, EU and Australasia continue to raise awareness of the cybersecurity and privacy threats posed by Chinese tech, particularly in sectors including central and local authorities, utilities, banking and corporate enterprises.

We should not be surprised, given the reported vulnerabilities of Chinese video technology such as remote 'backdoors', the cybersecurity of video surveillance is now treated as critical, with end users keen to eliminate risks and cyber loopholes. During installation they are looking for cameras that force MFA or use mutual authentication with storage platforms to protect against spoofing and deepfakes; and multi-layered technologies, with proprietary protocols to ensure secure transmission without impacting on performance.

There's little doubt that, when it comes to the progression of video tech, deep learning-based analytics have been transformational. Today, users not only see them as crucial to providing enhanced domain awareness, but they also give operators the tools to better detect, verify, and respond to threats. They also proving to be a force multiplier for operational efficiency at a time when labour shortages are acute across many Western economies.

Traditional Binary Large OBject (BLOB) technology analytics are now a de facto expectation on modern network cameras, and undoubtedly remain an important feature of many surveillance operations. Motion detection, for example, particularly out-of-hours and for low traffic areas of buildings, helps keep recording to a minimum. Trip zones and line cross features were designed to defend perimeters, yet many users find they are prone to false positive alerts caused by harmless environmental factors.

The larger the perimeter the bigger the problem. Unnecessary and time-consuming officer dispatch soon becomes operationally inefficient and can delay response times to real threats, particularly across extensive sites. Once control rooms become overwhelmed, operators are tempted to switch off analytics features on troublesome cameras or shut down alarms without investigating, which means they risk missing potential threats and incidents.

Alarm receiving centres typically increase charges for more frequent call outs and there's a risk they may withdraw monitoring services from problematic sites until cameras are re-configured or replaced. This can result in organisations needing to draft in additional security officers, to maintain protection, or risk leaving gaps in security.

THE ANSWER

Server and NVR-based architecture already has the computational power to utilise the most advanced deep-learning algorithms. These systems can satisfy most customer demands for intelligent analytics and deliver upgrades quickly. And these architectures remain a top choice, especially for outdoor environments where systems need to cope with varying light, weather and animals and where users can set limits on what is relevant, to eliminate the risks of latency and a backlog of data.

Yet today, processors inside edge AI cameras are powerful enough to run computing processing with artificial intelligence locally, while still encoding and streaming without the need or cost of upgrading software. Edge AI cameras are now becoming widely available and more cost-effective with 5MP domes and bullets that are able to deliver the intelligence and accuracy that users need. Once organisations are ready to upgrade, adopting edge cameras will mean greater flexibility, faster insights and better security, while overcoming bandwidth constraints and storage burdens.

But whatever AI mode organisations choose, customers can attain improved visual awareness across their entire estates, with highly accurate notifications for intrusion, object, loitering, license plate recognition and unusual event detection. Security operators can better manage everyday events and respond to more serious threats and emergencies. In short, security is enhanced by better and faster detection, verification and responses.

Unlike human brains, deep-learning algorithms don't get tired. They can constantly monitor multiple camera streams in search of suspicious behaviour, maintaining performance levels even in busy scenes. Relying on human operators to monitor multiple cameras means hiring enough staff to cope and allowing for regular breaks to ensure they stay alert, or outsourcing surveillance operations to third-party monitoring services.

Using AI-assisted notifications can free-up operators from having to constantly monitor multiple streams and video walls. Instead, they can respond quickly and flexibly, and not just from the control room. They can configure alarms to be received to client software and on mobile devices, giving the ability to detect, verify and respond to events on the move.

Improving the ability of security officers and managers to oversee security operations away from the control room – by giving them more accurate information, at the right time, along with powerful VMS functionality and tools – lets them better manage and coordinate incidents on the ground.

We're also seeing AI used beyond perimeters to provide a strengthened first layer of security. In the US and UK, many large schools and university campuses position cameras located some distance from the line of demarcation, such as at road junctions and traffic lights. This can help schools detect, identify and take appropriate action against known perpetrators before they reach campus boundaries, and supports better collaboration with the local police and public agencies. Intelligent analytics such as license plate recognition, line cross, object and loitering detection are proving to be valuable tools for campus police departments and their security teams, providing earlier and accurate alerts to threats to support faster escalation to evacuations and area lockdowns.

EDGE AI CAMERAS ARE NOW BECOMING WIDELY AVAILABLE AND MORE COST-EFFECTIVE

Highly accurate, AI-powered license plate recognition is also helping schools prevent unauthorised access, while at the same time improving efficiency by automating entry and exit into car parks and ensuring teachers and students have allocated spaces.

Deep learning and intelligent video analytics capture metadata even when analytics rules are not applied, meaning that users can benefit from advanced searches across single or multiple camera streams, including across large and dispersed estates.

By classifying people and vehicles, including the numbers of vehicles and people in each scene, as well as the colours and shapes, faster search and retrieval of footage is possible. In cases where time is of critical importance, such as where suspects need to be found and apprehended, this ability can make a crucial difference. For example, based on eyewitness reports operators can search for relevant video footage more quickly. Further, they can track the target's movements and pinpoint their last-known positions from the vast amounts of video data and do so in minutes rather than hours or even days.

Deep-learning algorithms also extract and record the appearance characteristics of people, providing a powerful person match capability that can find a person of interest or suspect. This improved detection capability allows security teams to be more proactive, identifying unusual behaviour and intervening to prevent crime and reduce losses.

In critical infrastructure and corporate enterprise environments, the insider threat is an ever-present risk. By integrating access control systems, security teams can be alerted by an employee acting suspiciously, for example entering facilities out of hours, during planned holidays or trying to access restricted areas. When the image of a person of interest is selected, deep learning algorithms rapidly scan vast amounts of video data by user-specified time and date to present and collate the

Picture credit: IDIS

closest matches. This can help security teams monitor employee behaviour and work with HR departments to intervene before a security breach occurs.

Designed for continuous evolution, deep-learning analytics need to keep pace with future technological developments and ever-evolving threats. One example is the largest and most significant surveillance upgrade of 2021 in South Korea to secure army garrison perimeters with advanced surveillance and analytics capabilities. As part of the Republic of Korean Armed (ROK) Forces Defence Reform, four military bases are currently deploying over 5,500 5MP cameras that utilise IDIS Deep Learning Analytics including object and intruder detection as well as intelligent, real-time auto-tracking. In collaboration with IDIS, the ROK is exploring custom analytics such as fight detection, that will alert control room operators as well as designated personnel to any potential disturbances on the perimeter.

SERVER AND NVR-BASED ARCHITECTURE HAS THE POWER TO USE DEEP LEARNING ALGORITHMS

Users are also finding new applications for analytics functions developed for the pandemic, such as people counting and occupancy monitoring. Airports are now using the same technology to prevent bottlenecks and improve passenger throughput. These may not be obvious security applications, yet the smooth running of airports is critical to national economies and the post-pandemic bounce back of leisure and business travel.

Facilities managers are realising the benefits of heatmapping and occupancy monitoring for planning future building usage, which will be strategic to ensuring welcoming, inclusive working environments where staff are likely to stay and where new talent will want to work. By looking at day-to-day and seasonal trends they now have the actionable insights to ensure staff have enough meeting rooms, collaborative workspaces and hot desks, while understanding peaks and troughs makes it possible to reduce energy consumption when fewer staff are using facilities.

The same is true for facial recognition. Deployed to ensure hygienic, touchless and frictionless access into facilities and to support flexible and hybrid working, it's also being used to provide more secure yet flexible access to meeting rooms, workspaces and hot desks for staff and contractors. In turn, eliminating the common vulnerabilities of lost or borrowed ID badges and tailgating.

Integration with Microsoft Active Directory goes a step further as it provides the backbone of many organisations' identity management. Once staff decide to leave an organisation their access to corporate networks and applications is usually automatically revoked. Yet HR and department heads often forget to instruct security teams to off-board employees and contractors from access control databases presenting the risk of disgruntled personnel gaining access to facilities, expensive assets and sensitive information. Integration of security tech with centralised databases not only strengthens security, it eliminates the inefficiencies and cost of siloed systems and technology stacks as well as manual and repetitive processes.

We are reaching a tipping point in AI video analytics adoption, but we are not stopping here: as threats evolve and operational requirements change, we're already developing future AI functionality to tackle those challenges and make security as frictionless as possible, and even more resilient ●

Jamie Barnfield is Senior Sales Director at IDIS Europe

Using AI-assisted notifications frees-up operators from having to constantly monitor multiple streams

Picture credit: IDIS