Architectural and Engineering Specification for a Video Surveillance System with Face Recognition Capabilities

Senstar Face Recognition

This document is intended to provide performance specifications and operational requirements for the Senstar Face Recognition video analytic. It is written in a generic format. These specifications may be copied verbatim to form a generic procurement specification.

Senstar and the Senstar logo are registered trademarks. Symphony is a trademark of Senstar Corporation. The information in this document is subject to change without notice. Senstar reserves the right to make changes to product design or manufacturing methods, as engineering progresses, or as other circumstances warrant.

PART 1 GENERAL

1.1 System Summary

The contractor shall install a scalable, standards-based Video Management Software (VMS) solution that includes built-in face recognition video analytics.

The VMS shall be installable on commercial-off-the-shelf (COTS) hardware that runs the Microsoft Windows operating system. The solution must be scalable and have automatic failover capabilities that do not require Microsoft Clustering technology.

The solution shall follow a flexible, per-camera licensing model in which face recognition capabilities can be added to the system on a per-camera license basis, without the need to purchase a group of camera licenses or other type of license.

1.2 Quality Assurance

A. The VMS manufacturer shall perform a vulnerability assessment of its software.

B. The VMS manufacturer shall perform penetration (PEN) testing of its software deployed in a standard configuration.

1.3 References

The following acronyms and abbreviations are used in this document:

- FPS – Frames Per Second
- VMS – Video Management Software
- TLS – Transport Layer Security
- NAS – Network-Attached Storage
- SAN – Storage Area Network

PART 2 PRODUCTS

2.1 Video Management and Face Recognition Software

A. The contractor shall supply an IP-based Video Management Software (VMS) solution that includes built-in face recognition capabilities.

B. Video management, camera configuration, and face recognition shall be configured from the same user interface.

C. Video management and any alarms or operational data generated by face recognition software shall be displayed within same operator interface.

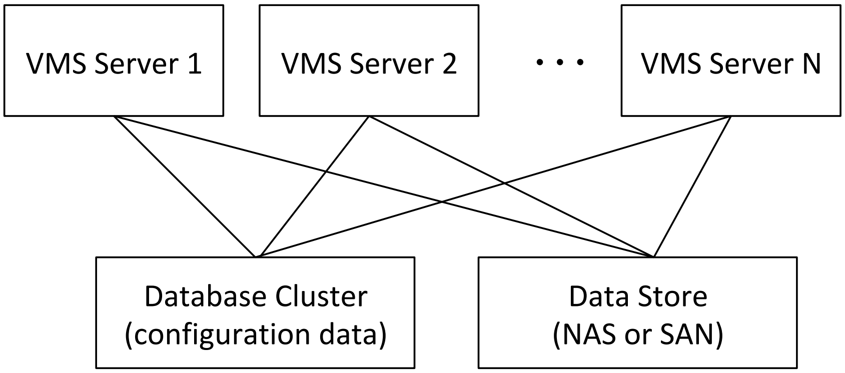
D. The software shall be fully integrated with Access Control and Perimeter Intrusion Detection Systems designed by Senstar Corporation and include the ability to control integrated systems via events generated by the face recognition software.

2.2 Manufacturers

A. The Senstar Symphony Video Management System from Senstar Corporation (senstar.com) meets the requirements stated in this document.

2.3 Architecture Requirements

A. The VMS shall support scalable, enterprise-level deployments that eliminates single points of hardware failure, as shown below.



B. The face recognition software shall run on the same servers as the other VMS components.

C. The system shall store photographs and metadata associated with individuals and configuration data in a SQL database.

2.4 Security and Privacy Requirements

A. Data transmission between core VMS and face recognition software components shall be fully encrypted via TLS 1.2.

B. User access:

1. User security privileges shall be managed directly for a user or through the creation of security groups. Users may be members of more than one security group.
2. Face recognition functionality, including viewing, adding or removing persons, shall be limited to users with the required privileges.

C. Audit logging of user actions shall be stored in plain text or a non-proprietary database.

D. Privacy masks: The VMS shall allow static and dynamic privacy masks to be defined per camera on a per user basis that do not affect the operation of the face recognition software.

2.5 Licensing Requirements

A. The face recognition analytic license can be moved from one camera to another without an additional license cost.

2.6 Camera Compatibility

A. The face recognition software shall be capable of processing any video stream from any camera supported by the VMS, assuming image quality and resolution requirement are met (recommended resolution is 640x480 or higher).

B. The face recognition software shall be able to work with cameras of various positioning. It shall be able to handle up to 70-degree of side-to-side face rotation (less than 45 degrees in optimal positioning), and up to 40-degree up-down face tilt (less than 20 degrees in optimal positioning).

2.7 Configuration Requirements

A. The face recognition software shall be configured from the same web-based administration interface as the VMS.

B. Configuration parameters shall include:

1. Analysis resolution
2. Analysis frames-per-second (FPS)
3. Face confidence threshold
4. Maximum degree of face turn
5. Maximum degree of face tilt
6. Liveness detection

2.8 Alarm and Event Requirements

A. The detection of known and unknown persons in the face recognition software shall be able to trigger corresponding alarms and other events in the VMS.

B. The detection of spoofing attacks, if enabled, in the face recognition software shall be able to trigger corresponding alarms and other events in the VMS.

C. Face recognition events shall be linked with a still image as well as metadata liking the captured video footage

D. Alarm types in the face recognition software shall include:

1. Alarm on all real faces
2. Alarm only on real faces in lists
3. Alarm only on real faces not in lists
4. Alarm on liveness attacks

2.9 Performance Requirements

A. Face detection and identification shall be performed in real time on configured video streams. The face recognition software shall be able to run at 5 FPS at least 720p video stream when the hardware conditions are met (3 GHz CPU).

B. The face recognition software shall generate a 3D mathematical model of individual faces from uploaded 2D video or still images.

C. The face recognition software shall be able to handle low-resolution videos. The allowable distance between eyes shall be as narrow as 30 pixels.

D. The face recognition software shall detect and identify faces from crowd, given hardware resource being sufficient.

E. The face recognition software shall demonstrate high performance in template generation (10 templates per second) and in face match comparison (25 million comparisons per second).

F. The face recognition software shall use a concise template representation, 128 bytes or less per template.

G. The face recognition software shall include spoofing attacking detection that prevents false positives generated displaying photograph of a person to the camera.

H. The enrollment process uses a subset of algorithms that guide users to obtain suitable enrollment images. The algorithms enable head pose detection, focus, lighting and the rest of the currently implemented ISO 19794-5 standards for biometric face images.

2.10 Persons Management

A. The face recognition software shall enable operators with sufficient privileges to manage the stored collection of photographs, including:

1. Adding and deleting records
2. Editing existing records
3. Linking individual records to multiple photos
4. Creating new records from captured video
5. Performing backup and restore functions

B. The software shall support the use of categorized lists, such as authorized and unauthorized lists.

C. The system shall be able to generate a face template from uploaded photos in real time.

2.11 Reporting Requirements

A. Face recognition report shall be enabled and configured through the web-based UI.

B. Face recognition report can be run on schedule.

C. Face recognition report shall include info of the entering camera and the exiting camera, as well as face/figure thumbnails at these cameras.

2.12 System Integration

A. The face recognition software shall in conjunction with the VMS support the integration with third-party systems via a vendor-supplied Software Development Kit (SDK).

B. The face recognition software shall in conjunction with the VMS support Senstar Network Manager software, including the ability to trigger device output points.

C. The face recognition software shall in conjunction with the VMS support Symphony Access Control software, including the ability to trigger device output points.

D. The system shall enable a deployment to be pre-configured off-site, so that the VMS software can become fully functional after installation with minimal on-site configuration.

PART 3 EXECUTION

3.1 System Installation

A. The system shall be installed in accordance with the manufacturer's recommended procedures as defined in the manufacturer's documentation for the system.

3.2 System Configuration

A. The system shall be configured in accordance with the manufacturer's recommended procedures as defined in the documentation for the system.

B. If bundled with a hardware platform, the system may be configured prior to delivery and installation.

C. All device firmware shall be the most-recent provided by the device manufacturer, or of a version specified by the VMS manufacturer.

3.3 User Documentation

A. The supplier shall provide user documentation that explains how to install, configure, operate and maintain the software.

3.4 Training

A. The supplier shall provide training materials that provide instruction in the installation, configuration, and operation of the system.

B. The supplier shall offer professional training services to assist the organization in meeting their training requirements.