



IDENTIFICATION MATCH

Facial Recognition System



Technical Specifications

Powered by



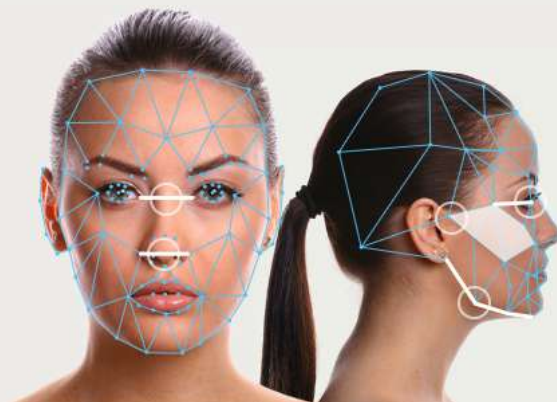
Today, technology such as social media, television and other more specialised communication networks play a more influential role in the recognition process. Advancements in artificial intelligence and biometric technology, including the development of Machine Learning capabilities, have led to increased accuracy, accessibility and the widespread use of computerised facial recognition. The significance of this means that facial recognition can occur on an even larger scale and in more challenging environments.

Security and Safety Applications

The idea behind all facial recognition technologies is broadly the same: you start with an image of a person's face (ideally a high quality one, although machine learning means that to a point we can now even use video without reducing accuracy). A fully front facing image is best, think a passport photo, but machine learning and new software has made this more flexible.

An algorithm converts this image into a numeric template, which cannot be converted back to an image and so represents a secure one way system. Every numeric template is different, even if it started out as an image of the same person, although templates from the same person are more similar than templates from different people.

What happens next sounds simple although the technology is extremely complex: templates of people's faces are taken in real time and compared to those in the database. The technology identifies individuals by matching the numeric template of their face with all the templates saved in a database in a matter of seconds or milliseconds. To put this into perspective, imagine you are at the turnstiles of a busy train station looking for a person on the run.

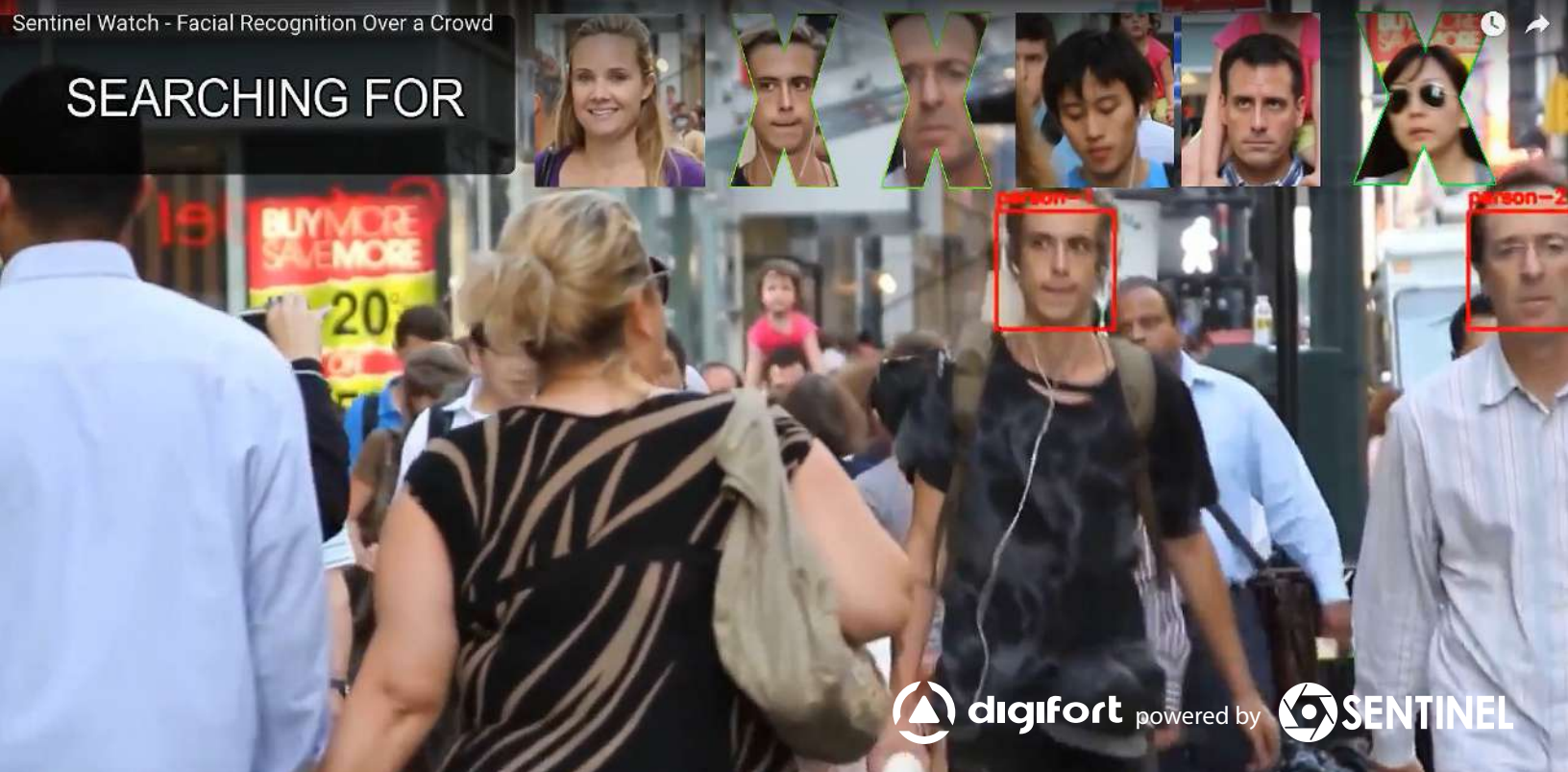


Colour image

Infrared image



SEARCHING FOR



Digifort facial recognition provides a solution for facial biometrics able to identify and record in real time, the presence of individuals previously registered in a database, moving in front of one of the cameras connected to the system. Optionally, each detection unregistered in the database, it may be stored for further analysis and possible enlistment.

The main features of the solution are:

- Facial recognition in real time.
- Facial recognition algorithms allow recognition art very under precise posture variations, changes in lighting and facial features (beard, hair, glasses, etc.).
- Scalable system. It works with multiple types of camera.
- Web interface monitoring with alerts and sound in real time. This gives the option of accessing information from any point connected to the system network (credentialed Suitable).
- Real-time notifications (emails, SMS, mobile notifications)
- Registration of individuals through mobile application, previously captured images, analysis video or recorded events from earlier in the system.
- Possibility of having whitelist (for detection of authorized users) and Blacklist (Searched / unwanted individuals).

“ Facial recognition technology would be able to identify that person should they pass in view of a CCTV camera, as well as notify the police of any additional persons of interest, whether they are a known terrorist or missing vulnerable person on an entirely separate watch list.

Because of technical progression, facial recognition can now be used in a variety of governmental and commercial environments, from identifying barred hooligans attempting entry at a football stadium or helping self-excluded gamblers at casino to overcome addiction.



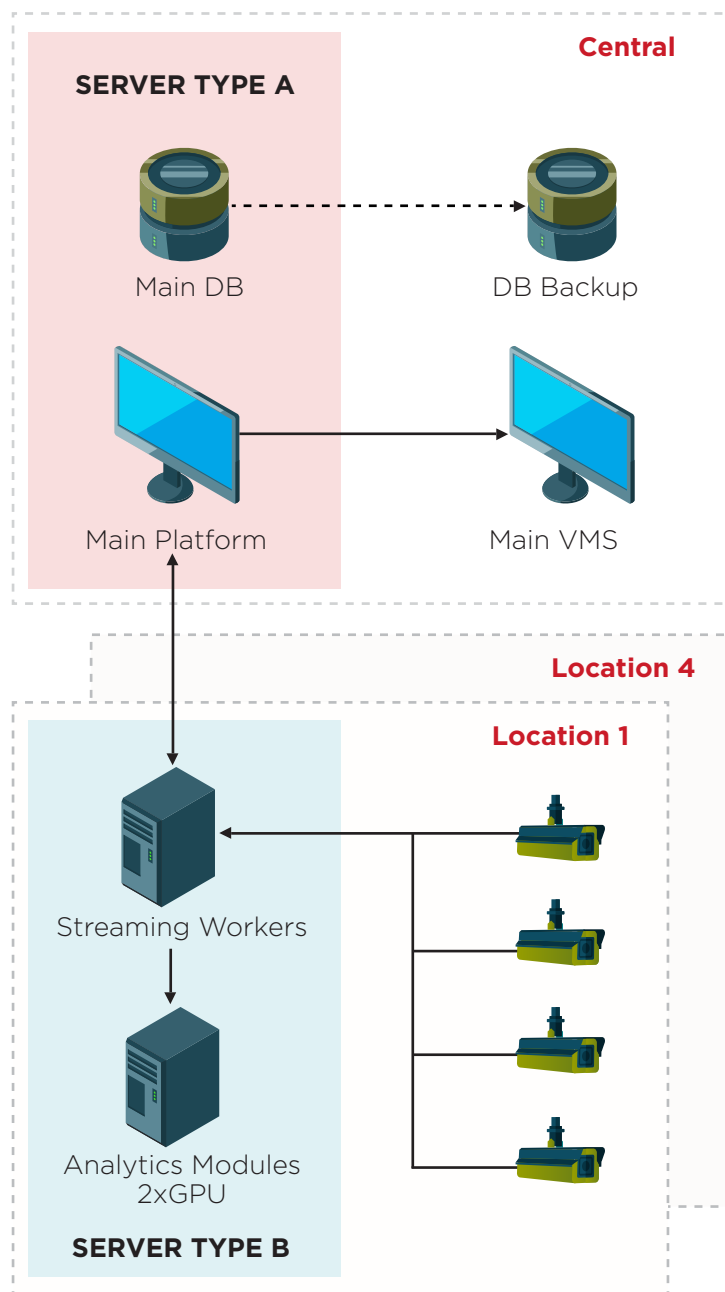
HARDWARE SPECIFICATIONS

System Architecture

Digifort facial recognition is designed by modules that can be installed on one or more servers. Modules main ones are:

- **Server :** API and web interface serves System
- **Analytics Worker :** detection and face recognition
- **Streaming Worker :** processing video stream from the VMS or direct from cameras
- **Database :** Database choice: Postgres (recommended), mysql

In the most general case Digifort facial recognition operates as a distributed architecture that streams video of cameras are processed by Monitoring Servers installed on site. These servers monitoring modules are composed of management of the video stream (streaming workers) and a analysis module (module analytics). Additionally a central server contains the platform main and common display interface and configuration. The information registered individuals and events generated can be stored in a common database between different locations.



The database system (individuals and / or events) may be shared between Different places.

Cameras

The primary requirement regarding the specifications of the camera is the minimum size (in pixels) face captured. To meet this requirement two factors come into play:

- **Hardware Specifications Camera:** Resolution, fps (frames per second) and type sensor.
- **Camera positioning** relative to the area of interest to be monitored.
- **Minimum face size:** 96 x 96 pixels.
- **Minimum resolution:** 1080p camera and 2MP (2 megapixels).
- **Sensor:** minimum size of 1/3 " (progressive), RGB (color) minimum capture frequency: 10 fps.



Server

Server type A, you are responsible for running the web interface and visualization and configuration coordinate monitoring servers besides the management database of individuals and events. The technical specifications are:

Type A: Database Server / Main Platform Server

| |
|---------------------------------------|
| Intel - Core i7-8700K 4.2GHz Xeon |
| 32GB (4 x 8GB) DDR4-3200 Memory |
| 10TB 3.5 "7200RPM Hard Drive Internal |
| Linux OS Ubuntu 16.04 |

One or more servers monitor (type B) will be installed at each location, depending on the number of cameras to monitor. These servers require great computing capacity so include dedicated graphics cards. The technical specifications of these servers are summarized in the following table:

Type B: Main Analytics Server

| |
|--|
| 2 x Intel Xeon Processor 5115 Gold 10-core 2.40GHz 13.75MB Cache (85W) |
| 12 x 4GB PC4-19200 2400MHz DDR4 ECC Registered DIMM |
| 10.0TB SATA 6.0Gb / s 7200RPM - 3.5 "- Seagate Exos X10 Series (Helium) (512e) |
| Intel C621 Chipset - 4U / Tower GPU Server - Dual 10-Gigabit Ethernet |
| Linux OS Ubuntu 16.04 |
| 2200W Redundant Power Supply |
| 4 x PNY NVIDIA GeForce 1070 GTX 8GB GDDR5 (1xDVI, 1xHDMI, 3xDP) |
| LG 24x Super Multi DVD +/- RW with M-DISC (SATA) |

Server capacity type B is 20 2MP camera for face size 200 px. Smaller configurations can be designed for fewer cameras



Connectivity Requirements

Synchronization database shared between locations and real-time notifications require monitoring servers count with a broadband connection standard between different locations. Requiring notifications outside the internal network, you must have Internet connectivity to the outside.

Warranty

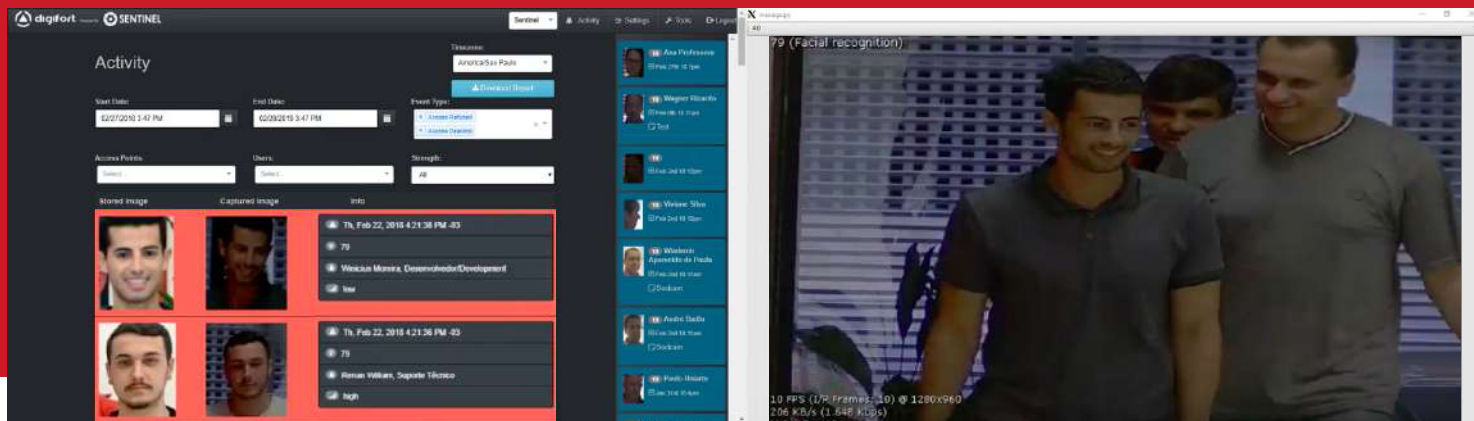
Buying the license Digifort facial recognition, it has included support configuration and maintenance facial recognition software and database of individuals for the period of 1 (one) year.



OPERATIONAL CONSIDERATIONS

System Accuracy

The system can be calibrated to operate at various operating points, privileging rate positive hits (number of detections) or a lower rate of false positives (false alerts). The system, with typical parameters, has a positive recognition rate of 98% with a rate false positive 0.067%



Registration of Persons

The system allows registration of individuals through different mechanisms:

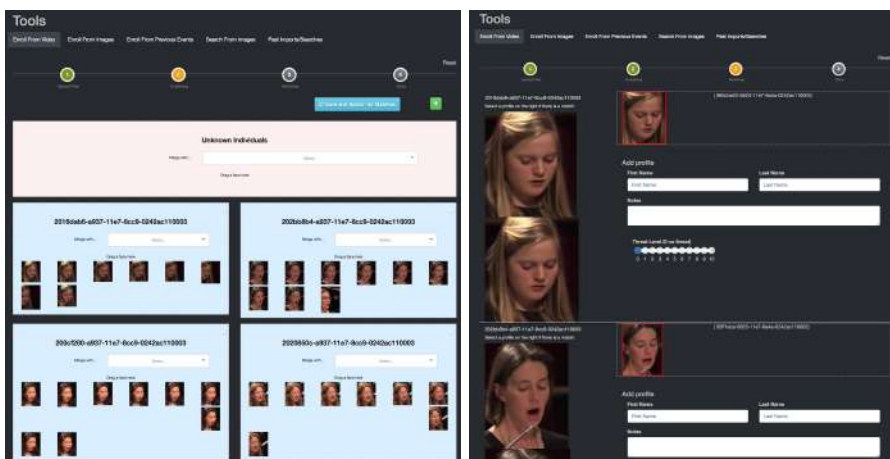
1. Previously stored images of the individual, which are uploaded to the web interface system for registration.
2. Mobile applications for Android and IOS allowing the system administrator or person authorized, register a person capturing a sequence of photos of the face.
3. Forensics video files. The system allows you to upload a video, detect all individuals present and semi-supervised manner, registering new subjects of interest.
4. Auto enrollment of users through the web interface and a standard USB camera (from good quality) connected.
5. A feature of the system is that enroll people from previous detections unknown individuals. The system has the ability to record the faces of individuals not stored in

the database to be subsequently selected by the user and registered.

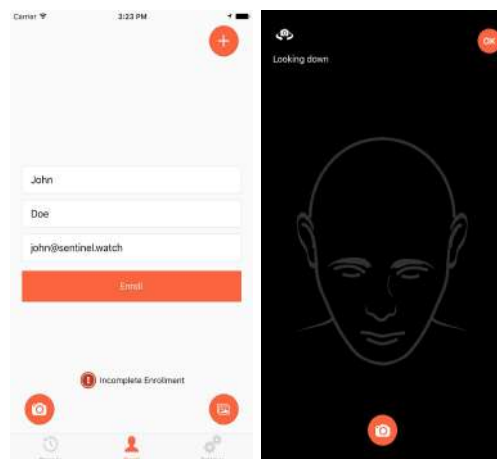
The facial recognition system allows individuals to register in a gallery whitelist (Allowed users) or gallery blacklist (unwanted or unauthorized subjects) with different for each notification. These lists can be configured for each point and monitoring is the ability to generate calendars days and hours allowed for each individual.

Updating the database, which includes registration, removal or renovation of individuals and Instant registered is performed for each of the locations and monitoring points way.





Enrollment via Web tools for video and image extraction



Tocsin app enrollment

Real-time Notifications

The Digifort facial recognition system is also capable of delivering real-time notifications whenever an individual has been identified by the system. These notifications can be e-mails or SMS sent to key individuals and / or mobile notifications

For example, to identify an individual risk by one of the cameras connected to Digifort, is send real-time, push notification security personnel

located on the premises. The staff could then exert some preventive action in the field, call the police or dismiss the alert. The notice given by Digifort includes the recorded image of the individual, the captured image recently by the system and any information entered at enrollment (for eg identification, hazard level, etc. individual)



Event Web Interface and Configuration

The web interface system displays real-time access all events recorded by the system. The events can be filtered by date, time, event type, and Monitoring Point Name the individual. Other important features of the Web interface:

- **Reports of these events can be downloaded in PDF format.**

- **Add / delete / modify cameras**
- **Add / edit / delete individual enrollees**
- **Configuring notifications**
- **Enlistment by Web camera, images or video**

