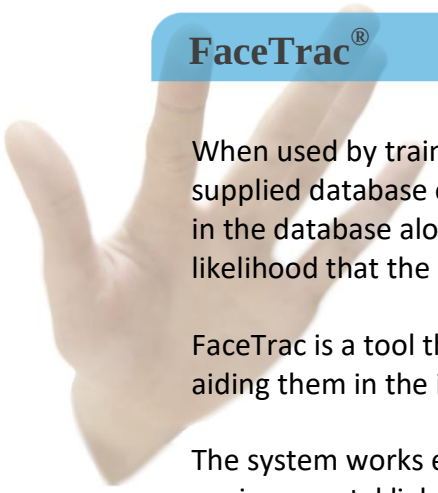
Securlinx

FaceTrac®



When used by trained security personnel, FaceTrac compares a person's face to a customer-supplied database of persons of interest and returns an ordered list of the most likely matches in the database along with a customizable numeric or color-coded score reflecting the likelihood that the person in question is indeed among the persons of interest in the database.

FaceTrac is a tool that greatly increases the productivity of your existing security personnel by aiding them in the identification of subjects that are on a particular "watch list".

The system works extremely well where individuals must pass through a central point where environmental lighting conditions are stable and/or predictable (metal detectors and doorways for example) or in surveillance-rich environments where multiple cameras can be used to get a high-quality image of a person's face (casinos, lobbies, airport terminals, etc.).

This process harnesses technology to perform a task with which human beings have great difficulty (memorizing the faces of large groups of people unfamiliar to a security officer) and converts the task into a problem that human beings are very good at solving (determining whether a person in one photo is the same person currently under the officer's scrutiny).

Threat Scenarios
FaceTrac has been designed for and tested in the following threat scenarios:

Hospitals, Courthouses and Other Public Buildings
Many publicly accessible healthcare, government and commercial buildings utilize surveillance cameras, magnetometers and/or require photo identification for entry into the facility. Some of these facilities have a list of potentially dangerous individuals whom they wish to deter from entering. Examples include:

- Individuals who have made threats against judges, jurors or witnesses
- Individuals under restraining order
- Shoplifters
- Disgruntled employees
- Known criminals or persons of interest

Images of these individuals are loaded into the database. When identified by the system upon attempted entry into the facility, alarms and alerts are generated. The database also facilitates the addition of images of individuals wanted by local, state or federal law enforcement agencies.

FaceTrac was installed in the Dirksen Federal Building in Chicago, IL and the Lloyd D. George Federal Building in Las Vegas, Nevada for 4 week trials.

Airports

FaceTrac can be used at security checkpoints in a similar fashion to the case outlined above. The database is populated with multi-jurisdictional law enforcement agency watch lists.

Sports Arenas and Other Event Venues

The system has been deployed in beta-tests at Raymond James Stadium in Tampa, FL for the NFL Championship Game in 2001. It was also tested at the Winter Olympics in 2002 at the E Center in West Valley, Utah. In both instances, multi-jurisdictional law enforcement agencies utilized the system to scan entrants into the events for comparison to their watch lists for persons of interest.

Retail

The system has been tested in a major retail department store in Boston, MA. In this application the retailer had a database of previously detained shoplifters who were released under the condition that they not re-enter the store. FaceTrac was incorporated into their existing surveillance system to identify any such individuals as they entered the premises.

Operation Activities

Installation of a system in conjunction with a screening device entails the mounting of a video camera on the entry portal and the placement of a digital scanner near the entry point. Both of these peripherals are connected to a standard desktop computer system or virtual machine. The FaceTrac database or watch list is populated with digital images provided by the user. The images are enrolled in the facial recognition provider's algorithm. In this live condition, the video camera extracts an image of each individual as they approach the portal. This image is then compared with all targets in the watch list. A positive identification will generate an alert for the security personnel at the station. They will then intervene as per their defined policy and procedure. ID management using a standard photo ID can be added to the system's capabilities. Simultaneously, an image and name can be extracted from the individual's photo ID and this data is also compared to the watch list for added probability of generating a match. If the individual is not recognized by the system as matching a target in the database, the system is passive and no information is retained in the database.

In a scenario where both friendly and threatening individuals are included, the system can be programmed to acknowledge a "safe" entrant and retain a record of that interaction while generating alerts and alarms upon detection of a "threat". In every case, the final decision and action plan is initiated and executed by trained security personnel.

FaceTrac requires the use of an embedded facial recognition biometric service provider (BSP) application programming interface (API). Currently the system is compatible with API's from Safran, AcSys Biometrics, Omni Perception and Cognitec. All other camera and computer hardware and software are commercially available.