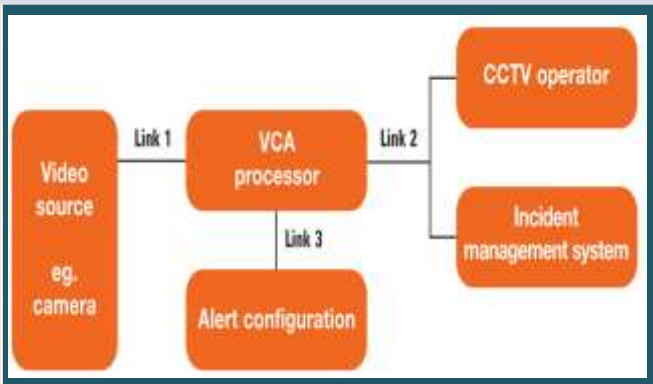
2015

CCTV Based People Screening



Homeland Security Research Corp.

CCTV Based People Screening – 2015

August 2015

Washington D.C. 20004, 601 Pennsylvania Ave., NW Suite 900,
Tel: 202-455-0966, info@hsrc.biz, www.homelandsecurityresearch.com

Table of Contents

1. Appendix E: CCTV Based People Screening

Most airports, secured facilities and business-related video monitoring systems are actively monitored by security personnel in a centralized setting, remotely monitored, streamed via the Internet to a monitoring station or passively taped for future viewing if needed (such as in the event of a bank robbery). Relatively new features in video monitoring such as night vision cameras, computer assisted operations and motion detectors that allow an operator to instruct a system to go on “red alert” when anything moves in view of the cameras, considerably enhance its power and scope. Infrared (IR) high sensitivity equipment and monitoring systems operate outside of the visible light spectrum.

Examples include Forward Looking Infrared imaging that is able to detect activity behind walls and infrared thermal imaging cameras that are able to detect activities in darkness. Local law enforcement and police use motion-activated IR thermal imaging monitoring cameras along the U.S.-Mexican border. According to INS officials, IR cameras detect the invisible infrared energy that all people and objects emit and can “see” better than the naked eye at night and in bad weather. Since the energy being sensed is heat and not light, thermal images can be used in both daytime and nighttime operations. The INS uses the cameras primarily at night to detect suspects crossing the border. Another use of IR thermal imaging cameras is to assist night search and rescue missions by both civil and military personnel.

New models of video cameras are equipped with bulletproof casings and automated self defense mechanisms to protect lenses. Picture clarity is equal to that of a compact disk - many cameras are able to read a cigarette package label at a hundred meters. Cameras are also becoming smaller, making it easier to conceal the equipment. A video camera can be hidden almost anywhere. These little devices are capable of zooming in on the smallest of details and can pan and tilt. Equipment costs have decreased to the point where a business might recoup its investment by cutting losses due to theft or by discouraging unproductive workers down time.

Also, the threat of industrial espionage has prompted many companies to resort to video monitoring. Video technology converges with sophisticated software, capable of recognizing facial features automatically, analyzing crowd behavior, and scanning the area between skin surface and clothes. The advent of new biometric software technologies, especially computerized biometric face recognition used in conjunction with video monitoring systems can facilitate law enforcement’s ability to identify suspected terrorists. Law enforcement can compare the captured images against national and international databases.

1.1. Fused Video Monitoring and Biometrics

Biometrics is a term that applies to the many ways in which human beings can be identified by unique aspects of the body. Fingerprints are the most commonly known biometric identifier. Other biometric identifiers include hand prints, vein dimensions, iris (eye) designs, the pattern of blood vessels in the retina, body odors, characteristic and unique movements, individual voices, and of course DNA. Countries around the world are implementing biometric monitoring procedures. For example, Spain has begun a national fingerprint system to track recipients of unemployment benefits and healthcare entitlements.

The technical definition of a biometric is "any measurable, robust, distinctive, physical characteristic or personal trait of an individual that can be used to identify, or verify the claimed identity of that individual." Every biometric system contains three components:

- Enrollment – the process of collecting biometric samples.
- Templates – the data that represents the enrollee's biometric located in a database.
- Matching – the process of comparing a submitted sample against one (verifying) or many (identifying) templates in the database.

1.2. CCTV Biometric Face Recognition Identification vs. Verification

Biometric identification or verification systems are distinct from each other. Facial recognition identification systems are being combined with video monitoring to identify suspected terrorists in airports and at border crossings. Combined biometric verification systems and video are used to control access to computers, secured areas and to verify passport information or citizenship status. When biometric face recognition technology is used to identify an individual, the system attempts to answer the question "Who is John Doe?" by reading the information or sample provided and comparing it to many templates in the database. It then reports or estimates on the person's identity. When the technology is asked to verify someone, the system is asked "Is this John Doe?" The system compares the biometric information presented to the template in the database identified as John Doe and either accepts or rejects the claim.

Templates in a biometric face recognition database typically are composed of complex, programmed, knowledge rules, statistical decision rules, neural networks and algorithms.

This means that the database is built using certain assumptions that introduce the potential for errors. In other words, biometric face recognition database templates do not contain exact likenesses of individuals but rather complex statistical and mathematical estimates of digitized images.

1.3. Performance of CCTV Based Biometric Recognition Technologies

Since identification and verification systems are different, so too are the performance procedures and protocols used to evaluate the efficacy of each type of system. For identification systems, the principal measure "equals the rate of queries in which the correct answer can be found in the top few matches." In other words, the higher the score of a correct match contained within the top matches, the better the system.

Thus, if used to attempt to capture terrorists in public places, the data input would be an image captured on video and the output from the database would be a list of top matches. The sheriff or airport security guard would make a subjective decision to further search or detain the individual.

Two error statistics, false-reject rate and false-alarm rate are used to measure the ability of a verification system. "A false reject occurs when a system rejects a valid identity (i.e., the real Michelle Kwan is denied access to the Olympic skating rink); a false alarm occurs when a system incorrectly accepts an identity."

In general, experts and researchers report that face recognition algorithms are sensitive to changes, such as shifting sunlight during the day and changes in facial positions. A systems' performance will drop significantly if the algorithms are not corrected to address lighting variations and moving faces.

The recent use of biometric face recognition technology at the Super Bowl is a good example of law enforcement's use of these emerging technologies and the debate over potential misuse. The faces of over 100,000 fans entering the stadium to watch the Super Bowl in Tampa, Florida were recorded by local law enforcement on video cameras. The facial images were then digitized by sophisticated software and checked electronically against a watch list database. Fans were not aware that this had occurred until after it was reported in the media. Law enforcement officials maintained that they were using the latest available security tool and that it was no more intrusive than a video camera in a convenience store.

The narrow accuracy range of the technology also raises concerns about false identification. A recent study by the National Institute of Standards and Technology found that when digitized posed photos of the same person taken 18 months apart were compared, they triggered a false rejection by computers 43% of the time. With such a large potential error, law enforcement relying solely on these technologies to identify individuals might often stop and question an innocent person instead of a possible terror suspect.

1.4. Tag and Track – Intelligent Video Surveillance

Intelligent video surveillance is an outgrowth of the basic video surveillance technology that has become quite ubiquitous in every public setting including city centers, transportation hubs, airports, stadiums, and shopping malls. This technology allows the operators to tag and track multiple "early suspects" - people who exhibited some type of behavior that attracted the operator's attention or other technical and/or behavioral screeners. The software application detects erratic behavior, entry into restricted areas, unattended luggage and other potential threats, tags them and alerts the operator to track them and further assess their level of threat using additional sensors and decision making algorithms (including human assessment).

1.5. TSA Advanced Video Surveillance Program

TSA partners with airport authorities to acquire surveillance capabilities by enhancing the airport's current/existing surveillance system with additional equipment necessary to achieve TSA's security and recording requirements at passenger checkpoints and checked baggage areas.

These closed circuit surveillance systems are an integral component in both TSA and airport operations providing value in terms of threat detection, personnel and facility security, loss prevention, emergency response, risk mitigation, employee performance, and other legal and investigative purposes. Remote monitoring enables TSOs to detect and prevent the placement or transport of explosives/devices and other threats by increasing situational awareness of activities occurring in critical airport locations.

Additionally, these partnerships promote sharing of information between federal and local authorities and provide an invaluable source of data for command and control coordination as well as for first responders dealing with an incident or threat.

TSA will provide approximately $8 million in ARRA funding to the Advanced Surveillance Program (ASP). This funding will be awarded to five airport authorities through project awards for facility modification projects to support the implementation of advanced surveillance.

More Information can be found at:
Global Video Analytics, ISR & Intelligent Video Surveillance Market – 2015-2020