



### About Ex-Sight.Com

Ex-Sight.Com is an Israeli software company that specializes in accurate Recognition Systems. Our technology allows high-end facial recognition detection based on the latest technology in the market. We provide worldwide OEM Development Services, High-End Biometric Engineering, Interactive systems and Image processing applications for both Security and Retail. We are protecting Corporate Security and Personal Identity using smart Biometric Authentication Algorithms with the latest technology.

### Face Recognition

We use faces to recognize individuals. Advance in computing capability now enables similar recognition automatically. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Major developments have propelled face recognition technology into the spotlight. Face recognition can be used for both verification (1:1), and Identification (1:N) applications.

### Face Template

The heart of the facial recognition system is the Local Feature Analysis (LFA) algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a "template", a unique numerical id for that face.

Once the system has stored a "template", it can compare it to the thousands or millions of "templates" stored in a database. Each template occupies only 2.3 KB of data

### Identification vs. Verification

Verification (1:1, one-to-one) - The process of determining a person's identity by performing matches against one biometric template that is located upon known ID. 1:1 verification usually uses tokens like: Card, code, or any other key based indexing.

Identification (1:N, one-to-many) - The process of determining a person's identity by performing matches against multiple biometric templates. Identification systems are designed to determine identity based solely on biometric information. There are two types of identification systems: positive identification and negative identification.

Our advanced applications allow our customer full control over recognition method. We support both 1:1 (verification) and 1:N (identification) methods.

Minimal image size	640 x 480 pixels
Multiple faces detection time (using 640 x 480 image)	0.07 sec
Single face processing time (after detecting all faces)	0.13 sec.
Matching speed	100,000 faces/sec.
Size of one record in the database	2.3 Kbytes
Maximum database size	Unlimited (upon license)

### FRS Suspect Detection

FRS Suspect Detection is an advanced surveillance system that has video analytics capabilities. It can automatically detect faces On-line or Offline using fast acquisition methods. With its intelligent face recognition algorithms, *FRS Suspect Detection* analyses the input from numerous CCTV cameras, comparing the captured face templates extracted from the cameras with database containing previously stored profiles and face templates.

As face images are detected, FRS Suspect Detection automatically alerts for any identified suspects using variety of interfaces (SMS, Email and Web).

FRS Suspect Detection allows evaluating the correlation between suspect list to incoming targets. Suspect list search is 1: N, it means the suspect image will run through a matching procedure with the database records. The best matches that will be above of the requested similarity level will appear as

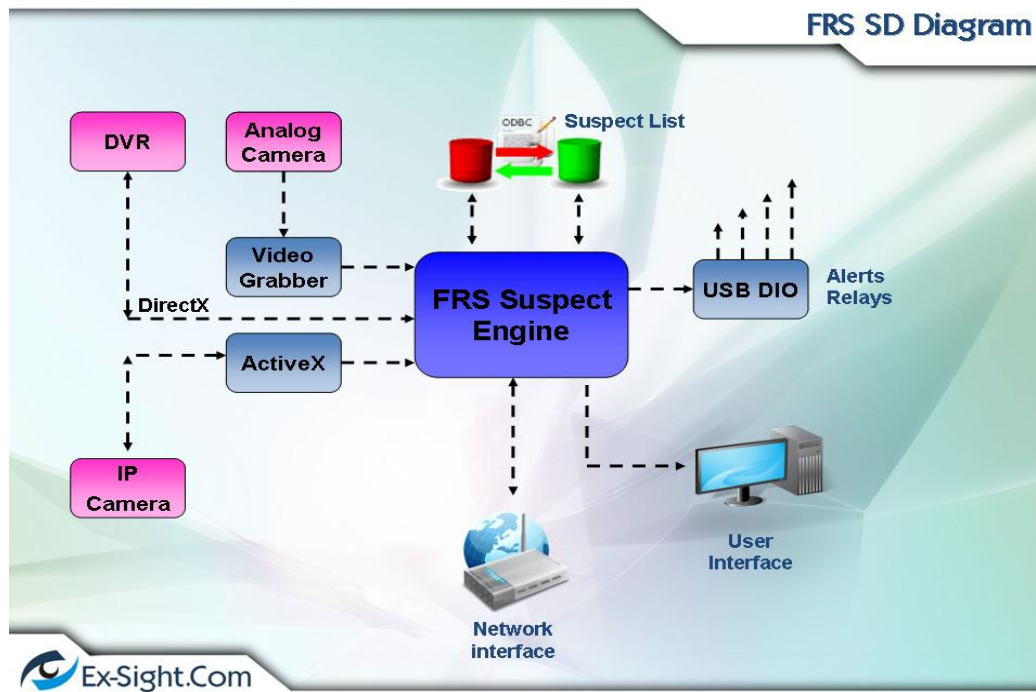
#### Features

- Multiple Real-time video streams at a time
- 1:N Matching, database matching between live images, video images and database images
- Real-time face comparison against watch list
- Alarm notification and recordings
- Enrolment from still image, still image camera and live video stream

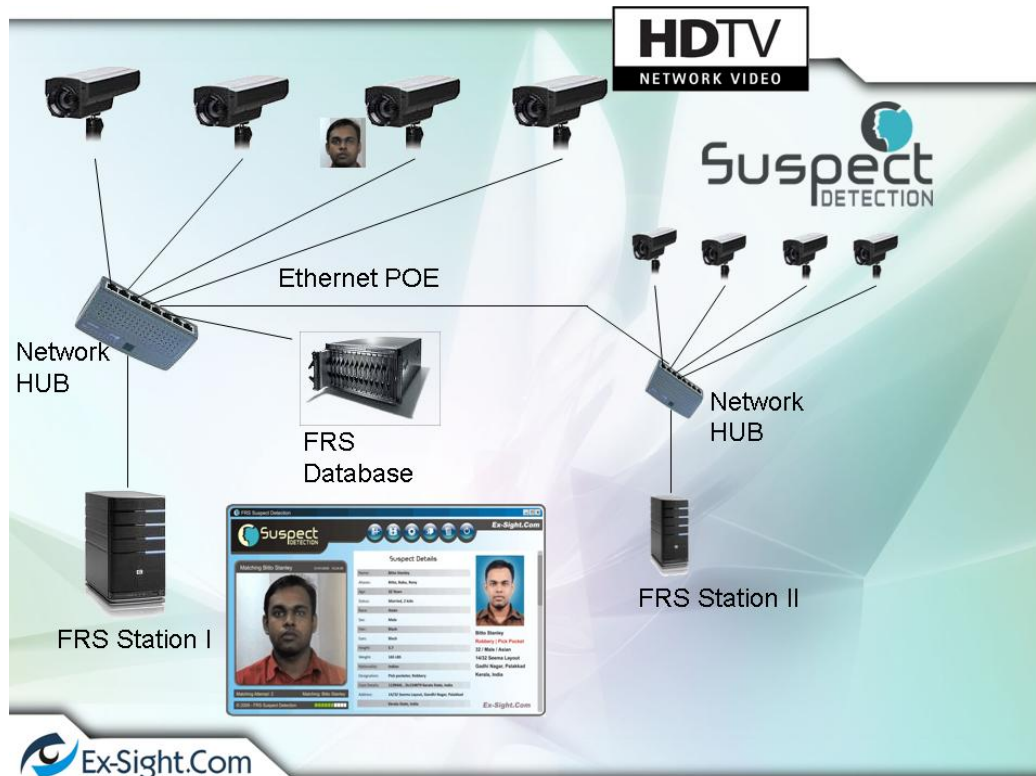
suspects once initiated.

### Working Scenario

- The cameras record and watch online on POIs (Points of Interest)
- The operator select image or video and run it through the system in order to enroll or match a suspect
- The system detects if the target are suspects according to existing watch list
- The watch list is located on a shared network database and can be shared between several operators / stations
- Every operator can work on different area / camera



## Technical Layout of Semi Automatic System



### System Inputs

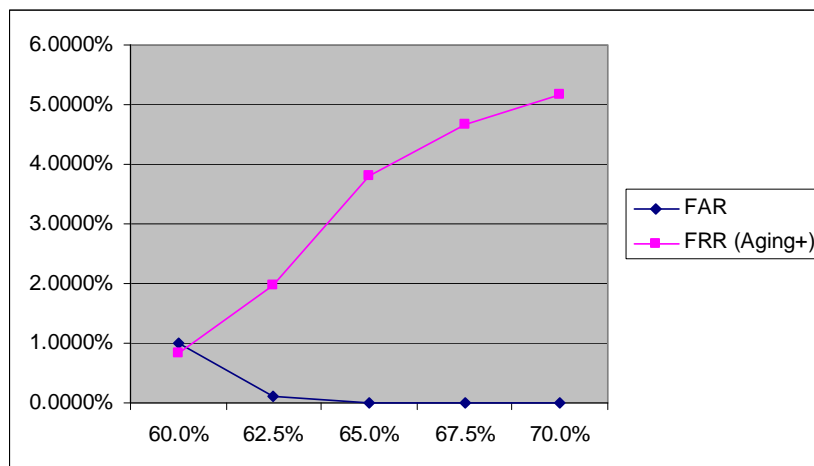
The system requires several inputs as minimum condition of work:

- **Minimal IOD** - Minimum face size will be (not recommended) 40 pixels between two eyes
- **Nominal IOD** - Recommended face size will be 65-70 pixels between two eyes
- **Supported Formats:** JPEG, GIF, BMP, PNG, TIFF
- **Maximum IOD:** 3,000 pixels
- **Image clarity** - Image should be cleared and focused on the subject's face
- **Image Source** - it is recommended the black list image source will be from same camera type that we the system will use for detection
- **Lens** - It is recommended same lens will be used both for detection and enrollment in order to prevent image distortion
- Images X/Y Ratio shall not be updated by the user

IOD = Inner Ocular Distance

## System Statistics

FAR (false acceptance rate)	Matching threshold (score)
10%	12
1%	24
0.1%	36
0.01%	48
0.001%	60
0.0001%	72
0.00001%	84
0.000001%	96



## System Constrains

### Face Pose

face pose must be frontal pose, with full face capturing, the subject should look directly to the camera

### Lighting

Lighting must be equally distributed on each side of the face and from top to bottom. There should be no significant direction of the light or visible shadows. Care must be taken to avoid "hot spots". These artifacts are typically caused when one, high intensity, focused light source is used for illumination.

### Eyeglasses

There should be no lighting artifacts on eyeglasses. This can typically be achieved by increasing the angle between the lighting, subject and camera to 45 degrees or more. If lighting reflections cannot be removed, then the glasses themselves should be removed. (However this is not recommended as face recognition typically works best when matching people with eyeglasses against themselves wearing the same eyeglasses).

Glasses have to be of clear glass and transparent so the eyes and irises are clearly visible. Heavily tinted glasses are not acceptable.

### Currently Supported cameras

Although there is no special limitation on camera type, we recommend using only high-resolution cameras (Mega Pixel Cameras) for suspect detection solution.

The use of these cameras will decrease the mistakes and will higher the detection possibility.

### Supported cameras / IP Servers:

Analog cameras

- AXIS
- VIVOTEK
- A-SONI
- MAVIX
- MOBOTIX

Additional support is possible according to client requirement

### FRS Station Requirements

The minimal requirements are defined according to the number of concurrent cameras and camera models are connected to the station. Normally we do not recommend more than 8 cameras per station in order to prevent overloading.

The definition of maximum number of cameras is according to camera manufacturer. There is no real limitation on number of cameras connected into one FRS system as long they are not overloading the hosting CPU.

FRS minimal requirements for the analytics station are:

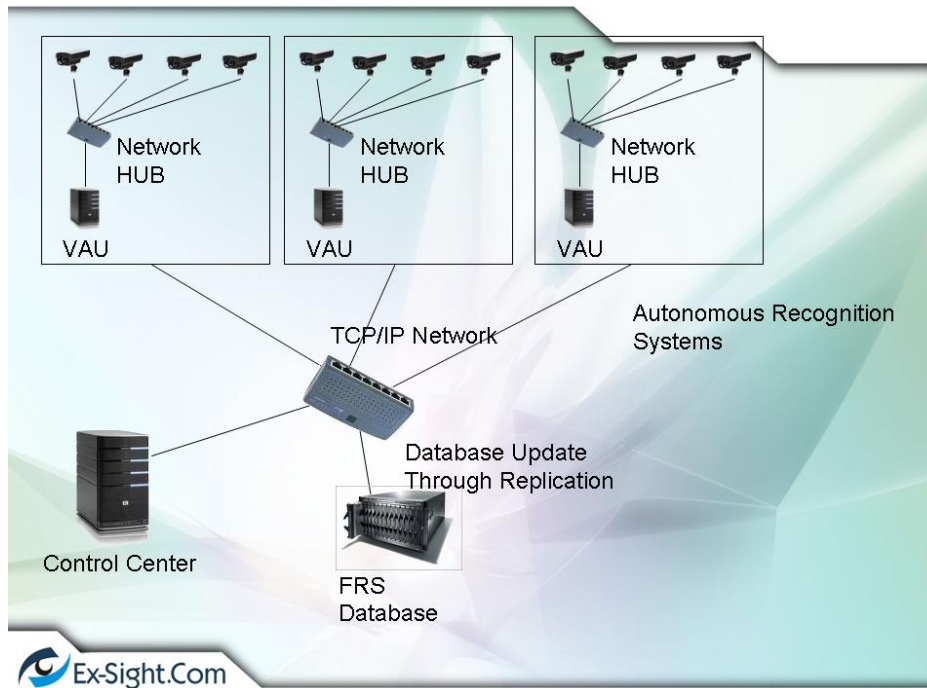
- CPU: 2.6 GHZ Pentium 4
- HDD: 20 GB
- RAM: 2GB

### Fully Automatic Face Detection – Visual Analysis Unit (VAU)

Video Analytics Unit is a 4 to 6 cameras connected together into a processing center. The cameras can be analog or digital. Each VAU reports individually to the command & control center using TCP/IP network. Each VAU will have face recognition module that its watch list source is based on a network database. Each VAU shall act as individual unit and will raise only detection events. All events shall be stored on the command and control station. Each VAU shall have the ability to be remotely monitored.



### Network Layout



### Detection Performance

