International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.743.1
(04/2015)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Audiovisual services

Requirements for intelligent visual surveillance

Recommendation ITU-T F.743.1

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
AUDIOVISUAL SERVICES	**F.700–F.799**
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
HUMAN FACTORS	F.900–F.999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T F.743.1

Requirements for intelligent visual surveillance

Summary

Recommendation ITU-T F.743.1 defines requirements for intelligent visual surveillance (IVS). The requirements are based on identifying specific objects, behaviours or attributes in video signals. The IVS system transforms the video signals into structured data, which can be transmitted or archived so that the video surveillance system can act accordingly.

This Recommendation defines the scenarios, the reference architecture and the requirements for IVS.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T F.743.1	2015-04-29	16	11.1002/1000/12450

Keywords

Intelligent visual surveillance, IVS requirement, IVS scenarios.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

© ITU 2015

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T F.743.1

Requirements for intelligent visual surveillance

1 Scope

This Recommendation defines requirements for intelligent visual surveillance (IVS), which are based on identifying specific objects, behaviours or attribute in video signals.

The visual surveillance service (see [b-ITU-T F.743]) is a telecommunication service focusing on audiovisual application technology that is used to capture remote multimedia information (such as audio signals, video signals, images and various alarm signals) and to present it to end users in friendly manner, based on managed broadband networks with ensured quality, security and reliability.

IVS systems can automatically identify specific objects, behaviours or attributes in video signals. They extract data from the video signals, which are then transmitted or archived so that the visual surveillance system can act accordingly.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.626] Recommendation ITU-T H.626 (2011), *Architectural requirements for visual surveillance.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 visual surveillance [ITU-T H.626]: A telecommunication service focusing on video (but including audio) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signal, etc.) and present them to the end user in a user-friendly manner, based on a managed broadband network with ensured quality, security and reliability.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 boundary detection: see *perimeter prevention*.

3.2.2 directed tripwire intrusion: Alarm output that is based on a polygonal region defined by the user. An alarm can be triggered when an object enters or leaves the polygon.

3.2.3 event recognition: Method that recognizes and analyses the events in the scene, and describes them using natural language.

3.2.4 facial recognition: Detection of the human face in video and extraction of its characteristics. The extracted information and/or image are compared with other images or a database of individuals' images, generating comparison results. Facial recognition can be used in airports, ports, railway stations, coach stations and other public places.

3.2.5 intelligent video diagnosis: Automatic recognition of video images failures, such as snowflakes, scrolling or fuzzy video, partial colour, picture freeze, gain imbalance, pan/tilt/zoom (PTZ) control problems and video signal loss.

3.2.6 intelligent video retrieval: Identification of useful or required information from videos. The search criteria can include target category, colour and velocity.

3.2.7 intelligent video synopsis: A simple summary of video content that can be generated in an automatic or semi-automatic way. First, the target motion is analysed and moving targets are extracted. Then, the different targets are spliced to the same background scenes, and combined in some way.

3.2.8 perimeter prevention; boundary detection: An intelligent surveillance scenario where target objects, such as persons or transportation, can be identified in key areas. Through a virtual cordon or virtual warning region, it can also identify the direction of a target.

3.2.9 region detection: Alarm output that is based on the polygonal regions defined by the user and that is triggered when an object enters or leaves the region.

3.2.10 region stranded: Alarm output that is based on the polygonal regions defined by the user and that is triggered when the retention time of an object exceeds a prescribed threshold.

3.2.11 target recognition: A method that separates an image region from the image background and uses some image feature value to classify the target types.

3.2.12 traffic/pedestrian flow analysis: Motion analysis and feature classification of the video of moving target(s) within the specified single or multiple video monitoring area. The pedestrian flow data can be detected accurately.

3.2.13 tripwire intrusion: The setting off of an alarm when an object crosses a line drawn within the surveillance area.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

APP	Application
CIV	Client Intelligent Video
CMS	Centre Management System
CMU	Centre Management Unit
CU	Client Unit
ICU	Intelligent Customer Unit
IPU	Intelligent Premises Unit
IVM	Intelligent Video Management
IVS	Intelligent Visual Surveillance
IVU	Intelligent Video Unit
MDU	Media Distribution Unit
MSU	Media Storage Unit
NTP	Network Time Protocol
PIV	Premises Intelligent Video
PTZ	Pan/Tilt/Zoom

PU	Premises Unit
SCU	Service Control Unit
SMS	Short Message Service

5 Scenarios for intelligent visual surveillance

This clause describes various scenarios for intelligent visual surveillance (IVS).

5.1 Target recognition

Target recognition separates the image region from the image background, using some image feature value to achieve the classification of the target type; the characteristics of target classification include space and time attributes. The *space attribute* comprises target contour, target size and target texture. The *time attribute* includes the change of target size and velocity. Accordingly, all targets are classified as follows: persons, vehicles or miscellaneous objects.

5.1.1 Person identification

The person identification system identifies human characteristics, which are different from those of vehicles and miscellaneous objects.

5.1.2 Vehicle (car, ship, aircraft) recognition

Vehicle recognition can identify the attributes of a vehicle, such as the type and colour. The type can be recognized using rules about the size of the vehicle. A vehicle smaller than a certain size might be a car and something larger might be a truck. In addition, the colour of the vehicle can be used for recognition, but it might be influenced by the ambient light. See Figure 5-1.

Figure 5-1 – Target recognition (vehicle)

5.1.3 Miscellaneous objects

As shown in Figures 5-2 and 5-3, miscellaneous objects include moving objects that are not persons or vehicles; e.g., animals, smoke, fire and pollutants. Specifically, smoke and fire recognition can be used in forests, tunnels, oil, petrol and gas stations. As shown in Figure 5-3, this system can distinguish between smoke and other objects that are moving in the video.

Figure 5-2 – Target recognition (miscellaneous object)

Figure 5-3 – Target recognition (miscellaneous object)

5.2 Event recognition and intelligent alarm

5.2.1 Perimeter prevention

Perimeter prevention (also known as *boundary detection*) identifies target objects (such as persons or vehicles) in key areas defined by a virtual cordon or virtual warning region. Perimeter prevention can also identify the direction of the target.

1) Region detection: Alarm output must be based on the polygonal regions defined by the user. When an object enters or leaves a region, an alarm can be triggered. See Figure 5-4.

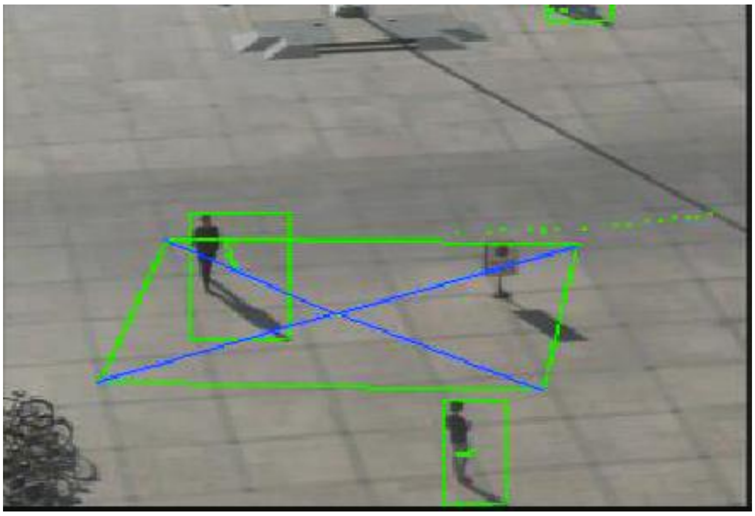


Figure 5-4 – Region detection

2) Region stranded: Alarm output must be based on the polygonal regions defined by the user. When the retention time of an object exceeds a prescribed threshold, an alarm can be triggered. See Figure 5-5.

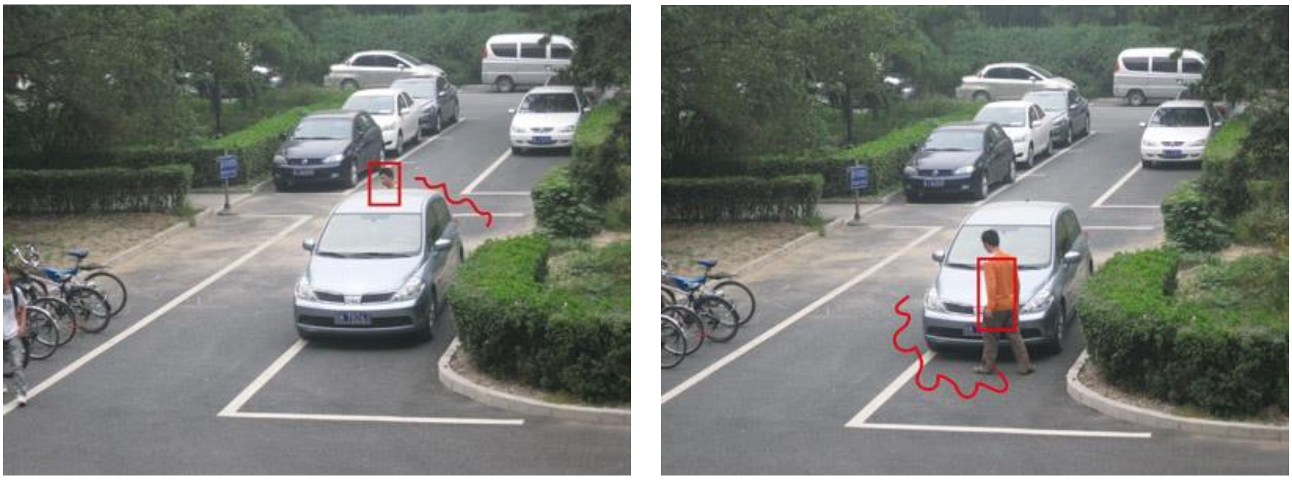


Figure 5-5 – Region stranded

3) Tripwire intrusion: A line that is drawn within the surveillance area. When an object crosses that line, an alarm is triggered. See Figure 5-6.

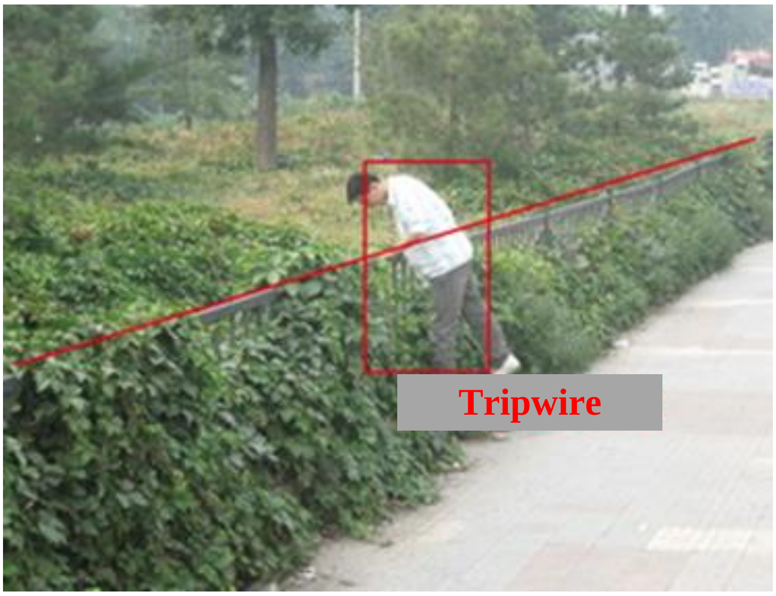


Figure 5-6 – Tripwire intrusion

4) Directed tripwire intrusion: A line is drawn within the surveillance area. When an object travelling in a specified direction crosses the line, an alarm can be triggered. A virtual cordon is drawn within the video image. When a target crosses the line in the specified direction, an alarm can be triggered. As shown in Figure 5-7, the direction of the virtual cordon can be unidirectional or bidirectional.

(a) Intruder detection (b) Wrong direction detection

Figure 5-7 – Directed tripwire intrusion

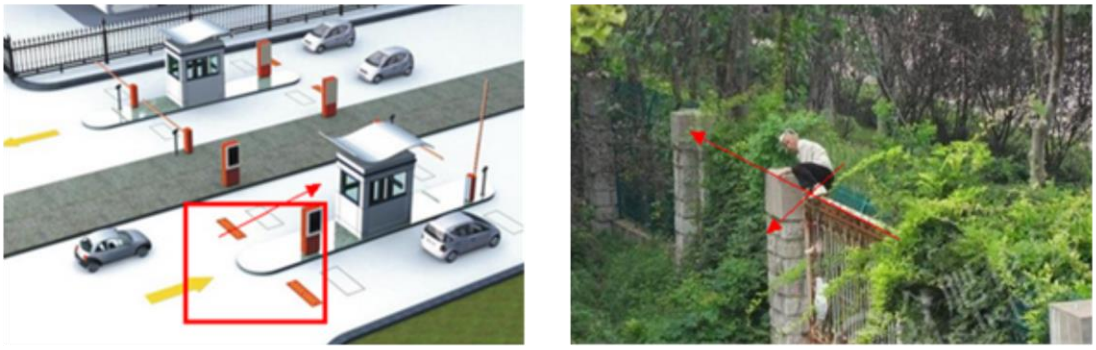
5.2.2 Region security alarm and linkage

– Step 1: Bob is a security clerk. His job is to find suspicious persons and abnormal behaviour by watching real-time video from residential areas of interest using a surveillance system.

– Step 2: Bob uses an IVS system, where an electronic fence is defined based on a virtual line or a polygon in the video images and that is linked to an alarm. When objects cross the electronic fence and their direction of movement is consistent with the setting, the system generates sound and light alarms to alert related personnel, who then deal with the situation.

– Step 3: Leonard lives in this residential area. He enters the underground garage from the exit. Since Bob had set an electronic fence, the IVS system identifies Leonard's abnormal behaviour and triggers an alarm. Bob receives the alarm and warns Leonard through a radio device to correct his behaviour. In addition, the public security on patrol in the area receives at the same time a short message service (SMS) sent by the alarm linkage system to indicate that something abnormal happened in the garage.

Similarly, this IVS system can detect other abnormal behaviours, such as climbing over a fence or entering a dangerous zone; see Figure 5-8. The user can also adjust the degree of sensitivity of the system in order to reduce false alarms, such as those due to interference by birds and changes in illumination.



Enter the garage using the exit Climb over the fence

F.743.1(15)_F5-8

Figure 5-8 – Examples of regional security alarm and linkage

5.2.3 Intelligent traffic violation monitoring

– Step 1: Sheldon is a traffic police officer, and his job is to monitor traffic violations using surveillance video. The traffic monitoring system can capture vehicle violation images as evidence.

– Step 2: Raj drives under a monitoring camera that is part of the intelligent traffic violation-monitoring system. His illegal driving behaviour in a wrong lane is captured by the monitoring camera. See Figure 5-9.

– Step3: The system recognizes Raj's vehicle licence plate and automatically sends a picture to Raj by e-mail or SMS, to warn him that the traffic violation has been detected and that he will receive a penalty.

This system can also detect automatically illegal parking, speeding and other violations.

Figure 5-9 – Traffic violation

5.3 Data analysis

5.3.1 Traffic/pedestrian flow analysis

By using intelligent tracking and recognition algorithms, a traffic/pedestrian flow analysis system can accurately acquire pedestrian flow data based on the video of a moving target, motion analysis and feature classification within a specified single or multiple video monitoring areas. This is illustrated in Figure 5-10.

Figure 5-10 – Pedestrian flow analysis

Real-time monitoring of pedestrian flow can be used to identify patterns that enable planning of efficient pedestrian flow across different surveillance regions during different times of the day. An intelligent analysis service can help managers to more quickly understand pedestrian flow, to make better planning, scheduling and layout decisions; and to help customers get more business opportunities. An intelligent pedestrian flow analysis service is useful in a variety of scenarios, which include statistics and analysis of pedestrian flows in shopping malls, bus stations, parking areas, places of entertainment, stadiums, theatres and other public places.

Statistics and analysis of pedestrian flow in shopping malls

Detection and statistics of pedestrian flow can provide an objective, scientific basis for companies to develop and adjust tactics that will help them achieve their commercial goals. These tactics can include sales to businesses and individuals, promotions, pricing decisions, and options for stocking products, store layouts, service modes and content.

Statistics and analysis of pedestrian flow in bus stations

Through automatic, intelligent, and accurate acquisition of in/out pedestrian flow, it is possible to record and manage vehicle operation information in each site. Transportation owners and managers should use traffic statistics as the basis of vehicle planning, vehicle scheduling and operations management.

Statistics and analysis of pedestrian flow in parking areas

Pedestrian flow statistics help security departments to determine peak times, to identify areas of pedestrian flow, and to help managers study pedestrian flow distribution.

Statistics and analysis of pedestrian flow in places of entertainment, stadiums and theatres

With accurately characterized pedestrian flow data, managers can deploy staff effectively and plan future activities accurately through time and personnel assignment optimization. Based on variations in pedestrian flow, it is possible to make adequate arrangements on the busiest day or the busiest week of every month, or at a busy entrance.

Pedestrian flow statistics are generally based on information from cameras at passageways. Most cameras are installed indoors, so the position of staff can be accessed and illumination can be controlled.

Traffic statistics are generally based on information from outdoors, such as wide multi-lane roads. It is therefore difficult to control the orientation of vehicles or the light and weather conditions. Intelligent traffic analysis techniques are currently more developed in pedestrian flow statistics; however, but the effectiveness of traffic statistics can be improved.

5.3.2 Facial recognition

Facial recognition detects facial images in video and extracts their characteristics. The extracted information is then compared with other images or a database of individuals' images, and comparison results are generated. This application can be used in airports, ports, railway stations, coach stations and other public places. See Figure 5-11.

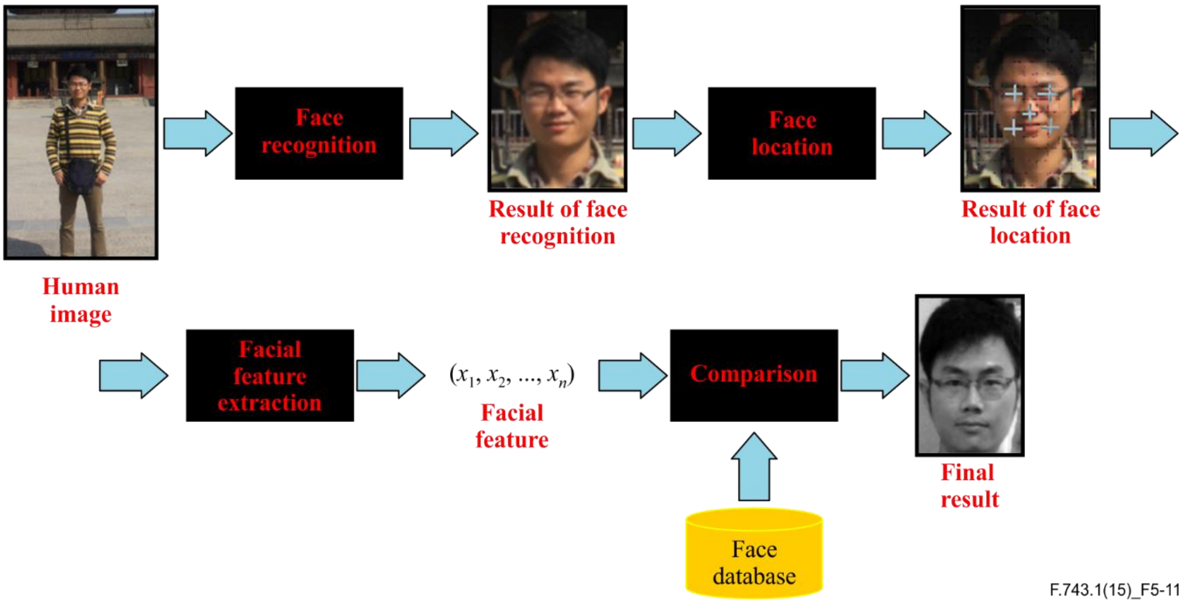


Figure 5-11 – Facial recognition

The process is as follows:

– Step 1: Bill works in the human resources department and work attendance management is one of his job responsibilities.

– Step 2: Two high-definition cameras are installed to capture video at the entrance/exit every day. The facial recognition system can automatically recognize faces.

– Step 3: The system compares those facial images with the company face database, and labels them with the time of passage. Thus Bill can acquire daily reports and easily manage staff attendance.

5.3.3 Vehicle licence plate recognition

– Step 1: Peter is a traffic police officer who works in a vehicle information management department. With a recognition system, Peter can get licence plate snapshots at an intersection.

– Step 2: First, the system locates the position of the licence plate; see Figure 5-12. Then, it identifies the plate colour, characters or numbers, and vehicle types using intelligent image analysis algorithms and stores the information in the database.

Peter can use this database for fake plate vehicles management, vehicle tracking, etc.

Figure 5-12 – Vehicle licence plate recognition

5.4 Intelligent video diagnosis

This scenario is illustrated in Figure 5-13:

– Step 1: Howard is a video surveillance maintenance staff member. He needs to ensure that 100 surveillance cameras in an office building are working normally.

– Step 2: The intelligent video system can diagnose whether cameras within the building are in normal working condition. This system helps Howard find any defective camera, and prompts him with the location and type during a routine inspection.

– Step 3: Howard sends an equipment maintenance worker to repair the defective camera.

Similarly, Howard can get alarms for picture quality abnormalities, such as snow, blur and colour cast.

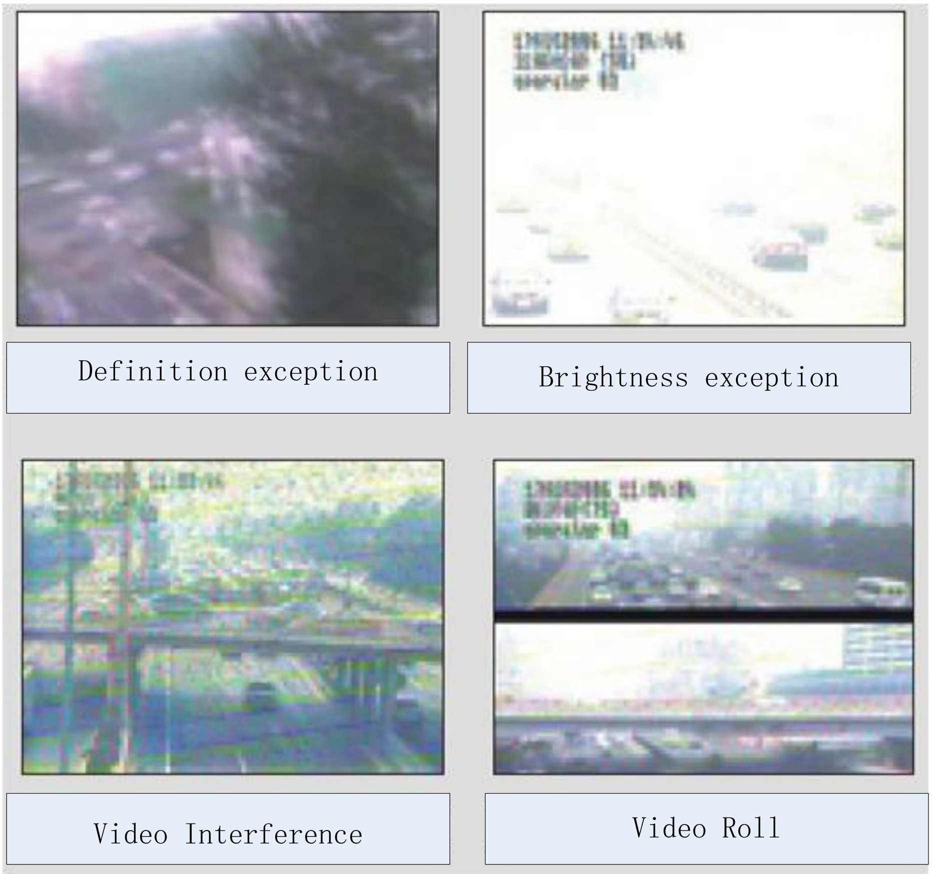


Figure 5-13 – Video diagnosis

5.5 Intelligent video retrieval

This scenario is illustrated in Figure 5-14:

– Step 1: Steven is a police officer working in a criminal investigation department. When a crime occurs, Steven and his colleagues collect signals from all the surveillance videos located in that area at that time.

– Step 2: Steven uses an intelligent video retrieval system to process the videos. The system extracts moving object information, such as size, colour and motion direction, and establishes a target index database. This database transforms the non-structured video into a structured index description.

– Step 3: Using scattered target feature clues, the suspicious objects in the video can be quickly located. For example, Steven searches for a red car in several surveillance videos. With the help of an intelligent video retrieval system, Steven can quickly locate all the red cars appearing in the video. The system assists Steven in searching important information in the mass of video data.

Figure 5-14 – Intelligent video retrieval

5.6 Intelligent video synopsis

This scenario is illustrated in Figure 5-15:

– Step 1: Amy is a company staff member. In order to oversee the elderly and children, she has installed a camera in the house. She wants to remotely see key information of what happened at home.

– Step 2: First, Amy imports the daytime videos into the video synopsis system. After target recognition is finished, targets and related information are indexed.

– Step 3: As Amy's requirement, different targets are stitched to the same background scene and combined together. After that, the duration of the video is compressed and Amy can view a 5 min compressed video instead of 1 h.

Figure 5-15 – Intelligent video synopsis

6 Reference architecture

Figure 6-1 shows the overall function architecture for IVS, based on that defined in [ITU-T H.626]. On the right side, the functional architecture for ITU-T F.743.1 focuses on a visual surveillance system with intelligent units, including an intelligent video management (IVM) server, intelligent video unit (IVU) and application (APP), shown on the left side of Figure 16.

NOTE – See also [b-ITU-T H.627] for signalling and protocols for visual surveillance, and [b-ITU-T H.626.1] for architectural requirements for mobile visual surveillance.

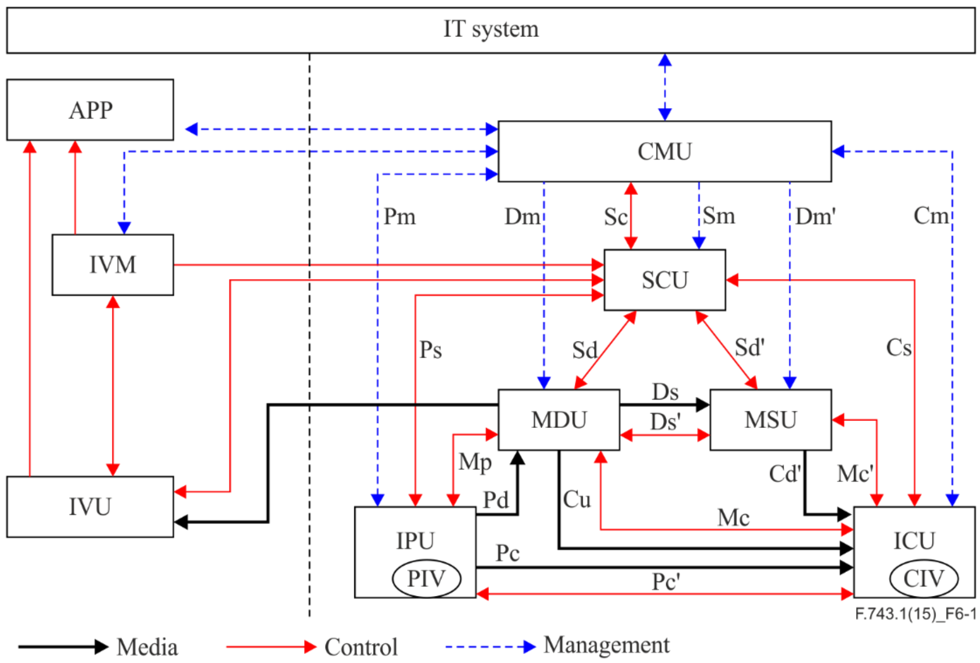


Figure 6-1 – Functional components of an IVS

The architecture also contains an intelligent customer unit (ICU) and an intelligent premises unit (IPU) shown on the right side of Figure 6-1.

Descriptions of IVS components follow.

IVU (intelligent video unit): automatically identifies specific objects, and outputs recognition results to IVM. Recognized information includes that from event triggers and data acquisition. An IVU can include more than one intelligent analysis algorithm that can be added or deleted according to requirements.

IVM (intelligent video management): supports users in configuring intelligent application strategies and dynamically scheduling video sources according to intelligent application strategies. IVM dynamically schedules the IVU and accepts registration, deletion and capability reports from it. IVM can be invoked by an intelligent application from the CMU (see below). Then IVM sends interface information to the CMU.

APPs (applications): third-party data application analysis systems, which in general are not standard units. An APP can accept data from the platform, and then configure data analysis algorithms and strategies. It can analyse data. An APP can send alarm information to the platform if needed. In addition, an APP can be built to meet a specific user requirement. Taking into consideration that alarm processing is a main function with a heavy load; an APP should be stripped from the CMU, which makes the function of platform units clear and allows the platform to be scalable.

ICU (intelligent customer unit): in order to achieve comprehensive intelligent video recognition, this unit adds a client intelligent video (CIV) module to the control unit (CU). A CIV recognizes required information from input videos, and outputs recognition results. In addition, a CIV can search designated records from video files. The identifiable information includes event trigger information and data acquisition information.

IPU (intelligent premises unit): this unit adds a premises intelligent video (PIV) module to a premises unit (PU). A PIV is an intelligent recognition module of the PU, which can be achieved and integrated in PU devices. A PIV can recognize required information from input videos, and output recognition results. The recognized information includes that from event triggers and data acquisition.

SCU (service control unit): is used to access service control and signal call control between the PU and the CU.

MDU (media distribution unit): its main functions include media reception, media processing, media routing, media transmission, media forwarding and media replication.

MSU (media storage unit): its main functions include media storage, media serving, media indexing and media downloading.

CMU (centre management unit): is used for centralized system management, service operation management, etc.

7 Requirements for an IVS

7.1 User requirements

7.1.1 User level requirements

USR-001: IVS system is recommended to classify users into several levels. Users of different levels have different operational rights; high-level users have more operation privileges than low-level ones. Low-level users can do basic operations that meet the basic requirements described in clause 7.1.2, and high-level users can do advanced operations that meet the advanced requirements described in clause 7.1.3.

7.1.2 Basic requirements

7.1.2.1 Common category

USR-002: The IVS system is required to have the ability to obtain the standard video streams transmitted or distributed by the platform, to analyse images, and to send the result back to the original system.

USR-003: The IVS system is required to have the ability to directly access the platform using embedded devices with intelligent analysis functions. The device analyses the image and sends the result back for the system to complete the recognition process, as well as the real-time media stream.

USR-004: The IVS system is required to have the ability to determine a certain area for picture snapshots through the CU or other controls, should support the drawing of trip lines, and optionally specify coordinates for designation.

USR-005: The IVS system is required to have the ability to designate the whole or a part of the area for intelligent detection.

USR-006: The IVS system is required to have the ability to filter redundant information from the image, including jitter and weather factors.

7.1.2.2 Perimeter alarm category

USR-007: The IVS system is required to have the ability to draw one or more trip lines on a video image.

USR-008: The IVS system is required to have the ability to support in/out two-way intrusion detection in both enclosed and unenclosed regions, and to support two-way intrusion detection for every warning line. The system generates an alarm when the target object moves out of the object detection region.

USR-009: The IVU/PIV is required to have the ability to determine automatically the features of the target object based on the type detected. The IVU/PIV should support at least person and vehicle feature detection, but it is not required to report the extracted feature information. Other information for the object detection function is optional; users can choose it according to the maturity of the algorithm.

USR-010: The IVS system is required to have the ability to set the detection period; the minimum unit is the minute. Alarms can be enabled at certain alarm periods or fixed time intervals within a day or week.

USR-011: The alarm result is required to include alarm information and one or more image(s).

7.1.2.3 Passenger flow category

USR-012: The IVS system is required to have the ability to set the counting region on a snapshot image through the CU or other controls.

USR-013: The passenger flow function is required to have the ability to be set either one-way or two-way for direction detection and passenger flow statistics.

USR-014: The IVS system is required to have the ability to set the density threshold, which triggers an alarm when the density of passengers exceeds a threshold.

7.1.2.4 Target recognition category

USR-015: The IVS system is required to have the ability to classify objects into persons, vehicles and other objects, based on target shape, aspect ratio and texture feature characteristics.

USR-016: The IVS system is required to have the ability to recognize the colour, velocity, direction of movement and other features of the target.

7.1.2.5 Video synopsis category

USR-017: The IVS system is required to have the ability to select a target of interest in the concentrated video; clicking on the original target will play the corresponding video, both the original video and the concentrated form, with the option of displaying them simultaneously.

USR-018: The IVS system is required to have the ability to output a shortened video including all targets in this video.

7.1.2.6 Video retrieval category

USR-019: The IVS system is required to have the ability to choose the target category and/or the target colour as keywords for searching.

USR-020: The IVS system is required to have the ability to search targets in the video, by drawing a circle on the sample picture, inside which is the target sample.

USR-021: The IVS system is required to have the ability to display search results in the form of key frames and video segments, sorted according to the matched similarities or in the order of appearance.

7.1.3 Advanced requirements

USR-022: The IVS system is required to have the ability to upload alarm video segments, if requested.

USR-023: The IVS system is required to have the ability to develop new algorithms, such as detection of abandoned items (to detect dangerous or suspicious items in a certain area), item preservation (to guard against certain items being moved) and licence plate recognition.

USR-024: The IVS system is required to have the ability to set the concentration density in real time while playing the concentrated video.

USR-025: The IVS system is required to have the ability to expand the search criteria, such as the switch value data from the front-end sensor.

USR-026: The IVS system is required to have the ability to track moving targets within the image.

7.2 Service requirements

7.2.1 Basic requirements

SRV-001: IVU/PIV is required to provide at least two types of control of algorithm parameter configuration: one for an administrator and another for ordinary users. IVU/PIV also requires the administrator to finish the initial scene studying, advanced parameter setting and other professional operations, while the business is opened via controls, in order to improve alarm accuracy.

SRV-002: It is required that users have the ability to set alarm rules via controls, when the background scene remains the same, but the warning area changes.

SRV-003: IVM is required to have the ability to provide the network time protocol (NTP) clock synchronization service to the IVM managed by it.

SRV-004: The alarm analysing strategies (including the type of algorithm and detection period) require setting by the CU and are stored on the platform. The platform is responsible for starting or stopping the intelligence analysis.

SRV-005: CMS (centre management system) is required to generate a temporary key valid for a certain period. It can be in form of a temporary username and password, when the intelligent analysing rule requested by the CU is transmitted by the CMU.

SRV-006: IVS system is required to keep a user log, including user log-in time, log-off time and operating options (video synopsis).

SRV-007: IVS system is required to keep a system log, including system start-up, system freeze and system failure. It should support log inquiring in accordance with both the content and the timing, as well as exporting logs and querying results.

SRV-008: IVS system is required to have the ability to manage user authority by setting the user role. It can add, delete and modify users; additionally, the system can customize user roles, set authority for each type of role, and classify users into the appropriate type.

7.2.2 Advanced requirements

SRV-009: The IVS system is required to have the ability to keep record of all synopsis strategies set by users. It should support strategy inquiring and exporting.

Bibliography

[b-ITU-T H.626.1] Recommendation ITU-T H.626.1 (2013), *Architecture for mobile visual surveillance.*

[b-ITU-T H.627] Recommendation ITU-T H.627 (2012), *Signalling and protocols for visual surveillance.*

[b-ITU-T F.743] Recommendation ITU-T F.743 (2009), *Requirements and service description for visual surveillance.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015