Biometric ID

Facial Recognition: Capitalize on the Information Coming In

Security environment can make better use of information by employing best-of-breed technologies in facial recognition.

Traditionally, facial recognition deployed as a stand-alone security and surveillance identification tool in involuntary, passive environments, such as airports and public locations, has been arguably unreliable and ineffective. As an industry, security and surveillance generally has moved away from using a single facial recognition technology as an independent security sub-system for ad-hoc identification, toward systems that employ multiple overlays of best-of-breed facial recognition technology in broader, more useful integrated converged environments, by sharing of common information and functionality. This approach improves not only the potential opportunity for valid identification, but also the actual value of the information of who, what and where has been or is being identified, thus providing significant economies in time and monies invested. With the digitization of this security and surveillance environment, the foundation has been set to take advantage of new converged technologies on the horizon including enhancements in facial recognition.

By James Moore

REACTIVE VS. PROACTIVE SOLUTIONS

In the past, facial recognition systems have been designed as reactive vs. proactive solutions. By combining and employing facial recognition in proactive involuntary and voluntary converged security and surveillance environments, the accuracy and value of identification becomes much more useful. To be effective, this converged approach should reach across people, systems, and technology enabling

enterprises to detect, record, isolate and respond to, any type of security event or incident.

In the security, surveillance and risk management world, information is the currency for any security related department to operate efficiently. The need created is for risk management environments, to pull real-time information together in order to be able to defend itself based on identified persons of interest and their respective activities. This extends across any risk managed environment from corporate security, casinos, retail and a like. When you move into a converged system environment, you are able to capitalize on the information that is coming in, from a variety of sources including facial recognition and use it efficiently. This in itself becomes a return on investment by reducing administration overheads.

Modern security practices have evolved from a compartmentalized approach toward a structured orderly 'Best Practice'/ Standard Operating Procedure based operational structure. The key to achieving this is a centralized information management system providing a unified system for security information, subject identification and reporting in a secure manner from multiple sources.

The information collected on a day-to-day basis has tangible value in protecting staff, patrons, the public and assets. However, to realize this value and use the information effectively it must be:

- Accurate
- Timely
- Consistent
- Subject to audit
- Rapidly retrievable
- Subject to logical work flow
- Secure

As discussed, key elements of the security management infrastructure may include:

- Intelligence gathering systems
- Investigative and reporting systems
- Subject Databases
- Employee information
- Dispatch operations
- Information dissemination systems / Interdepartmental communication
- Risk Management Systems
- Best Practices and Standard Operating Processes
- Data Analysis systems
- Visitor Management Systems
- Employee badging systems
- Access control Systems
- CCTV Surveillance Systems
- CCTV Recognition technology
- Fire Systems

PROACTIVE FACIAL RECOGNITION

By employing multiple facial recognition technologies as part of this integrated converged environment, it offers an additional tool that delivers an active vs. passive real-time security and surveillance

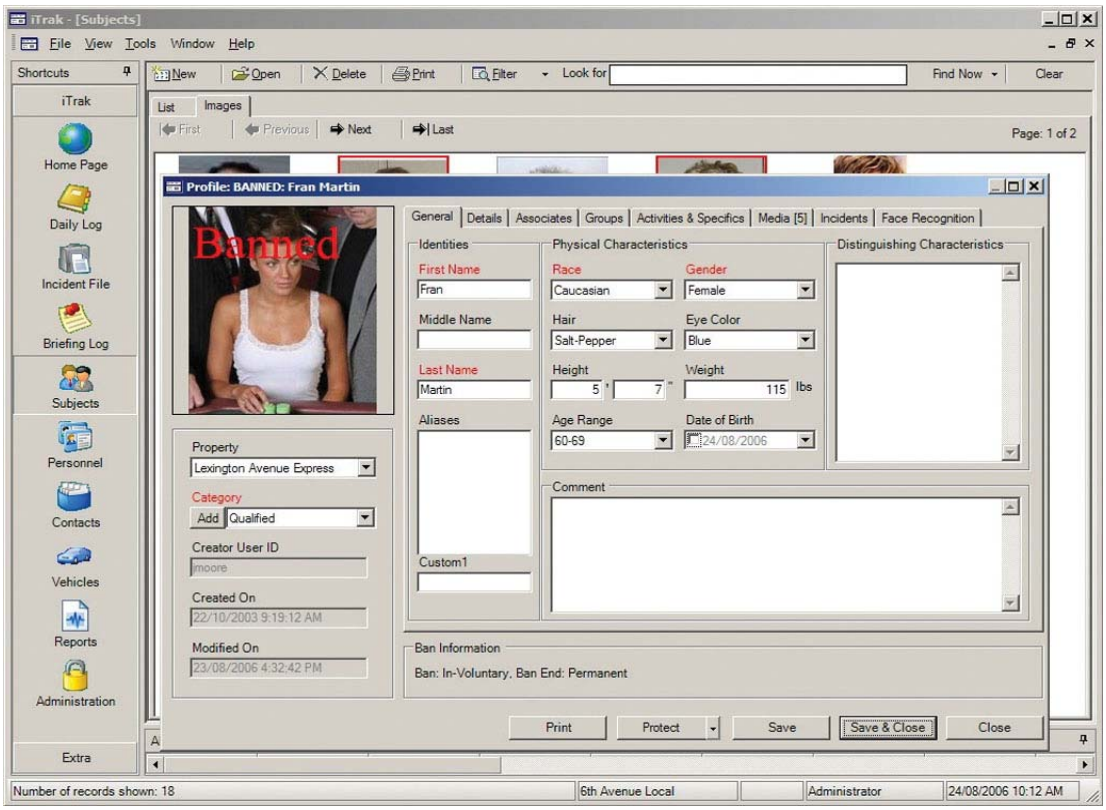
identification solution, providing event driven identification on selected individuals under watch or excluded status. This biometric solution replaces manual systems such as operator comparison of surveillance subjects to 'mug' books.

An example of movement to proactive use of facial recognition technologies can be seen in the casino responsible gaming environment. As the gaming industry becomes more accountable, social responsibility also becomes a key corporate responsibility; ensuring patrons are voluntarily enrolling and excluding themselves from play at casino properties. By enlisting their cooperation at the time of self-exclusion, the casino is not only enhancing the quality of facial recognition enrollments, but also potentially mitigating the risk by employing a series of self-exclusion best practices and a standard duty of care with patrons. By demonstrating this commitment, standardizing data collection, normalizing patron interaction and employing all reasonable efforts, casinos are potentially better able to manage the associated risks such as insurance, litigation and poor customer service.

BREAKTHROUGH IN FACIAL RECOGNITION

As facial recognition technologies evolve, enhanced methods of identification are being augmented and overlaid, including technologies employing different light wavelength analysis, pattern and behavioral models. These improvements by themselves may improve accuracy of facial recognition systems, but as part of a complete converged platform and employed as overlaid best-of-breed solutions.

By tying multiple overlaying best-of-breed facial recognition technologies into a converged incident management system, a company has access to a better complete overview of a customer's or individual's company experience, from a history of interaction with the company such as play history, self-exclusions, incident history, and so on.



Personnel module (Photo by iView Systems)

THE BIG PICTURE

Security and surveillance professionals in today's high technology gaming, banking & retail environments are faced with handling and processing vast amounts of both real-time and recorded video information from hundreds or thousands of cameras. Combined with their existing security, auditing and investigation workload, the task of identifying banned/self-excluded patrons, shoplifters, gang members and other undesirables becomes practically impossible.

Typically, security and surveillance environments will not have enough operators on shift to watch every camera at all times. Facial recognition systems act as additional 'eyes' allowing existing cameras to be configured as 'face ready'. Any individual that appears in front of these live cameras is automatically run through the existing enrolled subject database. If a match of a certain confidence level is made, then an alert is sent to an operator's desktop also displaying the next closest matches with details such as camera, time, and subject information. These systems automate and enhance the subject database search, instantly narrowing down possible subjects from 1000's to several individuals in seconds.

Single desktop facial recognition systems can also be configured to capture a 'Biometric Face Log' of patrons over a period of time. This log provides instant access by time, date and camera name to store faces that have been isolated and tracked by the system. Historical images can then be enrolled directly from the face log, based on missed, active criminal or selected activities, thereby potentially identifying the same individuals in the future who have been involved in historical incidents.

As no facial recognition system is perfect and simply another tool augmenting the existing security and surveillance environment, the integrated converged systems enhance security by providing a degree of automation in identifying subjects. However, it should be stressed that the system may not identify subjects who will fully disguise their appearance to avoid detection. Because face recognition deals in probabilities rather than absolute certainties, operators must exercise the final decision to determine the identities of individuals that the system matches.

Integrated into an investigation and subject management system, this information provides the ability to not only manage existing risk, but also better deploy personnel and isolate potential problem locations, subjects and incidents (i.e., slip & falls, assaults, etc.) before they occur. Ultimately these linked systems, including facial recognition, will provide better analysis of incidents and subjects, while delivering more accurate occurrence statistics and better analysis of risk trends. This information will enable refinement of policies, procedures and staff deployment to efficiently address current and future criminal or risk managed issues. Integration has enabled a high degree of centralization of security information and automation to create a transparent seamless security infrastructure. Systems integration of access control, CCTV and intrusion technology is now standard, providing automated control of security and resulting improvements in operational efficiency. In terms of natural integration of additional systems such as visitor management, opportunities exist by virtue of common information requirements in the aforementioned access control, Human Resource Management (HRM) and incident management systems.

As most advanced access control systems and incident management systems already interface with HRM systems, it makes technical and operational sense to integrate the visitor management functions with one or both of these systems. In turn by the overlay of best-of-breed facial recognition systems, enrolled individuals that attempt to visit a site, where they were potentially previously employed, banned,

or otherwise involved, can now be identified, reviewed and dealt with efficiently.

Using an incident management system as a platform for best-of-breed facial recognition integration is relatively new in the industry, but one which is logical to the overall security infrastructure of many industries, notably in casino, retail and many other risk management security markets.

By employing multiple overlays of best-of-breed technologies in facial recognition and integrating these into a converged reporting platform, security, surveillance and safety environments are able to make better use of information and outcomes. This provides measurable and dramatic efficiency improvements in security and risk data collection, with real-time subject identification and access, while providing a centralized view of all security related incident history.

James Moore is Vice President of iView Systems (www.iviewsystems.com).

Close