Video Analytics technology: the foundations, market analysis and demonstrations

Prepared by:
Dmitry O. Gorodnichy, Jean-Philippe Bergeron, David Bissessar, Ehren Choy, Jacques Sciandra
Canada Border Services Agency
Ottawa ON
Canada K1A 0L8

Contract Scientific Authority: Pierre Meunier
DRDC Centre for Security Science
613-992-0753

Contract Report
DRDC-RDDC-2014-C251
September 2014

IMPORTANT INFORMATIVE STATEMENTS

PROVE-IT (FRiV) Pilot and Research on Operational Video-based Evaluation of Infrastructure and Technology: Face Recognition in Video project, PSTP 03-401BIOM, was supported by the Canadian Safety and Security Program (CSSP) which is led by Defence Research and Development Canada's Centre for Security Science, in partnership with Public Safety Canada. Led by Canada Border Services Agency partners included: Royal Canadian Mounted Police, Defence Research Development Canada, Canadian Air Transport Security Authority, Transport Canada, Privy Council Office; US Federal Bureau of Investigation, National Institute of Standards and Technology, UK Home Office; University of Ottawa, Université Québec (ÉTS).

The CSSP is a federally-funded program to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology with policy, operations and intelligence.

Science and Engineering Directorate

Border Technology Division

Division Report: 2014- 36 (TR)

July 2014

Video Analytics technology: the foundations, market analysis and demonstrations

Dmitry Gorodnichy,
Jean-Philippe Bergeron,
David Bissessar,
Ehren Choy,
Jacques Sciandra

This page left intentionally blank

Abstract

This report provides the history and background information related to the PROVE-IT(VA) project conducted by the CBSA under the funding from Defence Research and Development Canada (DRDC) Centre for Security Science (CSS) Public Security Technical Program (PSTP). The key outcomes from the Interdepartmental *Video Technology for National Security* (VT4NS) meetings that led to establishing the project are presented, the key concepts behind automated recognition in video are summarized, survey of Video Analytics (VA) market offerings is developed, and the technology demonstration developed for the projects are described.

Keywords: video surveillance, video analytics, recognition in video, intelligent video, technology readiness, performance evaluation, data-sets.

Community of Practice: Border and Transportation Security

Canada Safety and Security (CSSP) investment priorities:

1. Capability area: P1.6. Border and critical infrastructure perimeter screening technologies/ protocols for rapidly detecting and identifying threats.

1. Specific Objectives: O1. Enhance efficient and comprehensive screening of people and cargo (identify threats as early as possible) so as to improve the free flow of legitimate goods and travellers across borders, and to align/coordinate security systems for goods, cargo and baggage;

2. Cross-Cutting Objectives CO1. Engage in rapid assessment, transition and deployment of innovative technologies for public safety and security practitioners to achieve specific objectives;

3. Threats/Hazards F. Major trans-border criminal activity e.g. smuggling people/material

Acknowledgements

This work is done within the project PSTP-03-402BTS “PROVE-IT(VA)" funded by the Defence Research and Development Canada (DRDC) Centre for Security Science (CSS) Public Security Technical Program (PSTP) .

The feedback from project partners: University of Ottawa, CRIM, ETS, RCMP, TC, CATSA, DRDC, UK HomeOffice, FBI is gratefully acknowledged.

Release Notes

Context: This document is part of the set of reports produced for the PROVE-IT(VA) project. All PROVE-IT(VA) project reports are listed below.

1. Dmitry Gorodnichy, Jean-Philippe Bergeron, David Bissessar, Ehren Choy, Jacque Sciandra, “Video Analytics technology: the foundations, market analysis and demonstrations", Border Technology Division, Division Report 2014-36 (TR).

2. Dmitry O. Gorodnichy, Diego Macrini, Robert Laganiere, “Video analytics evaluation: survey of datasets, performance metrics and approaches", Border Technology Division, Division Report 2014-28 (TR).

3. D. Macrini, V. Khoshaein, G. Moradian, C. Whitten, D.O. Gorodnichy, R. Laganiere, “The Current State and TRL Assessment of People Tracking Technology for Video Surveillance applications", Border Technology Division, Division Report 2014-14 (TR).

4. M. Lalonde, M. Derenne, L. Gagnon, D. Gorodnichy, “The Current State and TRL Assessment of Unattended and Left-Behind Object Detection Technology", Border Technology Division, Division Report 2014-13 (TR).

Jointly with the PROVE-IT(FRiV) project (PSTP-03-401BIOM):

5. D. Bissessar, E. Choy, D. Gorodnichy, T. Mungham, ``Face Recognition and Event Detection in Video: An Overview of PROVE-IT Projects (BIOM401 and BTS402)", Border Technology Division, Division Report 2013-04 (TR).

6. D. Gorodnichy, E. Granger J.-P.Bergeron, D.Bissessar, E.Choy, T. Mungham, R. Laganiere, S. Matwin, E. Neves C. Pagano, M. De la Torre, P. Radtke, “PROVE-IT(FRiV): framework and results". Border Technology Division, Division Report 2013-10. Proceedings of NIST International Biometrics Performance Conference (IBPC 2014), Gaithersburg, MD, April 1-4, 2014. Online at http://www.nist.gov/itl/iad/ig/ibpc2014.cfm

The PROVE-IT(VA) project took place from August 2011 till March 2013. This document was drafted and discussed with project partners in March 2013 at the *Video Technology for National Security* (VT4NS) forum. The final version of it was produced in July 2014.

Appendices: This report is accompanied by several appendices, which include the presentations from *Video Technology for National Security* (VT4NS) confrences related to better understanding of Video Analytics, its evaluation, and the Government of Canada efforts in researching and leveraging this technology for national security.

Contact: Correspondence regarding this report should be directed to DMITRY dot GORODNICHY at CBSA dot GC dot CA.

Table of Contents

1. Background

Over the past five years the Government of Canada (GoC) has been intensively exploring how to leverage the advances made in video technology for the national security needs. Starting from 2008 and built on the original collaboration between the National Research Council of Canada’s Institute for Information Technology (NRC-IIT) and the Computer Vision section of the USA Director of National Intelligence’s Intelligence Advanced Research Projects Activity (DNI IARPA), formerly USA Disruptive Technology Office’s Video Analysis and Content Extraction program (DTO-VACE), the Science and Engineering Directorate of the Canada Borders Services Agency (CBSA-S&E) took the lead in bringing together all GoC stakeholders working in the area Video Surveillance and Analytics in what has become known as the *Video Technologies for National Security* (VT4NS) initiative. Annual one-day long VT4NS workshops have been organized for the GoC stakeholders, where GoC stakeholders could exchange information about their needs in video surveillance, learn more about the state of the art in the field, and finally discuss the next steps for addressing their needs.

A dedicated VT4NS SharePoint portal https://partners.drdc-rddc.gc.ca/css/Portfolios/Biometrics/VT4NS accessible to GoC clients and partners has been created to facilitate the exchange of information on the topic and where the proceedings from the past five VT4NS workshops have been archived. The key excepts from the VT4NS proceedings archived at the VT4NS site are provided as Appendices in this report. As summarized in the Appendices, the key outcomes from the VT4NS initiative and its affiliated workshops were 1) raising the awareness of GoC video surveillance stakeholders on the technical challenges of deploying Video Analytics, and 2) preparing the foundation for developing and conducting – in partnership with all major GoC stakeholders (CBSA, RCMP, TC, CATSA, DTDC) and International and Academic partners (University of Ottawa, CRIM, ETS, UK HomeOffice, FBI) - two major Research and Development (R&D) studies called *PROVE-IT(FRiV)* and *PROVE-IT(VA)* dedicated to examining and improving, where possible, the Technology Readiness Level (TRL) of video surveillance technologies that can be potentially deployed by the GoC.

The current report presents the key outcomes of the PROVE-IT(VA) study. The key concepts behind automated recognition in video are summarized, survey of Video Analytics market offerings is developed and the technology demonstration developed for the projects are described.

2. Intelligent Surveillance Market Analysis

2.1 How Intelligent is “Intelligent Surveillance” ?

There are over 5000 companies registered in Canada doing business in video surveillance.[NUANS Search Results with keywords “video, surveillance” in 2008 (www.nuans.com)]. Any company doing business in video surveillance can potentially call its surveillance technology “Intelligent” or “Smart” by simply performing naïve “pixel brightness comparison” (More detail on the difference between pixel brightness comparison and real object motion detection as well as other key concepts related to the automated recognition in video are provided in Appendices D-E and [1-5]).

It is also expected that most companies that implement many video analytics applications, do so by using public domain computer vision and image processing libraries such as Intel Open CV. These libraries can be used at no charge for commercial applications and contain functions and primitives such as many low-level image processing libraries (edge detection, colour segmentation, motion/optical flow computation) and more complicated codes such as for OCR, Face Detection, and even some Face Recognition and Classification.

The use of these libraries is very common in the academic environment and many graduates from computing science and engineering departments can use them. As a result, there are many companies that are now capable of doing video processing and in doing so they can claim that they can provide *many* Video Analytic (VA) functionalities (as in listed in Table 1). Clearly, some of these functionalities are much harder than others, if possible at all. The key question therefore is to know which of these functionalities are really ready for deployment and which are not.

Table 1. Non-inclusive list of VA functionalities reported by the companies as ``possible`` according to their documentation and websites. Left column lists technologies that are of much higher difficulty than those listed in the right column.

Harder	Easier
Human / Object Recognition and Tracking	Intrusion Detection / Virtual Tripwire
Object Classification	Autonomous PTZ Tracking
People Counts	Stopped Vehicle Detection
Vehicle recognition	Camera Tampering Detection
People recognition / Face recognition	Congestion detection
Unattended Baggage Detection	Counter Flow
Object Removal Detection	Automatic Licence Plate Recognition
Loitering Detection	Object Alteration Detection
Tail-gating	Audio and Sound Classification
[Waiting] Line Control, Crowd management	Face Detection / Face Tracking
Special Attribute Detection	Graffiti / Vandalism detection
Advanced Behaviour Analysis	Highway (vehicle) count

Below we provide a more detailed overview of VA functionalities offered by the industry. The assessment of readiness of these functionalities is provided in separate PROVE-IT(VA) reports.

2.2 Main functionalities developed by the companies

The video surveillance market has many players that provide a range of commercial products using VA capabilities. Some companies are specialised in real time Video Analytics while others focused on a post processing mode.

This survey was based on Video Analytics running on the server side as its technology is more mature in terms of the reliability and the power of the hardware as well as the efficiency of the operating system. At the same time, we note that Video Analytics on the edge (i.e. performed on a camera or encode hardware) is becoming also possible, due to the recent increase in camera power and processing capabilities.

Video Analytics commercial products can be deployed in many security applications. The figures below provide illustrations of some commonly listed Video Analytics functionalities.

Figure 1 – Area detection

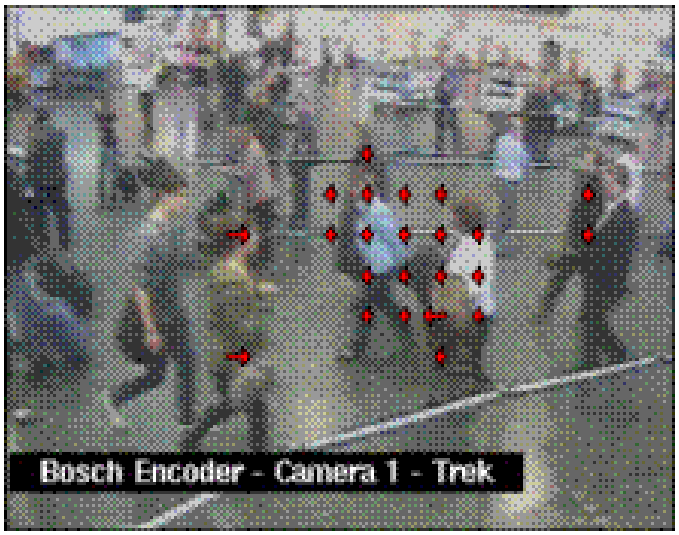


Figure 2 – Any flow detection

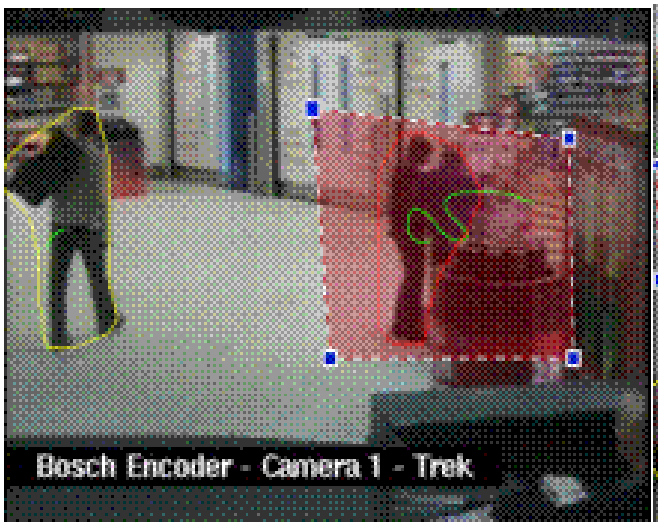


Figure 3 – Loitering detection

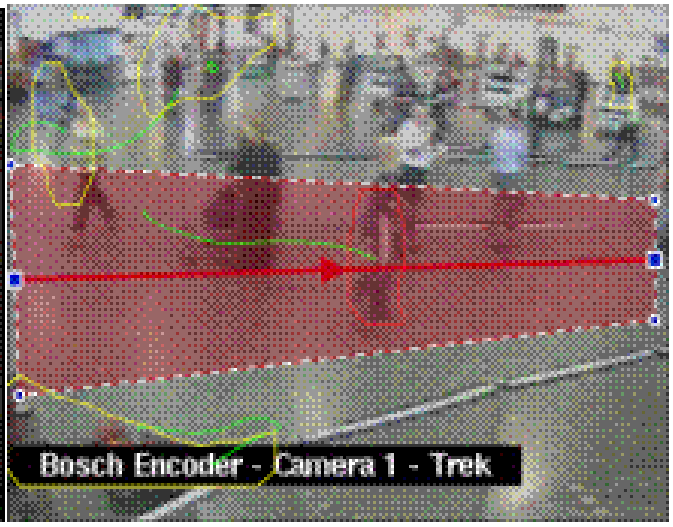


Figure 4 – Flowing Traffic direction detection

2.2.1 List of Video Analytics tasks

In the following we summarize the list of the most offered Video Analytics tasks, as provided in the commercial products description, based on the overview of 44 companies working in this area.

Unattended/Left-Behind Baggage Detection

> **Description**: refers to a person who carries a baggage and left it in the scene while he/she exits the area of interest.

Person Tracking in non-crowded and crowded environments

Description: refers to a person isolated and tracked while he/she stays in the scene.

Person-baggage Tagging (Association)

Description: refers to a couple person/baggage where the person left behind the baggage while he/she stays in the area of interest. The Video Analytics keeps an association between the person and his/her baggage.

Object Removal Detection

Description: refers to object that was previously present in the scene and is removed from his location.

Loitering Detection

Description: refers to a person who stays in a same area for a certain period of time.

Tail-gating Detection

Description: refers to a person or a vehicle that follows closely on the tail of another to gain access and attempts to circumvent access control.

Tamper Detection

Description: refers to an object put in front of the camera closing the field of view of the lens.

The above list is not exhaustive: other Video Analytics functions are provided by companies but these functions appear more specific.

2.2.2 Variations in Definition of Video Analytics tasks

There is no consensus on the VA terminology across the industry, so it is difficult to fairly compare the products. Similar functionality can be referred to in multiple manners. Additionally, the same term may be used to refer to different capabilities.

For example, “Object Put” and “Object Left Behind” may be similar or very different, depending on the scenario and definition chosen. In the first case, we only consider the status of the object in the scene as in the second case we consider the actor that put the object in order to know if the object is left (behind). In both cases the object can be considered as “put” in the scene and may create some ambiguity in the decision making.

2.2.3 Standardization of the Video Analytics tasks definition

Choosing a Video Analytics technology to solve a problem for a client is challenging since there is no standard in the level and the way of defining the event.

The National Institute of Standards and Technology (NIST) put an effort to standardise some Video Analytics events terminology in the TRECVID VA competition conferences that it organizes every year. It can be observed however that the list of Video Analytics events proposed by the NIST is not well aligned with the lists found in commercial product descriptions.

NIST describes events in a business-oriented manner, whereas industry uses inconsistent definitions with varying levels of business and technical language.

Ex1. “Person Run” is more business related whereas “Object Speed Change” or “Object Size Change” is more technically related.

Ex2. “Cross Fence detection” is more business related whereas “Cross Line detection” is more technically related.

2.2.3 Mapping of companies per tasks

Table 2 presents 44 Video Analytics vendors surveyed over the Internet. The column headings present some of the main common Video Analytics functionalities described above. For each company, the second, third and fourth column of the table puts emphasis on the existence of the VMS manufacturer partnership, while the other columns show (by `X`) the Video Analytics functions provided.

From Table 2 we can see that about 26 companies out of 44 (59.1%) surveyed in the study partner with an VMS manufacturer. This shows that VMS environment is a strategic criteria in choosing Video Analytics in order to have a full integration of the solution and to be able to run all capabilities of the VA with operational surveillance system.

Table 3 shows the number of companies that perform each of listed VA tasks . It can be seen from the table that the functions that are most commonly offered by industry are the following.

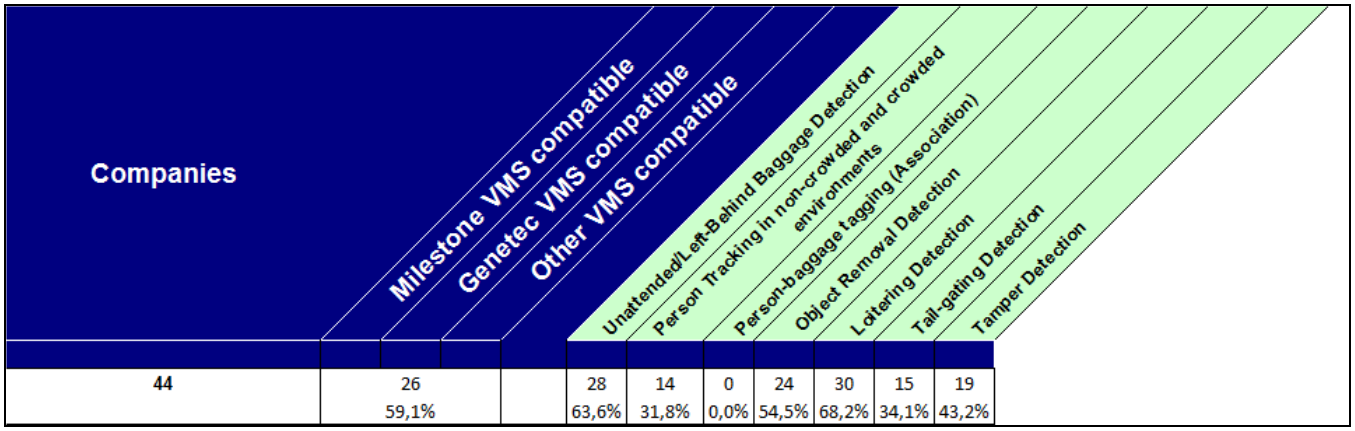
- Loitering Detection (68.2%)
- Unattended/Left-Behind Baggage Detection (63.6%)
- Object Removal Detection (54.5%)
- Only around a quarter of them offer the following functions:
- Tamper Detection (43.2%)
- Tail-gating Detection (34.1%)
- Person tracking in non-crowded and crowded environments (31.8%)

At the time of this writing none of the surveyed vendors offered “Person-baggage tagging (Association)”.

Table 2- List of VA companies mapped on VA tasks

Company	Milestone VMS compatible	Genetec VMS compatible	Other VMS compatible	Unattended/Left-Behind Baggage Detection	Person Tracking in non-crowded and crowded environments	Person-baggage tagging (Association)	Object Removal Detection	Loitering Detection	Tail-gating Detection	Temper Detection
3VR				X	X		X	X		
ACIC	X	X	X	X	X		X	X		
Acuity							X	X		
Agent VI	X	X	X	X	X		X	X	X	
All Go Vision	X	X	X	X			X	X	X	X
Arti-Vision	X									X
Aug Signals				X	X		X			
Aventura				X			X	X	X	
Ayonix				X			X	X	X	
BRS Labs	X	X	X							
Cisco				X			X	X		X
Delopt	X				X				X	X
Digital Barriers - Keeneo	X	X		X				X	X	X
Duos Tech					X			X		
Dvtel - IO Image	X			X	X		X	X		X
ezCCTV				X			X			
Geovision							X	X	X	X
Honeywell			X					X		X
i3 International							X	X	X	
IBM S3	X	X			X					
iCetana	X							X		X
iFacility Group	X							X		X
Indigo Vision			X	X	X					X
IntelliView				X			X	X	X	X
IntelliVision	X		X	X			X	X		X
iOmniscient	X	X		X			X			
Ipsotek	X	X	X						X	
Kiwi Security	X						X			
March Networks				X	X			X		X
Mate Intelligent Video	X			X			X	X		
Miragex				X			X	X	X	X
Nice										X
Object Video	X			X				X	X	X
Oncam Grandeye	X			X				X	X	X
Pikaia Systems			X	X	X			X		
Rep Logix	X		X							
Sightlogix	X	X	X	X	X			X		
Technoaware	X	X	X	X	X		X	X		
Vael Systems	X			X				X		
Verint				X			X	X		X
Vguard				X			X	X	X	
Video Inform					X					
Vigilant Video				X			X			
Vuetek	X			X			X	X	X	

Table 3- VA tasks that are most commonly offered.



Companies	Milestone VMS compatible	Genetec VMS compatible	Other VMS compatible	Unattended/Left-Behind Baggage Detection	Person Tracking in non-crowded and crowded environments	Person-baggage tagging (Association)	Object Removal Detection	Loitering Detection	Tail-gating Detection	Tamper Detection
44	26 59,1%			28 63,6%	14 31,8%	0 0,0%	24 54,5%	30 68,2%	15 34,1%	19 43,2%

2.3. Example case study

In 2006 at the Madrid’s Barajas International Airport a terrorist attack killed 2 people, injured 26 others while destroying 60% of the parking lot building and part of the terminal. Following this event Iberia Airline Company decided to improve their security level not only by installing more cameras but also by using Video Analytics technology. They selected the VI-System and its Agent VI’s real-time video analytics solution. Analytics rules applied to the cameras in Liberia Airlines facilities include:

- Person/vehicle moving in an area,
- Person/vehicle crossing a line.

Security manager at Liberia Airlines commented that “moving to an all IP-Based solution required that we look for a highly-scalable video analytics offering that would allow as to deploy hundreds of cameras while eliminating the need for additional server hardware and keeping operational costs down. Analytics have performed extremely well despite the challenging outdoor environment near a busy airport”.

2.4. Conclusions

There is substantial evidence showing the use of some of Video Analytics technologies in video surveillance of protected or limited access premises. There however very little evidence showing the use of Video Analytics technologies in monitoring public places.

3. Technology demonstrations

In this section the VA technologies developed by the CBSA for the demonstration of the highest achievable TRL are described. The development of technologies is done by CBSA-S&E Video Surveillance and Biometrics (VSB) section research scientists and engineers based on the commercially available products and the in-house developed Video Analytic Platform (VAP) [1-2].

3.1 Camera tampering detection and traffic statistics: VAP Pilot at 14 Colonnade

Installation details:

Entrance Camera: A camera (Entrance Camera) is installed on a tripod at the entrance of 14 Colonnade Room 210 (as shown in the figure at left) to view the people traffic through the entrance door. This camera is connected via IP experimental “orange” network to an experimental “orange” desk-top computer which will run VAP software (VAP pilot computer). The information from this camera is processed by VAP in real-time and the processing results is shown on a screen (VAP Pilot Screen) using VAP Browser and the commercial Video Management System software Milestone.

The extracted and saved information (meta-data) include timestamp of the detected person motion and the timestamp of the camera mal-functioning (including tampering). **No images are stored from this camera**. For debugging purpose, the program may save a tiny black-and-white image from the video (not more than 16x12 pixels) which if required can be deleted after not more than 24 hours.

Lab Cameras: In addition to the Entrance camera, several cameras from the VSB Lab (Lab Cameras) is also connected to the VAP Pilot Computer and the results obtained from those cameras is also displayed on VAP Pilot Screen.

With the consent from all VSB members, the images from the Lab cameras are saved in addition to the extracted meta-data.

VAP Screen and VAP Pilot computer: The data captured by VAP are stored on VAP Pilot computer, which is a desktop machine located in the Room that is accessible and can be logged only by VSB members.

This computer runs both modules of the VAP: the video analytic module called VAP Capture, which processes the video and extracts metadata, and the visual analytic module called VAP Browser which displays the extracted data and images (when available).

VAP Screen, located at the entrance of 14 Colonnade, is connected to the VAP Pilot computer using the 100ft VGA cable, as a second monitor. The control of all displayed information will be done from the VAP Computer.

The type of displayed information is shown in figures below. It can be switched from Event View to Time-line View, to Visual Statistics View.

Figure 5: **Event View (Entrance Camera).**

Figure 6: **Event View (Lab Camera).**

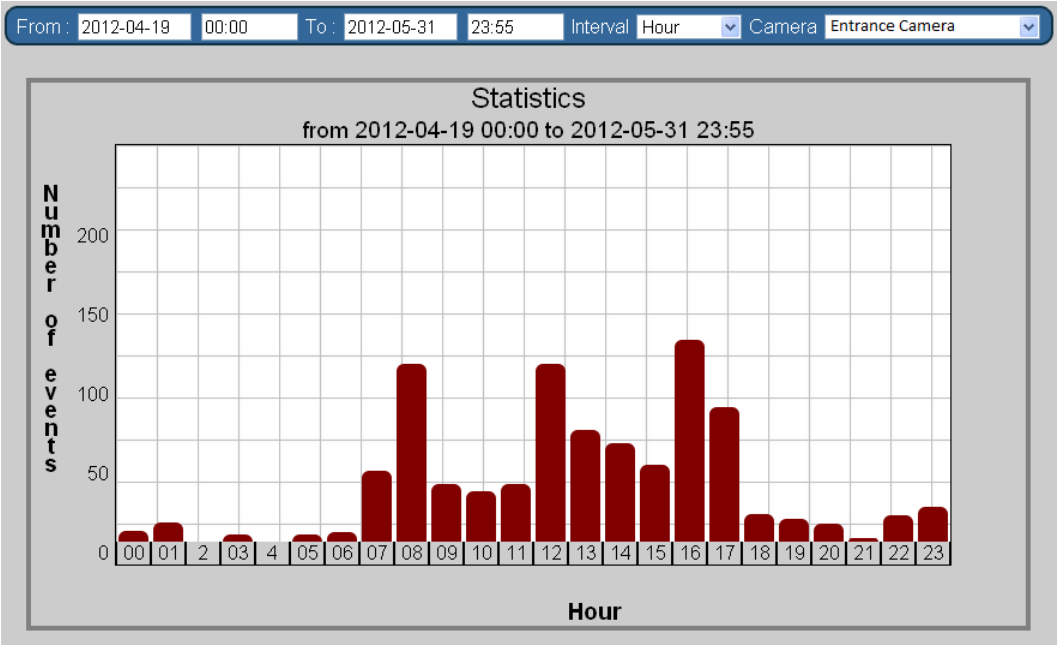


Figure 7: **Visual Statistics View.**

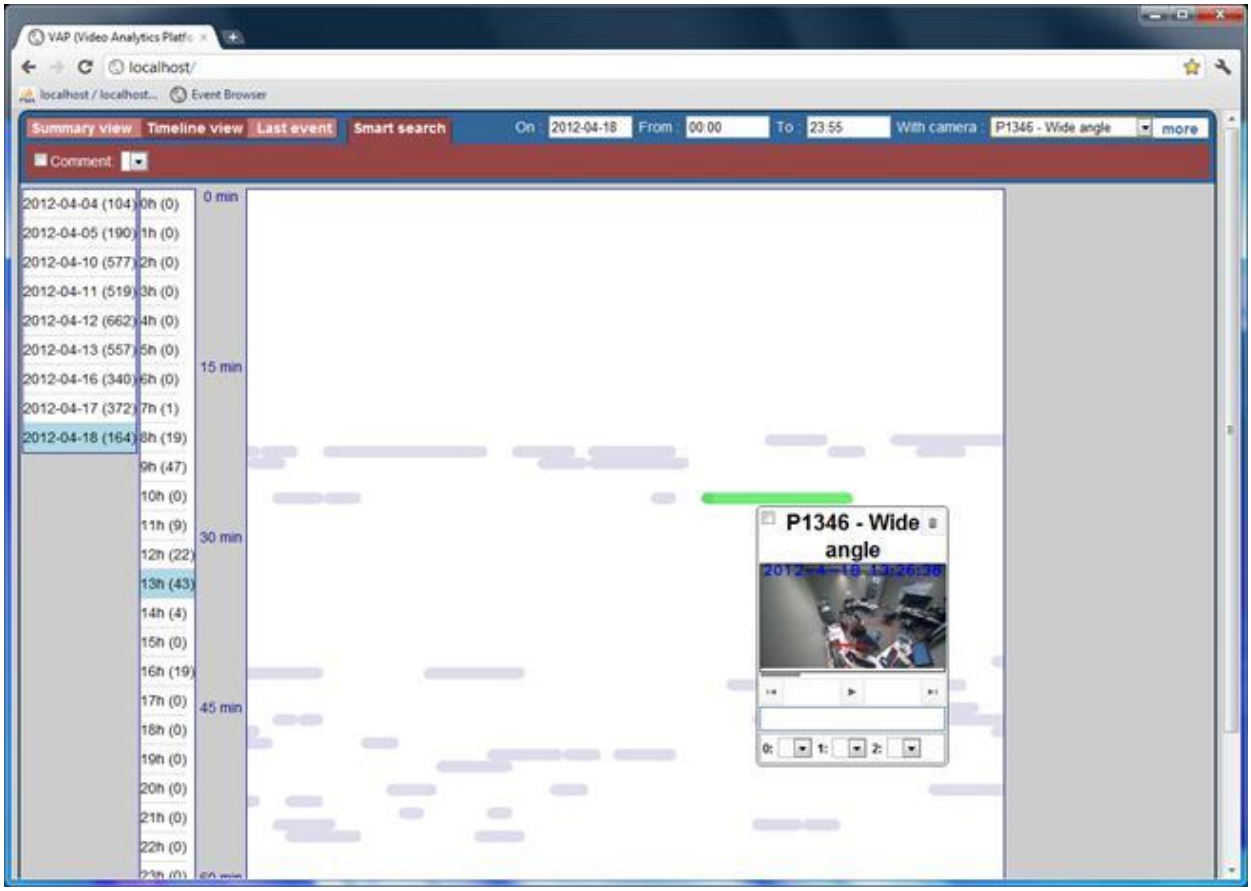
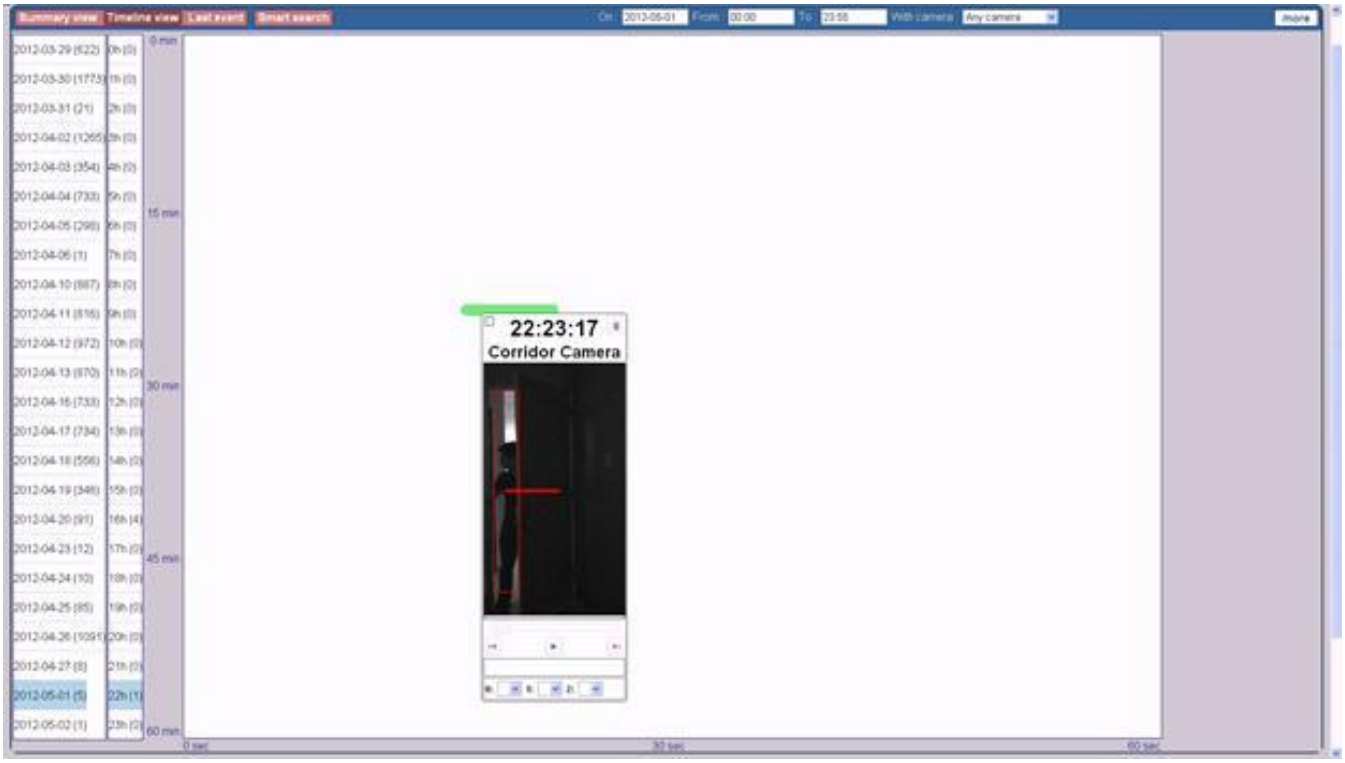


Figure 8: **Timeline View.**

3.2 Low-bandwidth remote surveillance with people detection alarm

The VAP software has been applied to address the operational need to view remotely who is visiting the premises after work hours.

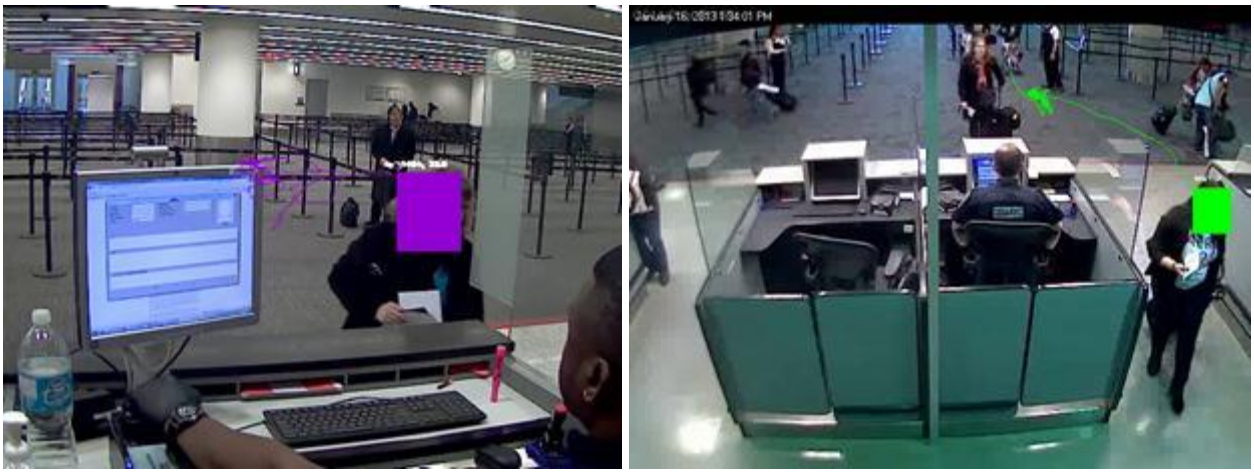
The VAP software was tuned to capture and transfer the images of moving objects via a secure IP channel. Because video data was not transmitted, but only the JPG images were transmitted, the system offered a solution to viewing remote locations, which have limited bandwidth connection.



3.3 Measuring PIL processing time and counting people

The VAP software has been used to address one of the operational needs of the CBSA related to the analysis of traveller processing time at Primary Inspection Lane (PIL), where the passport check is performed.

A COTS face detection SDK has been integrated with VAP and combined with object tracking modules in order to compute the time spent by travellers in front of the PIL.



2.4 Detection of events in simple environments with COTS VA-on-the-edge cameras

VA from Bosch COTS on-the-edge camera/encoder was tested in a variety of settings with in mock-up datasets and video recorded from operations .

The detection of the following events has been analyzed:

- object put
- object removed,
- idling
- loitering,
- person run
- wrong direction

It has been found that detection of these event is possible (TRL=5 or higher) in simple environments with little traffic and controlled lighting and traveller motion patterns

However, the detection of the same events in more challenging settings such as those observed with cameras installed in airports has not showed the readiness of the technology for these settings, unless an intensive manual filtering of false alarms is performed by a human operator, similar to the technique described in TRECVID evaluation, where VAP Browse is used to remove false alarms.

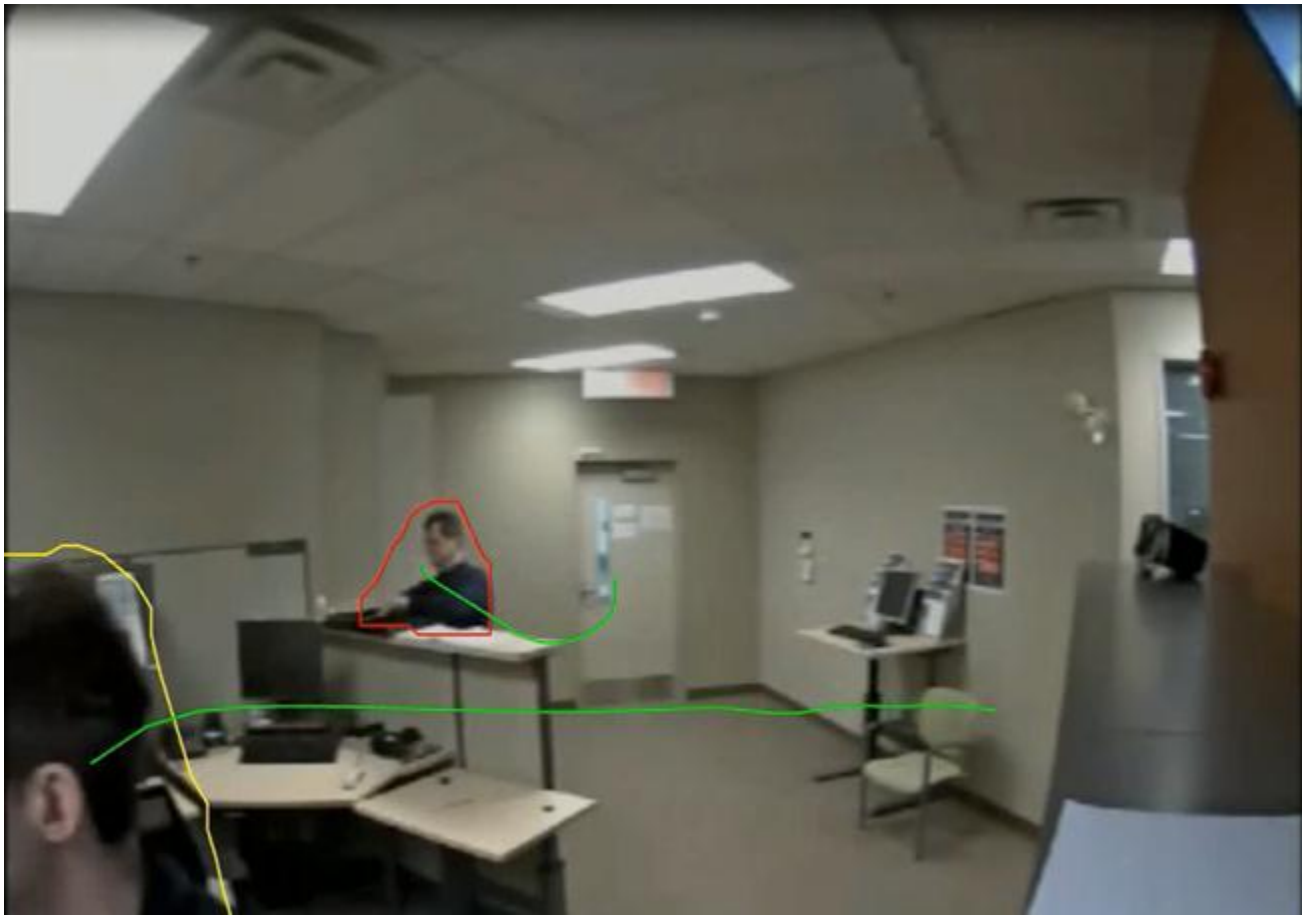


Figure 9: Testing of person loitering.

Figure 10: Testing of object removed.

Figure 11: Testing of put object.

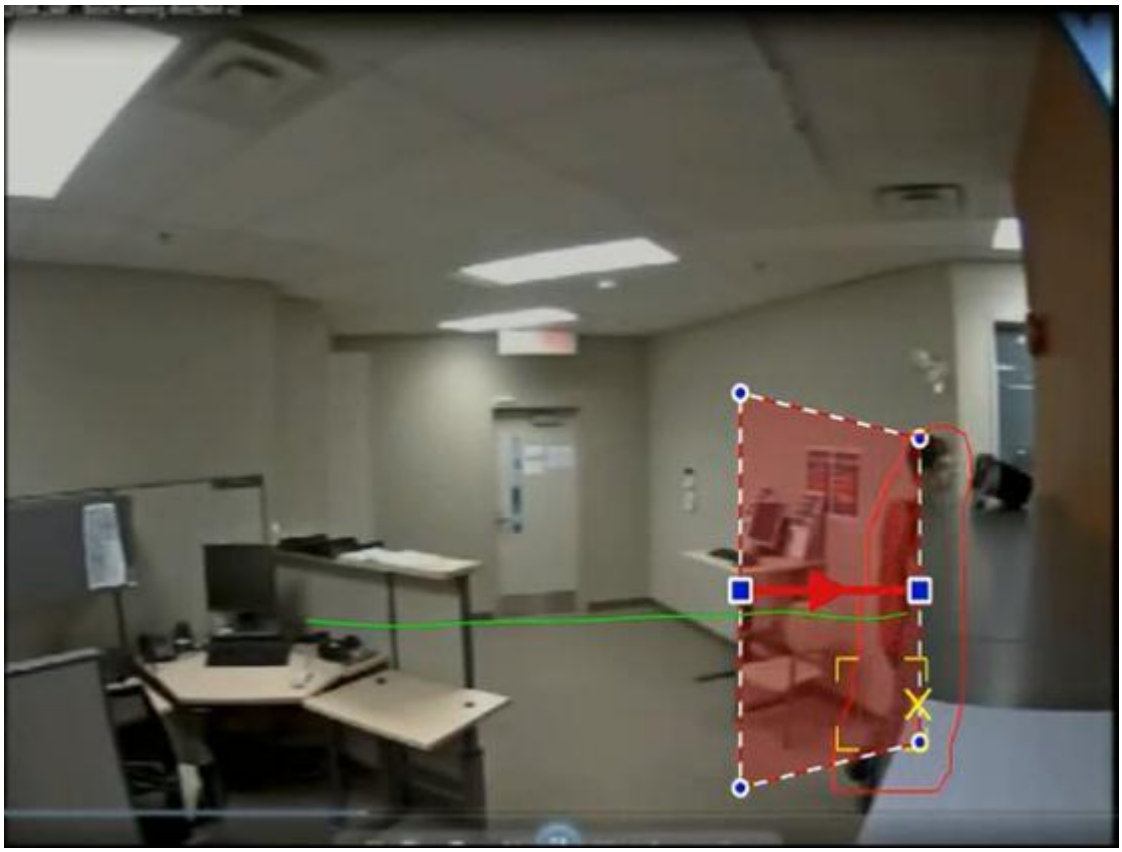


Figure 12: Testing of wrong direction.

4 VT4NS’13 demonstrations

The following VA technology demonstrations have been prepared for sharing with the project partners :

1. Measuring PIL processing time and counting people (tested in operational environment) – in-house developed VA + COTS Face Detection integrated on VAP.

2. Low-bandwidth remote surveillance with people detection alarm (tested in ops. environment) – in-house developed VA integrated on VAP.

3. Camera tampering detection and traffic statistics (Pilot on Colonnade) – in-house developed VA integrated on VAP.

4. CBSA-uOttawa participation at NIST TRECVID Interactive Surveillance Event Detection evaluation: “Person run and other event detection in complex environment using Visual Analytics” – see [6] for more details.

5. Detection of abandoned objects in simple environments with COTS VA software – evaluation of COTS VA products by CRIM.

6. Detection of events (object put/removed, idling/loitering, person run/wrong direction) in simple environments with COTS VA-on-the-edge cameras - evaluation of COTS VA products CBSA

In addition, in synergy with PROVE-IT(FRiV) project, the following technology demonstrations have been prepared on Face Recognition in Video:

1. Post-event face tagging, grouping and search– integration of COTS face recognition built with PittPatt FR SDK with VAP

2. Still-to-video watch-list screening: binary decision making – in-house built solution using Cognitec FR SDK

3. Still-to-video watch-list screening: triaging -– in-house built solution using Cognitec FR SDK

4. Video-to-video face recognition and triaging decision-making – developed by project partner ETS and TAMALE

VAP refers to the **Video Analytic Platform** that is developed by CBSA-S&E for integration of custom-made and third party VA and FRiV codes into operational CCTV IP-based video surveillance networks. It consists of two modules: **VAP Capture**, where VA and FRiV codes are executed, and **VAP Browser**, which is the state-of-art Visual Analytic s GUI data mining / filtering end-user tool. For more information on VAP see [1-3] and Appendices A-C.

These demonstrations have been recorded as AVI files and archived at VT4NS portal (https://partners.drdc-rddc.gc.ca/css/Portfolios/Biometrics/VT4NS) and on CBSA-S&E o:drive, as shown below:

Dmitry Gorodnichy *et al*, “Video Analytics technology: the foundations, market analysis and demonstrations"

VT4NS

Home

Technology Demonstrations

Type	Name	Modified By
	13-Watchlist-Part3-CBSA-Type2-Entrance-all	Dmitry Gorodnichy
	13-Watchlist-Part2-CBSA-Type2-one-at-time	Dmitry Gorodnichy
	13-WatchList-Part1-ChokePoint-all	Dmitry Gorodnichy
	13-WatchList-testing-multi-face-detection-tracking-matching	Dmitry Gorodnichy
	13-Face-Search-Part2(detect-more-with-FAR=0.1)	Dmitry Gorodnichy
	13-Face-Search-Part1(detect-with-FAR=0.01)	Dmitry Gorodnichy
	WATCH-LIST-Chokepoint-vs-Chokepoint+VSB+CBSA-binary	Dmitry Gorodnichy

Add new document

VT4NS 2013 - PROVE-IT(VA/FRiV) reports

Type	Name	Modified By
	Partner-ETS-FRiV	Dmitry Gorodnichy
	CBSA-demo-FR-Watchlist(WANTEDbyCBSA+Chokepoint+VSB)	Dmitry Gorodnichy
	CBSA-demo-FR-3-triagingGUI-wChokepoint	Dmitry Gorodnichy
	CBSA-demo-FR-3-triagingGUI-wCBSAdata	Dmitry Gorodnichy
	Partner-CRIM-VA-ObjectPut	Dmitry Gorodnichy
	CBSA-demo-FR-3-WatchList-GUI-tool	Dmitry Gorodnichy
	CBSA-demo-VA-3-2-VAPPilot-TamperingDetection	Dmitry Gorodnichy
	13-PROVE-IT(FRiV)-Results	Dmitry Gorodnichy
	13-VT4NS-Intro-PROVE-IT()-framework	Dmitry Gorodnichy
	13-PROVE-IT(VA)-Results	Dmitry Gorodnichy
	CBSA-demo-FR-2-2-WatchList(CBSA+ChokePoint+VSB)-EventBrowser	Dmitry Gorodnichy
	CBSA-demo-FR-1-PostEvent-FaceSearch-VAPBrowser2	Dmitry Gorodnichy
	PROVE-IT(VA)-FinalReport-v0.5 - ToC+Summary	Dmitry Gorodnichy
	PROVE-IT(FRiV)-FinalReport-v0.6 - ToC+Summary	Dmitry Gorodnichy
	Partner-TAMALE-FR-Candide	Dmitry Gorodnichy
	Partner-VIVA-VA-presentation	Dmitry Gorodnichy
	PROVE-IT(VA)-FinalReport-v0.5	Dmitry Gorodnichy
	PROVE-IT(FRiV)-FinalReport-v0.6	Dmitry Gorodnichy
	CBSA-demo-VA-2-PeopleDetection-VAPBrowser-Timeline	Dmitry Gorodnichy
	VT4NS'13-TRL-results-for-discussion-only-v0.2	Dmitry Gorodnichy

(More Items...)

Add new document

Relevant Links

- gcpedia CBSA Biometrics
- gcpedia CBSA Video Surveillance
- Link to VT4NS 2007 page (First VT4NS Meeting)

Add new link

PROVE-IT(VA/FRiV) reports & presentations

Type	Name	Modified By
	12-Biometric-Summit-Talk-Gorodnichy-workbook	Dmitry Gorodnichy
	12-NIST-PROVEIT(FRiV)-v1	Dmitry Gorodnichy
	12-NIST-TRL-based-evaluation-v1	Dmitry Gorodnichy

Add new document

Related documents (Repository)

Type	Name	Modified By
	NRC_Video Recognition Systems_2006	Jonathon Lee
	LSSD-Nato2008-ACE	Jonathon Lee
	Transport Canada_CCTV Manual	Jonathon Lee
	Video Analysis and Content Extraction_brochure	Jonathon Lee
	10-SPIE-VAP-P	Dmitry Gorodnichy

Add new document

Site Users

VT4NS 2011

Type	Name	Modified By
	VT4NS'11-report-minutes	Dmitry Gorodnichy
	CRIM-ProveIT-VA_Kick-off	Dmitry Gorodnichy
	VT4NS'11-agenda+minutes	Dmitry Gorodnichy
	11-VT4NS-1-intro-Recap-of-past-ourcomes	Dmitry Gorodnichy
	11-VT4NS-2-FR-inside-the-BlackBox	Dmitry Gorodnichy
	11-VT4NS-3-PROVE_IT-Tasks	Dmitry Gorodnichy
	11-VT4NS-4-SurveyResults-so-far	Dmitry Gorodnichy
	ETS-intro	Dmitry Gorodnichy
	ETS-FRiV-results	Dmitry Gorodnichy
	uOttawa(VIVA)	Dmitry Gorodnichy
	uOttawa-TAMALE	Dmitry Gorodnichy
	RCMP-Main Qualitative Review of FR Technology	Dmitry Gorodnichy
	DRDC-Ottawa	Dmitry Gorodnichy
	DRDC-Valcartier	Dmitry Gorodnichy
	PROVE-IT_VA_-FactSheet+Summary	David Bissesssar
	PROVE-IT(FRiV)-FactSheet+Summary	David Bissesssar
	VT4NS'11-agenda-REVISED-Sept22	David Bissesssar
	VT4NS'11-agenda-Sep12	David Bissesssar

Add new document

VT4NS 2010

Type	Name	Modified By
	Attendees_VT4NS_2010	Jonathon Lee
	Agenda_VT4NS_2010	Jonathon Lee
	CFP_VT4NS_2010	Jonathon Lee
	10-06-VSB-QuadCharts-Demos-BestVA_applications	Dmitry Gorodnichy
	CBSA-S-E	Dmitry Gorodnichy
	CBSA-Ops-POE and AV	Dmitry Gorodnichy
	Privy-PrivacyIssues	Dmitry Gorodnichy
	RCMP-AV-VT4NS_2010	Dmitry Gorodnichy
	CATSA-DRDC Presentation	Dmitry Gorodnichy
	TC-VT4NS10	Dmitry Gorodnichy
	10-06-VT4NS-intro-to-VSB-VAT	Dmitry Gorodnichy
	10-06-VT4NS-intro-to-VA-TRL	Dmitry Gorodnichy
	10-06-VT4NS-intro	Dmitry Gorodnichy
	10-06-VT4NS-handout	Dmitry Gorodnichy
	video analytics IPS Tech UK 2010	Meunier, Pierre
	Vallerand CSS in VT4NS 20100530	Meunier, Pierre
	FinalMediaPlayerSetup	Meunier, Pierre
	IPS-CCTV-Intelligent-Video-Analysis-System	Meunier, Pierre

Add new document

VT4NS_2008

Type	Name	Modified By
	Intelligent Surveillance_Dmitry Gorodnichy	Jonathon Lee
	CBSA_LAB Overview	Jonathon Lee
	CBSA_Video Technology	Jonathon Lee
	CRC_overview	Jonathon Lee
	CRIM_Projects in Video Analysis	Jonathon Lee
	DRDC_Non-Cooperative Target Recognition	Jonathon Lee
	DRDC_Pace-Imaging	Jonathon Lee
	DRDC_Qinghan_FaceRec	Jonathon Lee
	IARPA_CV	Jonathon Lee
	RCMP_Audio and Video Analysis	Jonathon Lee
	RCMP_Video management software evaluation Project	Jonathon Lee
	VT4NS Conference Introduction	Jonathon Lee
	VT4NS_08_Program	Jonathon Lee
	VT4NS_08_Attendees	Jonathon Lee

Add new document

VT4NS 2007

- VT4NS 2007 Attendees, Agenda, Presentations

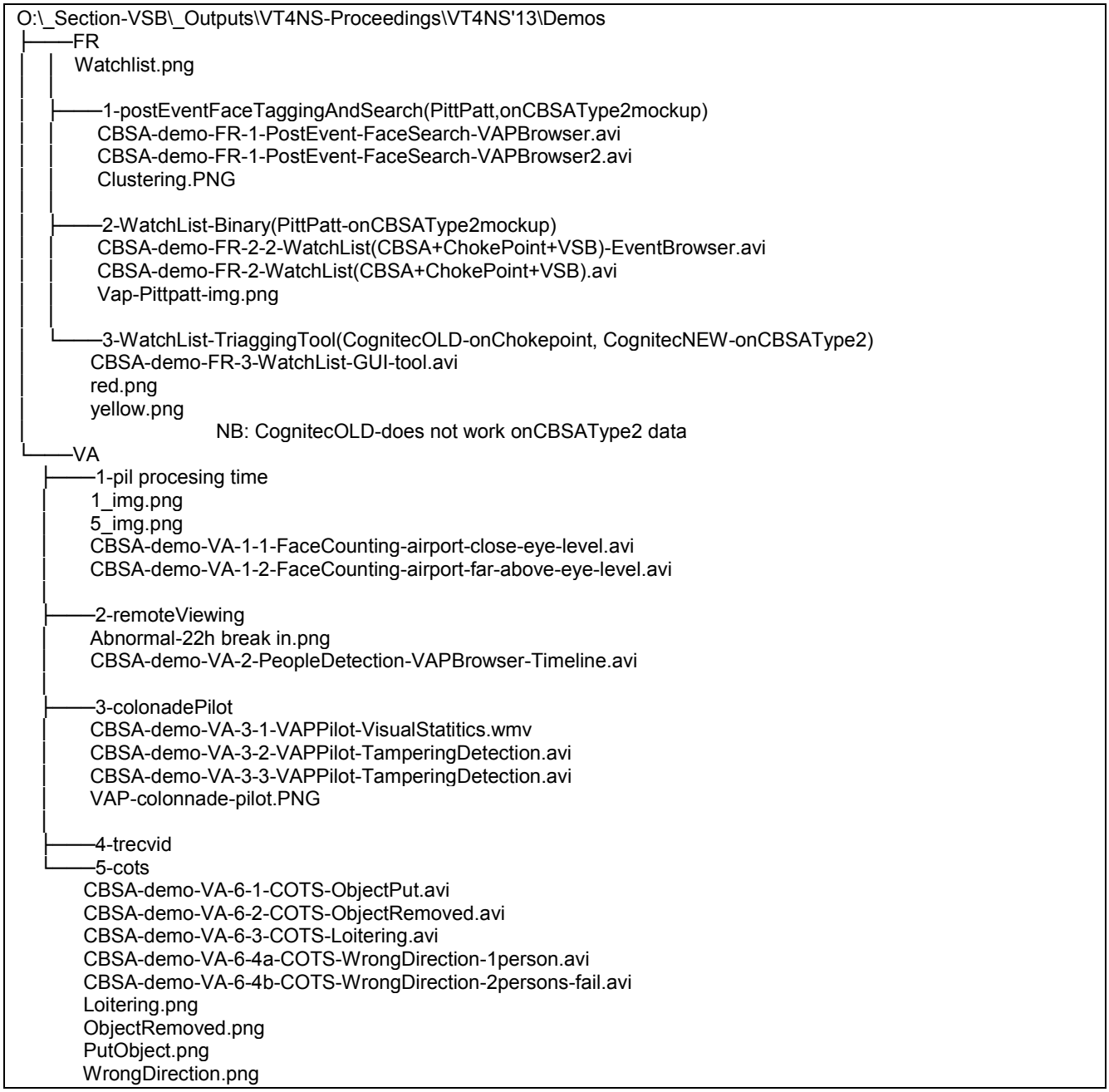


Figure 13: The archival structure of the VT4NS proceedings and the PROVE-IT() reports and demonstrations on the DRDC SharePoint Portal (previous page) and CBSA internal hard-drive (this page).

References

[1] Dmitry O. Gorodnichy and Elan Dubrofsky. "Automated extraction of intelligence from video using Video Analytics Platform (VAP)". (Extended Abstract & Demo), Justice Institute of British Columbia and the U.S. Department of Homeland Security's Center of Excellence VACCINE Workshop on "Visual Analytics for Public Safety Professionals", September 20 -21, New Westminster, BC, 2010

[2] Dmitry O. Gorodnichy and Elan Dubrofsky. VAP/VAT: Video Analytics Platform and Testbed for testing . Proceedings of SPIE Conference on Defense, Security, and Sensing, DS226: Visual Analytics for Homeland Defense and Security track. 5 - 9 April 2010, Orlando

[3] Dmitry O. Gorodnichy, Tony Mungham, "Automated video surveillance: challenges and solutions. ACE Surveillance (Annotated Critical Evidence) case study", NATO SET-125 Symposium "Sensor and Technology for Defence against Terrorism", Mainheim, April 2008.

[4] Dmitry O. Gorodnichy, Mohammad A. Ali, Elan Dubrofsky, Kris Woodbeck. **Zoom on the evidence with ACE Surveillance.** International Workshop on Video Processing and Recognition (VideoRec’07). May 28-30, 2007. Montreal , QC , Canada . [Pdf and Poster]

[5] Dmitry O. Gorodnichy, **ACE Surveillance: The Next Generation Surveillance for Long-Term Monitoring and Activity Summarization.** First International Workshop on Video Processing for Security (VP4S-06), June 7-9, Quebec City, Canada. [Pdf]

[6] C. Whiten, R. Laganiére, E. Fazl-Ersi, F. Shi G. , Bilodeau, D. O. Gorodnichy, J. Bergeron, E. Choy, D. Bissessar . “VIVA-uOttawa / CBSA at TRECVID 2012: Interactive Surveillance Event Detection”. On line at http://www-nlpir.nist.gov/projects/tvpubs/tv.pubs.12.org.html (http://www-nlpir.nist.gov/projects/tvpubs/tv12.papers/viva-uottawa.pdf)

Appendix A: Fifth Interdepartmental Conference on Video Technologies for National Security (VT4NS 2013), March 2013

Agenda

Foreword Presentation

“PROVE-IT() Framework”

By D. Gorodnichy

Gov't departments and By invitation only

Fifth Interdepartmental Conference on

Video Technologies for National Security (VT4NS 2013)

Theme: **Presentation and review of PROVE-IT (FRiV/VA) projects results.**
PSTP BIOM-401: Real-time Face Recognition Technologies for Video-surveillance Applications
PSTP BTS-402: Video Analytics for Border and Transportation Security in Indoor and Outdoor Environments

When: Wednesday, 27 March, 2013. 8:30 – 16:30

In Person: DRDC-CSS, 222 Nepean Str

Via Telecom: Call-in toll-free number: 1-877-413-4788 / Call-in number: 1-613-960-7513
Attendee access code: 947 417 6

Portal: https://partners.drdc-rddc.gc.ca/css/Portfolios/Biometrics (Human ID Systems)/VT4NS
(will be provided in separate email)

Organized by:
- Defence R&D Canada's Centre for Security Science (DRDC-CSS), and
- Canada Borders Services Agency's Scientific and Engineering Directorate (CBSA-S&E)

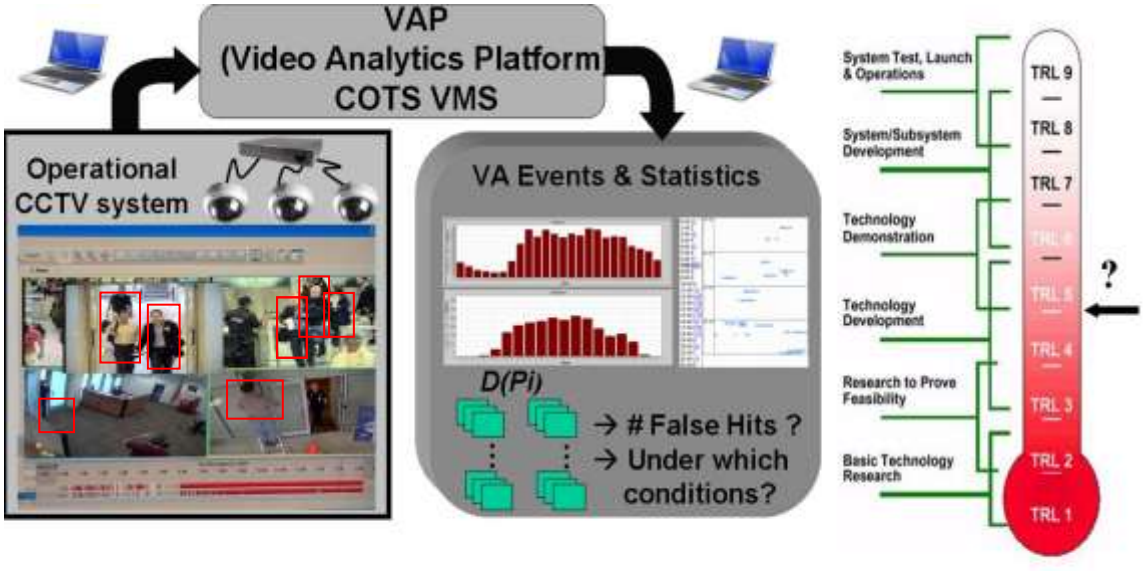
Chairs:
- Dmitry O. Gorodnichy: dmitry.gorodnichy@cbsa-asfc.gc.ca
- Pierre Meunier: pierre.meunier@drdc-rddc.gc.ca

Facilitator:
- David Bissessar: david_bissessar@hotmail.com

Scope and Objectives:

As in the past, the primary objective of this conference is to bring together GoC Border and Transport Security (BTS) and Biometrics (Biom) Communities of Practice (CoP) in) for the exchange of information on the activities, needs, and interests related to *deploying video surveillance technology* within GoC - in particular, in the area of Video Analytics (VA) and Face Recognition in Video (FRiV).

The secondary objective is to present and discuss the findings from the DRDC-CSS-funded PROVE-IT() projects led by CBSA-S&E in partnership with Academia and federal partners related to TRL assessment of VA and FRiV technologies.



Attendees:

In person: CBSA, DRDC, DND, RCMP, PCO, CATSA, Public Safety, TC, DFAIT
Dial-in: HomeOffice, FBI, NIST, AFP

Tentative Program (time indicated as guideline only)

8:30 Introductions, Foreword – CSS, CBSA-S&E

9:00 PROVE-IT() objectives, framework and findings - CBSA-S&E
- Main objective: Find technologies/applications/settings { Xi: TRL(Xi)>4 }
- Tools: VAP, Visual Analytics, COTS products, academia partners work
- Main results: TRL(VA/FRiV) assessment tables and technology demonstrations

10:00 Presentations from project contributors:
- PROVE-IT(FRiV) – ETS and uOttawa-TAMALE
- PROVE-IT(VA) - uOttawa-VIVA and CRIM
- Presentations from other project partners (TBC)

12:00 Technology demonstrations

12:30 Lunch (not provided)

For Government attendees only:

13:30 Technology demonstrations (continued)
15:00 Round table discussion, review of results, next steps
- Presentations from other project partners (TBC)

16:30 Adjurn

Technology demonstrations
(most demonstrations will be pre-recorded and will be uploaded to the Portal along with all presentations)

VA:

1. Measuring PIL processing time and counting people (tested in ops. environment) – VA+COTS FD on VAP
2. Low-bandwidth remote surveillance with people detection alarm (tested in ops. environment) – VA on VAP
3. Camera tampering detection and traffic statistics (Pilot on Colonnade) – VA on VAP
4. CBSA-uOttawa participation at NIST TRECVID Interactive Surveillance Event Detection evaluation: Person run and other event detection in complex environment using Visual Analytics – by VIVA and CBSA
5. Detection of abandoned objects in simple environments with COTS VA software – by CRIM
6. Detection of events (object put/removed, idling/loitering, person run/wrong direction) in simple environments with COTS VA-on-the-edge cameras - by CBSA

FRiV:

1. Post-event face search and retrieval – with PittPatt SDK and VAP
2. Still-to-video watch-list screening: binary decision making – with Cognitec SDK
3. Still-to-video watch-list screening: triaging - with Cognitec SDK and new end-user interface
4. Video-to-video face recognition – ETS / TAMALE

VAP refers to the **Video Analytic Platform** that is developed by CBSA-S&E for integration of custom-made and third party VA and FRiV codes into operational CCTV IP-based video surveillance networks. It consists of two modules: **VAP Capture**, where VA and FRiV codes are executed, and **VAP Browser**, which is the state-of-art Visual Analytic s GUI data mining / filtering end-user tool.

CBSA ASFC
PROTECTION • SERVICE • INTEGRITY

Fifth Interdepartmental Workshop on

Video Technologies for National Security (VT4NS'13)

March 27, 2013, Ottawa

Organized by CBSA-S&E and DRDC-CSS

Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

Welcome!

CBSA ASFC

Gov't:

- DRDC-CSS
- CBSA NHQ S&E: VSB
- CBSA NHQ Solutions
- CATSA
- TC
- DFAIT
- RCMP
- Public Safety
- Office of the Privacy Commissioner

Academia / Industry:

- ETS
- uOttawa TAMALE Lab
- uOttawa VIVA Lab
- CRIM

International:

- HomeOffice
- FBI
- NIST
- AFP

VT4NS: outcomes

CBSA ASFC

2007: by NRC with US IARPA / VACE:
- first (live) demo of VA (inc. Face detection and annotation in video)
- first population of issues / first call for coordination of efforts

2008: by CBSA-S&E with DHS, IARPA
- Theme: "Building future-proof video surveillance systems (VSS)"
- Addressing CBSA's need in VSS upgrades

Outcomes: Recommendation on Open Architecture systems
- which allows integration of VA & in-house testing / pilot

2010: by DRDC-CSS & CBSA-S&E
- Theme: "***Moving Video Analytics into operational environment.*** / ***"Faces in video"***
- Presentation: "*Video Analytics: inside the Black Box*"
- (re-) Introducing TRL for VA testing
- Demonstration of CBSA's Video Analytics Platform (VAP)
- Brain-storming: in search for "killer" (best) VA applications

Outcomes: SoW for two new PSTP studies

VT4NS: outcomes (cntd)

CBSA ASFC

2011 Sept: by DRDC-CSS & CBSA-S&E
- Theme: Kick-off of ***PSTP BIOM401 & BTS402 Studies***
- Presentation: "*Face Recognition: inside the Black Box*"
- Demos of FR COTS systems for "watch list" screening (issue)
- Discussion on other FR deployment issues

2013 March: by DRDC-CSS & CBSA-S&E
- Theme: Closing of ***PSTP BIOM401 & BTS402 Studies***
- Presentations from CBSA and partners
- Demos of FRiV and VA systems with TRL > 4
- Discussion in TRL assessment results

VT4NS portal

CBSA ASFC

Presentations, demo videos, and other documents posted at

https://partners.drdc-rddc.gc.ca/css/Portfolios/Biometrics (Human ID Systems)/VT4NS

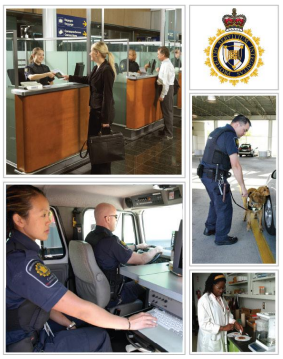
USER = "VT4NS", Password ="password"

CBSA ASFC
PROTECTION • SERVICE • INTEGRITY

Biometrics Community of Practice – Study No. 2:

Real-time Face Recognition Technologies for Video-surveillance Applications

Duration: 1 + 1year
Funds: $200K + 80 K
In-kind: $500K



Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

Objectives

- investigate and elevate, if possible, the maturity of face recognition technologies that are applicable for real-time identification of individuals using video cameras.
  - To encourage focused national and, potentially, international collaborative efforts … for identity/accreditation management and access control.
  - To recommend technological solutions to border surveillance and interdiction challenges that blend with current doctrine and technologies.

FRiV applications considered

Scope of the study: to assess how face recognition (FR) technologies can be applied to facilitate real-time recognition of individuals captured by video cameras in *applications* such as:

I. Triaging of faces according to their resemblance to a Wanted List;

II. Fusion of face recognition from different cameras while tracking

III. Face recognition-assisted tracking;

IV. Matching a face/person across several video feeds;

V. Multimodal recognition, e.g., face and voice recognition;

VI. Soft-biometric based tracking/recognition techniques.

Study deliverables

1. Identify the applications and scenarios where FR technology can be applied with existing video-surveillance (CCTV) infrastructure for instant (real-time) extraction and recognition of faces in unconstrained surveillance-type applications.
2. Investigate the applicability and feasibility of multimodal biometric recognition by combining face recognition with other modalities that are collectable in surveillance applications.
   1. Such biometric modalities may include hard biometrics modalities, such as voice, and iris, and
   2. softer biometrics modalities such as height/weight, face shape, and gait.

Study deliverables (cntd)

3. Examine the technology readiness levels (TRLs) of the FR technologies for the SIX FRiV *applications* listed in the scope, and identify those that have TRL 5 and higher, i.e., the technologies have been successfully piloted or tested in relevant or operational environments.
4. Conduct an analysis of the FR technologies listed in the scope
   1. by examining reports from trusted unbiased sources (such as government and academia organizations) or
   2. by hands-on testing of recognition technologies embedded into a common/operational video surveillance system.
5. Execute a demonstration of a video surveillance system that performs live instantaneous analysis of the observed faces.
6. Organize and host a combined workshop/information session for the CoP (approximately 30 people) to review findings.

CBSA ASFC
PROTECTION • SERVICE • INTEGRITY PROTECTION • SERVICE • INTÉGRITÉ

Border and Transportation Security – Study No. 2:

Video Analytics for Border and Transportation Security—Indoor and Outdoor Environments

Duration: 1+1 year
Funds: $200K+80K
In-kind:$300K

VA applications considered

Scope of the study: focus on the analysis of TRLs for Video Analytic technologies applied to the following border security challenges:

1. Unattended/left-behind baggage detection;
2. Person tracking in non-crowded and crowded environments,;
3. Person-baggage tagging (association) in crowded environments;
4. Object removal detection;
5. Loitering detection;
6. Tail-gating detection; and
7. Camera tampering detection.

CBSA ASFC

PSTP BIOM-401, PSTP BTS-402

PROVE-IT() Framework

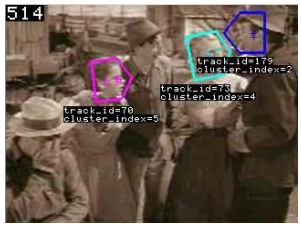
Dmitry Gorodnichy

PROVE-IT (X) key objective

find applications/technologies/scenarios/settings

Xi: {TRL(Xi)>4 }

If the technology does not work for the application …

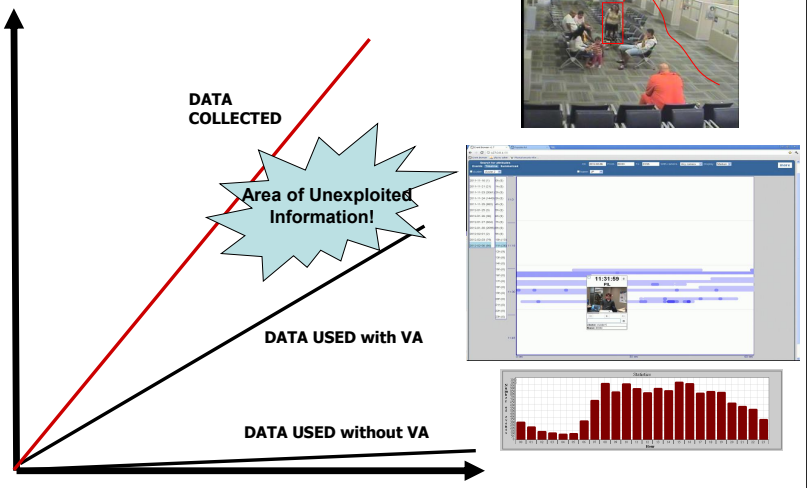


"Wizard Oz" video-clip with faces detected and clustered by COTS FR.

… there are two ways to proceed:

- Find another application!
- Find another technology!

With and without VA / FRiV



PROVE-IT (X) framework

In Search for High-TRL Applications, using :

- on Public datasets and in Mock-up setups
- with traditional and new applications
- in different Surveillance setups / scenarios
- with commercial and academic products

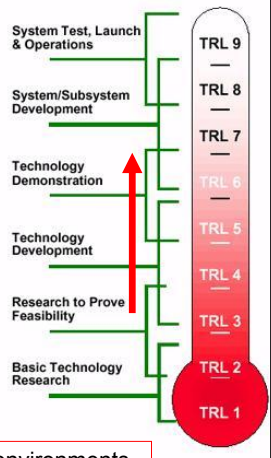
+ surveys (end-users, media, companies, academia)

Tools:

1. 5-grade TRL assessment scale
2. Taxonomy of video-surveillance setups
3. End-user software (eg. VAP)
4. TRL assessment table

Technology Readiness Level

9. Actual system 'flight proven' through successful mission operations (over 30)
8. Actual system completed and 'flight qualified' through test and demonstration.
7. System prototype demonstration in operational environment. ← PILOT
6. System prototype demonstration in relevant environment. ← MOCK-UP
5. Component validation in relevant environment.
4. Component validation in laboratory environment.
3. Analytical and experimental critical function - characteristic proof of concept.
2. Technology concept / application formulated
1. Basic principles observed and reported.



TRL-based evaluation requires access to real environments, real end-users, and real operational needs!

1. Five-point TRL assessment scheme

	Years to deploy	TRL	Additional Applied R&D requirement
++	0 (can be deployed immediately by any operational agency with no R&D capacity)	TRL=8-9, complete COTS system deployed and proved useful by many users	no development effort is required to deploy it
+:	<1 (by most operational agencies with minimal Applied R&D capability)	TRL=7-8, compete COTS system deployed somewhere	some minor development effort is required to fit business requirements
oo	1-2 (only by operational agencies that have substantial Applied R&D capability)	TRL=5-6, system validation in mock-up or pilot	solid development effort is required
o	2-3 (only by operational agencies that have access to major to Applied R&D)	TRL=4, component validation in relevant 24/7 environment	major development effort is required
-	>3 (not foreseeable for deployment in near future)	TRL=1-3	significant academic / industry R&D required

Other technology maturity criteria

- Producibility – Manufacturing Readiness
- Readiness to Receive (If Goal Is Transition from Technology Developer and Technology Receiver)
- Practice Based Technology Maturity (Emphasis on Community of Users) –
- User Readiness Program Readiness (program needs and constraints).
- R&D Readiness, which measures the in-house R&D capacity Required to deploy the technology (such as required for Customization & tuning of the technology

Biometric vs. Surveillance: objectives

Biometrics

Real-time applications

1. "Access/Border Entry Control" – in cooperative mode facilitate entry to "Travellers"
   - Iris: www.NEXUS.gc.ca)
   - Faces: ePassports
2. "Screening applications" – in non-/un-cooperative mode prevent entry to "Criminals"
   - Faces: "Wanted by CBSA"

Other applications

1. "Imposter" problem
2. For Intelligence & Enforcement

Video Surveillance

Four operational objectives:

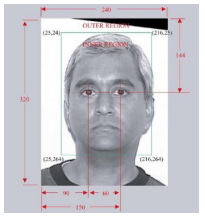
1. Observe
2. Detect (abnormality/event)
3. Recognize (event/incident)
4. Identify (individuals)

Three modes of operation:

- **Real-time Active** (24/7 live viewing)
- **Real Time Passive** (in conjunction with other duties)
- **Archival** (post-event analysis, thru recording)

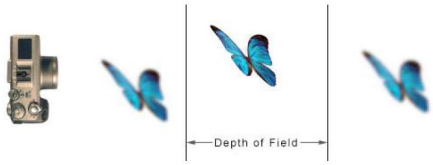
Biometric setup (Type 0)

- Faces captured in controlled environment are much easier to recognize (as in e-Gates with e-Passport)
- Photos taken in a controlled environment provide:
  - Canonical face model adopted by ICAO'02 for passport-type documents
  - high resolution - 60 pixels between eyes
  - face "nicely" positioned (front-faced, eye-level)
  - neutral facial expression
  - no occlusion (eye-glasses, scarf)
  - high quality
    - No motion – no blur
    - In focus
    - Good (best possible) illumination
    - No compression artifacts



Face resolution in surveillance video

- Basic capture principle: either blur or lack of focus !
  - The image quality of the moving object depends: aperture, exposure.



Face resolution (pixels between eyes)

- Sensor resolution: 24 – 200 pixels (1/32-1/8 frame width)

However:

- Informative resolution (aka Actual, Shannon index, Entropy-based): 10 – 46 pixels

2. Taxonomy of Surveillance setups

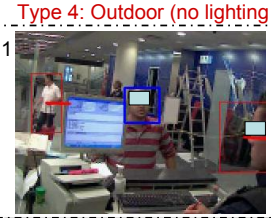
Type 0: Cooperative Biometric setup (access control, eGate)

Type 1: constrained setup
- Eg. Primary Inspection Lane (PIL)

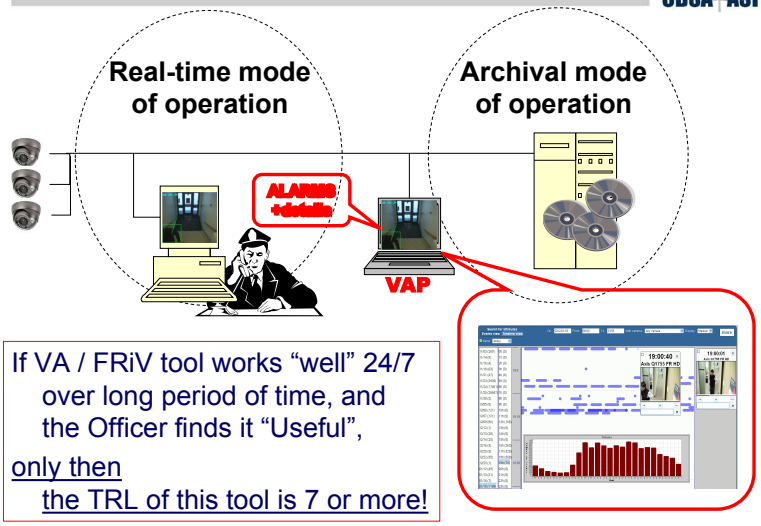
Type 2: unconstrained free-flow, one-at-time
- Eg. Port of Entry / Chokepoint entry

Type 3: unconstrained free-flow, many-at-time
- Eg. in Airport

Type 4: Outdoor (no lighting or structural constraints)



3. Testing using end-user software (VAP)



If VA / FRiV tool works “well” 24/7 over long period of time, and the Officer finds it “Useful”,

only then

the TRL of this tool is 7 or more!

VAP: Video Analytic Platform software

Developed in house for end-users in the field (to be used with existing cameras and Video Management Systems)

Consists of :

- VAP Event Capture:
  Video Recognition modules
  (includes camera tampering, people/object tracking, face detection, face matching)
- VAP Event Browser:
  Visual Analytics GUI
  (end-user interface)

GUI tools for the officer:

For Real-time mode:

1. Last Event view with Alarm code

For Archival mode:

2. Event summary view
3. Timeline summary view
4. Smart Search tool

D.O. Gorodnichy and Elan Dubrofsky. **VAP/VAT: Video Analytics Platform and Testbed for testing and deploying video analytics**. SPIE Conference on Defense, Security, and Sensing, Visual Analytics for Homeland Defense and Security track. 2010, Orlando

Appendix B: Fourth Interdepartmental Conference on Video Technologies for National Security (VT4NS 2011), September 2011

Agenda

Foreword Presentation

Gon't departments and By invitation only

Registration is required.

Those planning to attend in person or via telecom should provide their names to Pierre Meunier.

Forth Interdepartmental Workshop on

Video Technologies for National Security (VT4NS 2011)

Theme: **Kick-off of PSTP projects PROVE-IT (VA) and PROVE-IT(FRiV)**

When: Friday, 23 September, 2011. 9:00 – 16:00
In Person: Large Boardroom on 11th floor, DRDC-CSS, 222 Nepean Str.
Via Telecom: Numbers to be provided.

Portal: https://partners.drdc-rddc.gc.ca/css/Portfolios/Biometrics (Human ID Systems)/VT4NS
(Gov't organizations will receive login/password to the portal in a separate email)

Organized by:

- Defence R&D Canada's Centre for Security Science (DRDC-CSS), and
- Canada Borders Services Agency's Scientific and Engineering Directorate (CBSA-S&E)

Chairs:

- Dmitry O. Gorodnichy: dmitry.gorodnichy@cbsa-asfc.gc.ca
- Pierre Meunier: pierre.meunier@drdc-rddc.gc.ca

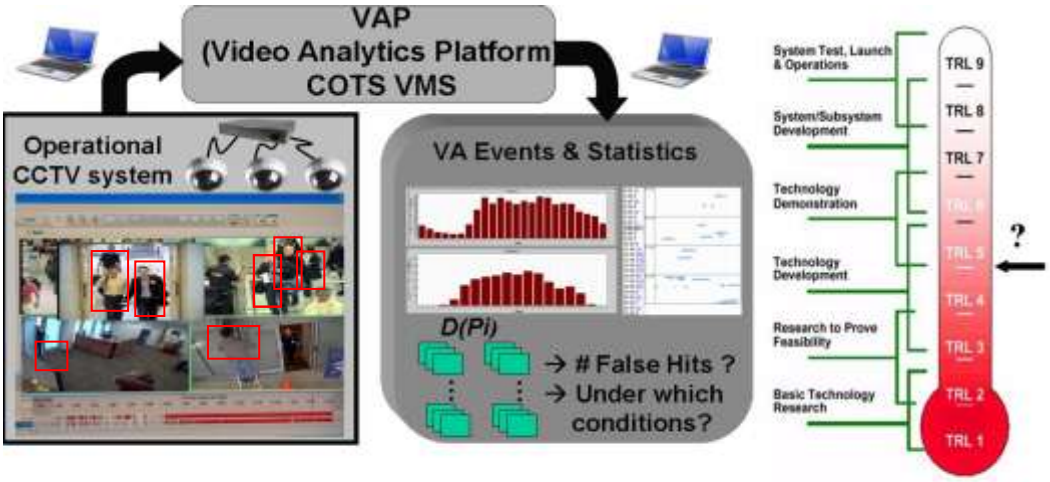
Facilitator:

- David Bissessar: david_bissessar@hotmail.com

Scope and Objectives:

As in the past, the primary objective of this workshop is to bring together GoC Border and Transport Security (BTS) and Biometrics (Biom) Communities of Practice (CoP) in) for the exchange of information on the activities, needs, and interests related to *deploying video surveillance technology* within GoC - in particular, in the area of Video Analytics (VA) and Face Recognition in Video (FRiV).

The secondary objective is to present an updated on two DRDC-CSS-funded projects that CBSA-S&E has launched this year in partnership with Academia and its federal partners to address the VA and FRiV needs of the GoC BTS and Biom CoP: PROVE-IT (VA) and PROVE-IT(FRiV).



Tentative Program
(time is indicated as a guideline only)

8:45 Welcome and Introduction to the workshop - Pierre / Dmitry

9:00 Intro to PROVE-IT(FRiV) project: Objectives & Logistics – David

- Assess applicability of FRiV technologies for various video surveillance tasks
- Investigate, develop and test required Face Processing (FP) components
    1. Pre-processing, Post-processing, Fusion
    2. Face Detection, Face Tracking, Face Tagging

Intro to PROVE-IT(VA) project Objectives & Logistics – David

- Analyze Technology Readiness Level (TRL) of various VA technologies:

Common objectives:

- Develop evaluation methodology (including data-sets, mockups, and pilots).

9:30-12:30

BIOM 401 PROVE-IT(FRiV) project:
Presentations from Project's main contributors -Tasks, proposed solutions, results obtained to date

9:30 CBSA: Dmitry

- Survey of commercial products; companies; deployments; media reports;
- FR Projects in other countries / govn'ts / FISWG & Intern'l Face Collaboration Meeting
- FR Software SDK selected / acquired for testing
- FR Datasets selected / acquired for testing
- Integration of commercial FD / FR software into VAP & In-house code development
- Other: R&D investment priorities

10:00 ETS: Eric

- Survey of public domain knowledgebase in FRiV: academic papers, patents, codes
- Survey of datasets of faces in video
- Evaluation methodology & benchmarking
- Video-based FR using incremental learning neural networks

11:00 uOttawa TAMALE LAB: Stan

- Post-processing for face triaging problem: feature engineering, feature selection, data fusion, classifier selection, and performance evaluation, esp. with noise and limited set of the training images

11:15 tentative – uOttawa VIVA Lab: Robert

- Pre-processing for FRiV: Face/Person Tracking, best facial image selection

11:30 Presentations from partnersother (potential) contributors:

- *What FRiV problem keeps you awake at night?*
- *What would you like to get out of this study for your organization? Which of the discussed VA tasks are most interesting to your organization?*
- *How can you contribute to this study ? (datasets, software, testing methodologies/setups, cameras/equipment, opportunities for pilots?)*

12:00 – 12:30:

Live demonstrations – with live feed from IP-camera, with datasets:

1. Face Detection / Tagging
2. "Watch List" screening against CBSA WANTED LIST
3. Matching faces across several video feeds

4. Combing face and iris images
5. Tamper detection

12:30-13:30 Lunch (not provided)

13:30 Focus group discussion (roundtable): feedback, recommendations, next steps

14:30 – 16:30

BTS 402 PROVE-IT(VA) project:
Presentations from Project's main contributors -Tasks, proposed solutions, results obtained to date

14:30 CBSA: Dmitry

- Survey of commercial products; companies; deployments; media reports;
- Milestone VMS VA functionality and partners
- VA Projects in other countries / govn'ts
- VA Software selected / acquired for testing
- VA Datasets selected / acquired for testing
- Integration of commercial VA software into VAP; In-house code development
- Other: R&D investment priorities

15:00 uOttawa VIVA Lab – Robert

- Survey, Selection and development of techniques, datasets and evaluation practices for VA.
- people tracking problem : in crowded and non-crowded environments, dealing with occlusions, applications to object dropping/removal, person-object tagging and loitering detection ; experimental methodology & Benchmarking

15:15 CRIM -

- Unattended / Left-Behind Baggage Detection problem: Survey, Selection and development of techniques, datasets ; experimental methodology & Benchmarking

15:30 Presentations from other (potential) contributors:

- *What VA problem keeps you awake at night?*
- *What would you like to get out of this study for your organization? Which of the discussed VA tasks are most interesting to your organization?*
- *How can you contribute to this study ? (datasets, software, testing methodologies/setups, cameras/equipment, opportunities for pilots?)*

16:00 - 16:30
Focus group discussion (roundtable): feedback, recommendations, next steps

Invited Attendees:

CBSA, DRDC-O, DRDC-T, DRDC-V, RCMP, PCO, CATSA, Public Safety, TC, FAITC, DND, HomeOffice, FBI

CBSA ASFC
PROTECTION • SERVICE • INTEGRITY

Fourth Interdepartmental Workshop on

Video Technologies for National Security (VT4NS'11)

September 23, 2011, Ottawa

Organized by CBSA-S&E and DRDC-CSS

FOREWORD
Dmitry Gorodnichy

Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

Welcome!

CBSA ASFC

Gov't:
- DRDC-CSS
- CBSA NHQ S&E: VSB
- CBSA NHQ Solutions
- CBSA Programs
- CBSA-NOR
- CBSA-GTAA
- CATSA
- DFAIT
- RCMP - Video and Audio Analysis Unit,
- RCMP- Technical Security Branch
- RCMP- Biometrics Section
- Public Safety
- RCMP - National Video Systems Integration Section
- DRDC-O (Network Information Operations)
- DRDC-Toronto
- DRDC-Valcartier
- DND - Directorate of Geospatial Intelligence
- HomeOffice

Academia:
- ETS
- uOttawa TAMALE Lab
- uOttawa VIVA Lab
- CRIM

Regrets:
- FBI
- NIST
- Office of the Privacy Commissioner
- TC

PROTECTION • SERVICE • INTEGRITY

VT4NS: history & outcomes

CBSA ASFC

2007: Led by NRC-IIT with support from US IARPA :
- first get-together (>10 GoC depts)
- first (live) demo of VA (inc. Face detection and annotation in video)
- first population of issues
- first call for coordination of efforts

2008: Led by CBSA-S&E with participation from DHS, IARPA
- Theme: —Building future-proof video surveillance systems (VSS)"
- Higher attendance (>20 departments)
- More live VA demos
- Addressing CBSA's need in VSS upgrades

Outcomes:
- Recommendation on Open Architecture systems
  - which allows integration of VA & in-house testing / pilot
- CD-ROM Proceedings published (with 12 presentations)
- CBSA VA Pilots

PROTECTION • SERVICE • INTEGRITY

VT4NS'10

CBSA ASFC

- Led by CBSA-S&E and DRDC-CSS

Themes :
- ***Moving Video Analytics into operational environment.***
- ***Faces in video***

- Tutorial: —Video Analytics: inside the Black Box"
- (re-) Introducing TRL for VA testing
- Demonstration of CBSA's Video Analytics Platform (VAP)
  - With Operational IP-cameras
  - Included face detection
- Brain-storming: in search for —killer" (best) VA applications

Outcomes:
- Proceedings published at DRDC portal
- Two PSTP CFP on proposed SoW

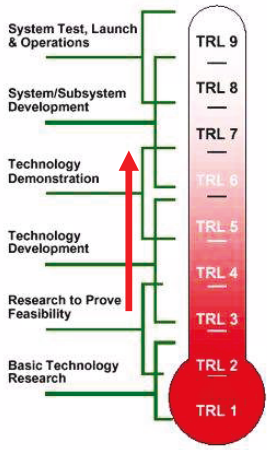
PROTECTION • SERVICE • INTEGRITY

Technology Readiness Level (Source: DOD, 2006)

9. Actual system 'flight proven' through successful mission operations (over 30)
8. Actual system completed and 'flight qualified' through test and demonstration.
7. System prototype demonstration in operational environment. ← PILOT
6. System prototype demonstration in relevant environment. ← MOCK-UP
5. Component validation in relevant environment.
4. Component validation in laboratory environment.
3. Analytical and experimental critical function - characteristic proof of concept.
2. Technology concept / application formulated
1. Basic principles observed and reported.

TRL (VA / FRiV) = 3-7

TRL (VAP) = ~7



VT4NS'10

CBSA ASFC

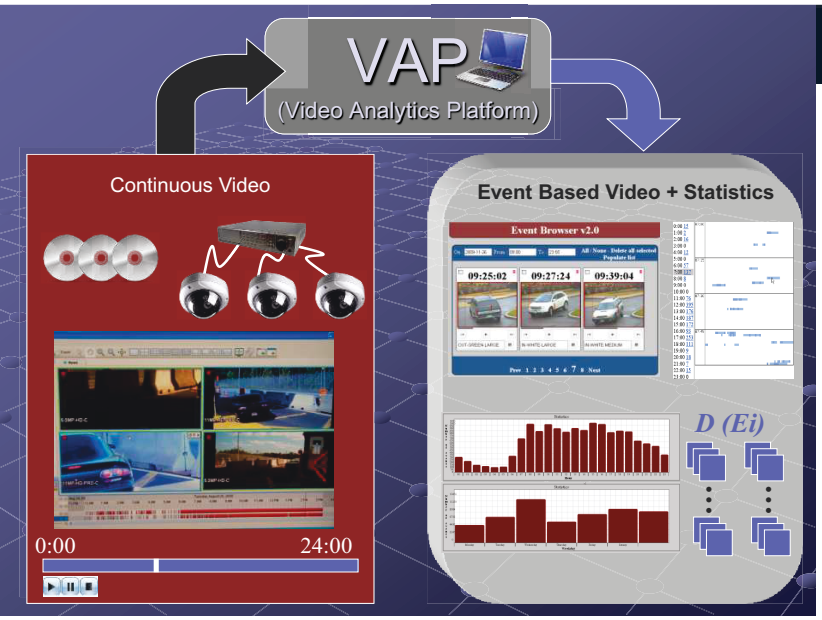
- Led by CBSA-S&E and DRDC-CSS

Themes :
- ***Moving Video Analytics into operational environment.***
- ***Faces in video***

- Tutorial: —Video Analytics: inside the Black Box"
- (re-) Introducing TRL for VA testing
- Demonstration of CBSA's Video Analytics Platform (VAP)
  - With Operational IP-cameras
  - Included face detection
- Brain-storming: in search for —killer" (best) VA applications

Outcomes:
- Proceedings published at DRDC portal
- Two PSTP CFP on proposed SoW

PROTECTION • SERVICE • INTEGRITY

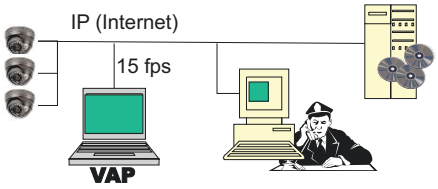


Embedding VA into Operational CCTV

Open Architecture

- Allows to directly access the video-feed
- Allows to control the video-feed quality/size

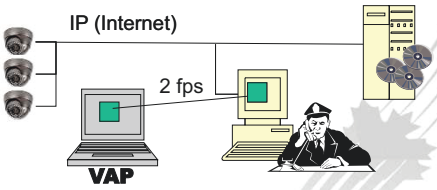
➔ VAP *IPCamCapture*



Closed Architecture

- Does not …
- Does not …

➔ VAP *ScreenCapture*



VT4NS'10

CBSA ASFC

- Led by CBSA-S&E and DRDC-CSS

Themes :

- ***Moving Video Analytics into operational environment.***
- ***Faces in video***

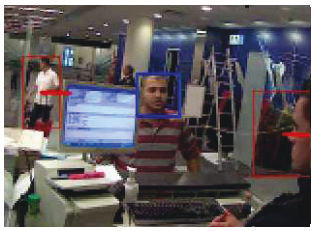
- Tutorial: —Video Analytics: inside the Black Box"
- (re-) Introducing TRL for VA testing
- Demonstration of CBSA's Video Analytics Platform (VAP)
  - With Operational IP-cameras
  - Included face detection
- Brain-storming: in search for —killer" (best) VA applications

Outcomes:

- Proceedings published at DRDC portal
- Two PSTP CFP on proposed SoW

VA + FR for Airport POE

CBSA ASFC



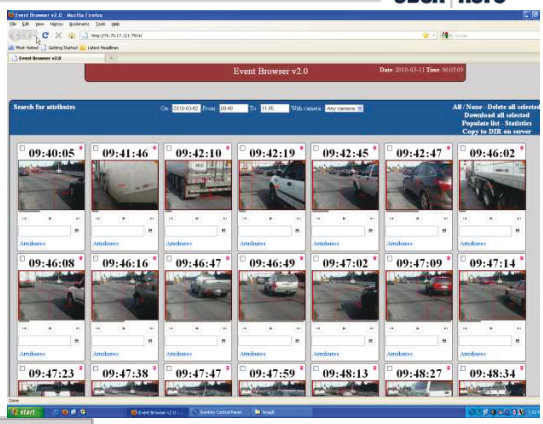
- *Face Triaging at PIL*": covert screening against —Wanted List"
- *Face Tagging at Exit (POE)":* archival of all faces seen in CBSA cameras – time-stamped/annotated

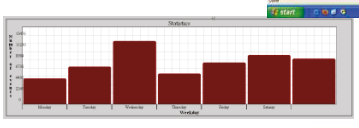
- Camera Tampering detection
- Other extracted intelligence:
  Abnormal motions, Stats / Trends, Waiting time

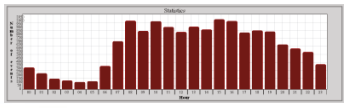
VA + FR for Land POE

CBSA ASFC

➢ For automated evidence extraction:
-"Non-reporter"
- —Portrunner"
+ extending LPR
- - Statistics (Trends)







VT4NS'10

CBSA ASFC

- Led by CBSA-S&E and DRDC-CSS

Themes :

- ***Moving Video Analytics into operational environment.***
- ***Faces in video***

- Tutorial: —Video Analytics: inside the Black Box"
- (re-) Introducing TRL for VA testing
- Demonstration of CBSA's Video Analytics Platform (VAP)
  - With Operational IP-cameras
  - Included face detection
- Brain-storming: in search for —killer" (best) VA applications

Outcomes:

- Proceedings published at DRDC portal
- Two PSTP CFP on proposed SoW

PSTP 2010 CFP

- Biometrics – Study No. 2:

  Real-time Face Recognition Technologies for Video-surveillance Applications

  Winning bid - BIOM401: PROVE-IT (FRiV) by CBSA

- Border and Transportation Security – Study No 2.

  Video Analytics for Border and Transportation Security—Indoor and Outdoor Environments

  Winning bid - BTS402: PROVE-IT (VA) by CBSA

VT4NS 2011

- Led by CBSA-S&E and DRDC-CSS

Themes :

- ***Update on PSTP BIOM401 Study***
- ***Update on PSTP BTS402 Study***
- Tutorial: —Face Recognition: inside the Black Box”
- Presenting studies work plan & results to the community
- More demonstrations of extended VAP
  - With several COTS Face Recognition SDK
  - Using in-house developed FRiV
- Soliciting feedback & Brain-storming: on next steps

Expected outcomes:

- Feedback from everyone
- Feedback for next round of PSTP CFP

VT4NS portal

presentations and other documents will be posted at

https://partners.drdc-rddc.gc.ca/css/Portfolios/Biometrics (Human ID Systems)/VT4NS

...

Appendix C: Third Interdepartmental Conference on Video Technologies for National Security (VT4NS 2010), May 2010

“Video Analytics: Technology Maturity, Deployment Challenges, and Roadmap”

By D. Gorodnichy

Canada Border Services Agency | Agence des services frontaliers du Canada

Video Analytics: Technology Maturity, Deployment Challenges, and Roadmap

VT4NS 2010

Dr. Dmitry O. Gorodnichy
Video Surveillance & Biometrics Section
Science and Engineering Directorate

Canada

Outline

1. What is Video Analytics (VA)
2. Technology Maturity (adaptation from DoD):
   - Technology Readiness Level: TRL(VA) = 1, …, 6
   - Other Technology Maturity criteria
3. VA deployment challenges
4. Three-Phase Roadmap for VA deployment
   - Our 1st objective - to test TRL (VA)
   - Our 2nd objective - to raise TRL (VA) to 7 & 8

What is Video Analytics?

- **Video Analytics (aka Intelligent Video, Smart Camera, Video Recognition): Computational Analysis of Video Data that deals with Automated Extraction of Intelligence from Video.**

21st c.
- High resolutions
- IP cameras
- Digital
- Analog

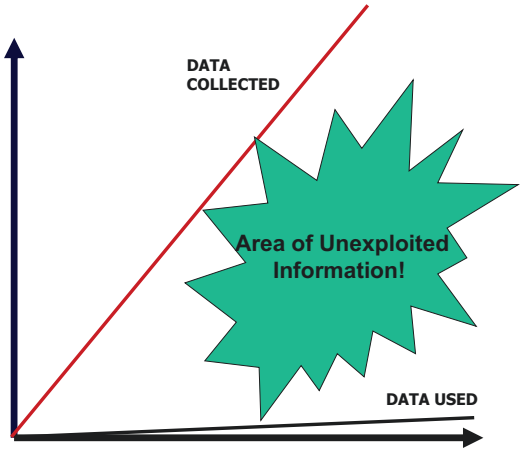
20th c.

←Animated image example:
The entire 17:00- 24:00 activity is summarized into a few annotated snapshots

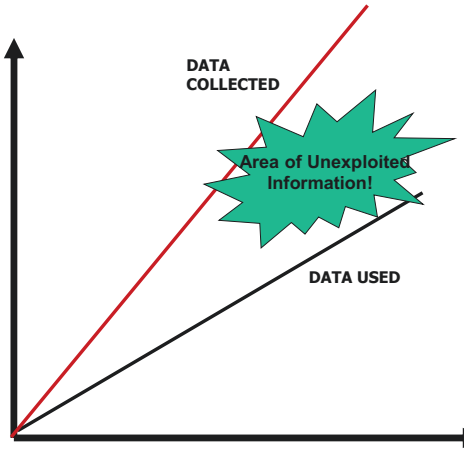
(with NRC's ACE Surveillance™).

- Video Technology (VT) of the 1990's was primarily concerned with video capture (Cameras and Recorders)
- Today, VT is Video Capture + Video Analytics

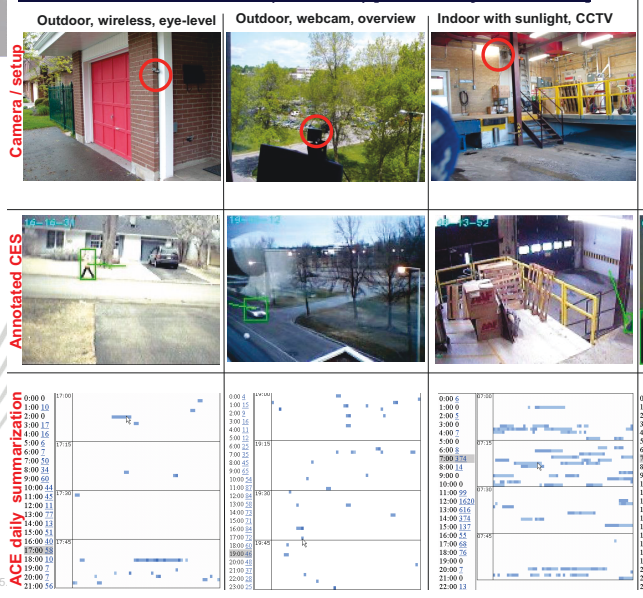
Without Video Analytics - as it is now



With Video Analytics - what we can do



ACE Surveillance™ VA Pilot (2006-2008) [Gorodnichy, NATO-2008]



Video Technology components / cost

1. Video Data Capture
2. Transfer
3. Storage
4. Protection and security

Technologically solved

- cameras
- encodes, decoders
- transmitters and receivers
- routers and multicast switches
- network video recorders
- storage media

5. Integration with other sensors / software
   - Motion, heat sensor, audio, Video Analytics
6. Video data management
   - Indexing, visualization, retrieval of data
   - Data = video + associated Meta-data (Annotations) obtained with Video Analytics
7. Video analytics for automation and filtering:
   - Real-time event detection / recognition
   - Analysis of archived video data

Being solved – requires exploring, evaluation, tuning (inc. RFI, Pilots)

Total cost = Hardware + Software/Testing/Tuning
Video Analytics expertise minimizes the cost of both components.

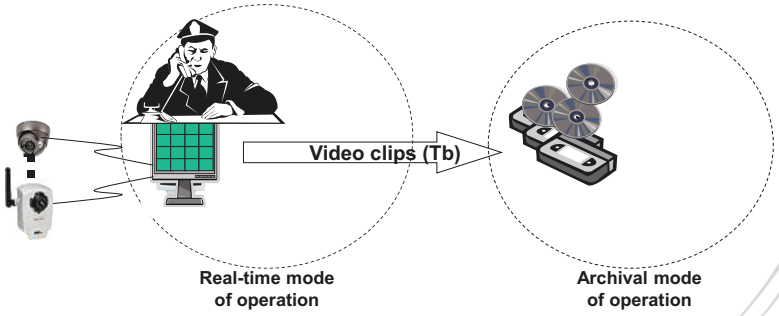
+ Operational Cost/Value

What Video Analytics is NOT ?

- "Brightness change detection" marketed by industry as "motion-detection", which is NOT.
- NOT a "Magic bullet":
  - Just as with ANY image recognition (inc. Biometrics), there will be "False Hits" and "False Misses".
  - ➔However, their Rates can be minimized to acceptable for operational needs – by evaluation and customization.
- NO "one size fit all" solution (esp. in Non-cooperative scenarios)
  - Different VA codes required for each setup, environment, task.
  - ➔However, experts may use the same library to write these codes.
- "High resolution / quality" do NOT assume "high intelligence".
- It is NOT expensive with proper (unique) skills and planning.
  - In fact, it (significantly) reduces the entire cost operation, though the optimized equipment build-up and efficient data analysis.

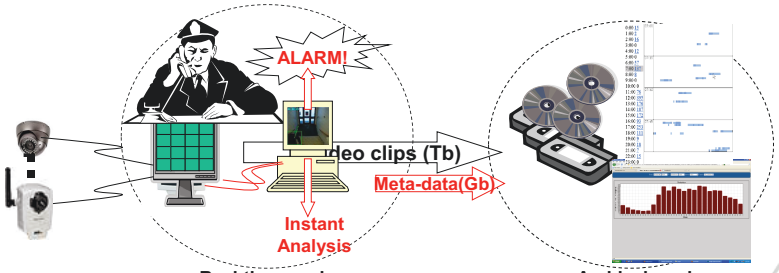
Monitoring Tasks Performed by Human (Status quo)

Two modes: a) real-time monitoring, b) post-event analysis



Monitoring Tasks Performed by Human & Software

Two modes: a) real-time monitoring, b) post-event analysis



Main condition - Open Architecture:
To be able to tap into (video signal) input and (data) output.

(Critical) analysis of VA Market and readiness

Main question:

What is possible,

what is not,

and

how to distinguish one from the other ?...

Insider's view – how industry does it

- There are >5000 companies registered in Canada doing business in "Surveillance" [NUANS Search Results in 2008]
- Anyone who does Surveillance" can add "Intelligent" or "Smart" just by doing "pixel brightness comparison".
- Some go further
  - by creating many "heuristics"
    - no University knowledge required,
    - tuned for one setting / does not work for another
  - use Public domain codes, of which there many
    - OCR, Face Detection, Some Face Recognition,
    - Many low-level image processing libraries (edge detection, colour segmentation, motion/optical flow computation)
- However, very few go further – hire MSc/PhD in Computer Vision / Pattern Recognition to do higher-level (semantic) processing of images –which is still one the most challenging research areas (eg See CRV conference)
  - (eg. http://www.computerrobotvision.org/tutorial_day.html)
- As a result, many companies list *many* VA tasks they "can" do.

VA tasks companies "can" do:

From www.i3dvr.ca, www.intelliview.ca www.visualcortek.com www.miovision.com, www.marchnetworks.com www.ioimage.com www.nice.com www.indigovision.com www.iomniscient.com, www.objectvideo.com (and many more):

- Human / Object Recognition and Tracking
- Object Classification
- People Counts
- Vehicle recognition
- People recognition / Face recognition
- Object left behind / Unattended Baggage Detection
- Object Removal Detection
- Loitering Detection
- Tail-gating
- [Waiting] Line Control, Crowd management
- Special Attribute Detection
- Advanced Behaviour Analysis
- Slip and Fall Detection
- Intrusion Detection / Virtual Tripwire
- Autonomous PTZ Tracking
- Stopped Vehicle Detection
- Camera Tampering Detection
- Congestion detection
- Counter Flow
- Automatic Licence Plate Recognition
- Object Alteration Detection
- Audio and Sound Classification
- Face Detection / Face Tracking
- Graffiti / Vandalism detection
- Highway (vehicle) count
- Automated summarization of archived video

13

Insider's view – how Academia does it

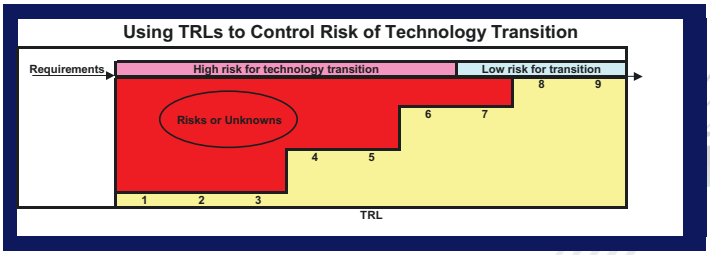
- VA is one of the least resolved and most researched areas:
  - Every year, >5 major conferences, >1000 papers published
  - Every year, practically every university has 2-10 MSc/PhD students working on un-resolved problems in content (semantics) retrieval from images/video
- Some VA tasks are indeed now possible,
  - But all have limitations
- Most of reported VA solution have never been tried in live (24/7) operational environments

14

Technology Maturity 101 (from DoD, NASA)

Main: Technology Readiness Level (TRL)

- intensively used by (DoD, NASA, DHS, DNI)
  - Provides aCommon Understanding of S&T Exit Criteria
  - A Risk Management Tool & Allows to estimate Cost/Investment required
- However, it is only one dimension of Techn. Maturity.



15

Other Technology maturity criteria:

Adopted from Air Force Research Lab:

- Producibility – Manufacturing Readiness
- Readiness to Receive (If Goal Is Transition from Technology Developer and Technology Receiver
- Practice Based Technology Maturity (Emphasis on Community of Users) – User Readiness
- Program Readiness (program needs and constraints)

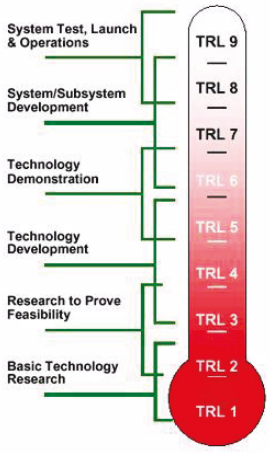
+ (added by VSB)

- Required In-house R&D capacity: R&D Readiness
  - Customization & tuning required

16

Technology Readiness Level (Source: DOD, 2006)

1. Basic principles observed and reported.
2. Technology concept / application formulated
3. Analytical and experimental critical function - characteristic proof of concept.
4. Component validation in laboratory environment.
5. Component validation in relevant environment.
6. System prototype demonstration in relevant environment.
7. System prototype demonstration in operational environment.
8. Actual system completed and 'flight qualified' through test and demonstration.
9. Actual system 'flight proven' through successful mission operations (over 30)



TRL (most VA) = 3-6 !
TRL(ACE Surveillance) = ~7
TRL (VAP) = ~7

17

Doing VA TRL assessment

- DNI VACE (2005-2008) –selected successful VA projects
- Several Video datasets developed to test VA
  - NIST TREKVID – the most comprehensive
  - CLEAR (used by VACE)
  - From Home Office (UK)

However: They allow to test / achieve TRL up to 6 only! (ie. prototype is successful in relevant environment)

Besides: the participant are all from Academia (not from Industry!)

So how will you know the TRL of the VA that you need ?..

18

Video Analytics Technology Readiness

Traditionally performed by Humans, many of these Monitoring Tasks can now be facilitates with VA software

TYPE 1: Real-time monitoring tasks	Customization, testing required	Technical readiness	Program readiness
1* - "Face extraction/tagging"	Little	5	4: Ready for Pilot
2* - "Wrong direction detection (Run-away alarm)"	Little	5	4: Ready for Pilot
3 - "Loitering alarm"	Major	4	4
4 - "Object-left behind or abundant object alarm"	Major	4	4
5 - "Tripwire (trespassing) alarm"	Little	5	4: Ready RFP
6 - Other events (door opening, car parking etc) alarm	Major	4	4
General Tracking / Detection of people in multiple streams		1	
TYPE 2: Post-Event (Archival) monitoring tasks			
1 - Summary of detected events & statistics (trends)	Little - Medium	5	4
2 - Searching for a object/person in stored streams	Little - Major	5	4
General Summary / Search in unstructured environment		1	
Special case tasks			
LPR (License Plate Recognition)	None	7	5
Face Recognition	Little-Medium	1-7	1-4

5 – ready for pilot, 4 – requires Evaluation, 3/2– requires further Refining/Exploration, 1 – not ready yet

19

Main objective of R&D prior to deployment

Our goal with VAP/VAT:

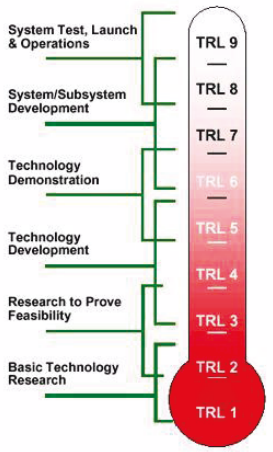
- to test TRL /achieve TRL (VA) =7 (in operational environment)

  and,

- possibly to attain TRL 8 and 9 for some VA technologies

+

- work with Operations/Programs/Industry to examine other dimensions of VA Technology maturity



20

VA deployment challenges & Road-map

Phase 1 (Foundation): Building Business, Infrastructure foundations; R&D capacity

- From Knowing the Art of Possible (TRL) to Making it Possible
  - Dealing with Stereotypes / Misconceptions
  - Not to over-estimate or under-estimate what VA can do
  - Investigating TRL, risks/capacity to do R&D

Phase 2 (Development): Resolving Technological Challenges

- R&D programming + Knowledge of Operational Tasks
- Dealing with "Closed Architectures"
- Selecting/Building a solution

Phase 3 (Pilots). Testing and deploying the solution in the "field"

- Knowing Clients needs & Educating/Training the Client
- Customizing, stress-testing (in Mock-up and real setups)

21

Building VA Solution: Technical challenges

1. Different tasks and scenarios require different VA codes to be written, and the customization of the VA codes can be properly done only by a Video Recognition expert. At the same time, VA customization requires strong knowledge of operational tasks as well as constant communication with the involved regions. As a result, a solution coming from outside is often very expensive and in many cases not reliable.
2. IP-cameras contain vendor-specific coding/encoding mechanisms, and getting a video-feed from these cameras requires customization in programming codes specific to each vendor. Furthermore, while some vendors provide functionality to perform direct capture of the video-feed from their cameras through the use of a dedicated SDK (Open Architecture cameras), others do not (Closed Architecture cameras).
3. Selecting a good VA product requires the testing of different products for the purpose of measuring and comparing their performance for a given task. Most agencies cannot afford to perform such testing and have to fully rely on the vendors' claims instead.

22

These challenges are being resolved by

- Creating CBSA-S&E VSB section
- Developing VAP/VAT technology

… proceed to next presentation

23

Appendix D: Third Interdepartmental Conference on Video Technologies for National Security (VT4NS 2008), October 2008

Background, Program and References

“Intelligent Surveillance: examples, myths and lessons”

By D. Gorodnichy

UNCLASSIFIED

Second Interdepartmental Meeting on

Video Technologies for National Security (VT4NS'08)

CENTURION CONFERENCE & EVENT CENTER
170 Colonnade Road South, Ottawa, K2E 7J5

23 October 2008

Theme: *Deploying "future-proof" video technology*

Goals | **Participants** | **Presentations*** | **Repository** | **Next steps**

Organized by: CBSA LSSD (Canada Borders Services Agency, Laboratory and Scientific Services Directorate).

In coordination with: US DHS (Department of Homeland Security), and US DNI-IARPA (Director of National Intelligence, Intelligence Advanced Research Projects Activity), Computer Vision section, formerly DTO-VACE (Disruptive Technology Office, Video Analysis and Content Extraction).

Coordinator: Dmitry O. Gorodnichy, CBSA LSSD (Dmitry.Gorodnichy@cbsa-asfc.gc.ca)

Background:

- In the context of enhancing security, Video Technology (VT) is one of the most demanded technologies of the 21st century.
- Expanding and improving the capacity and functionality of VT is one of the current priorities for many federal departments:
    - US: fibre optic network along both borders, cams, motion/heat sensors deployed (2002-03) / General purpose monitoring cams with remote monitoring deployed / Secure Border Initiative (2005, SCONSAD)
    - CBSA, a major VT user at Points of Entry (POE): launched several VT-related initiatives and business cases (2007-2008):
        1. Port Runner (2007) - focus on visitors: capturing intelligence/evidence related to port violators (faces, license plates).
        2. Interview Rooms (2007) - focus on personnel/visitors monitoring
        3. Port Integrity (part of Agency Integrity, 2008) - focus on personnel: deals with violations within the agency.
        4. Call for increased deployment of face recognition and other biometric technologies at border crossings and ports of entry (inc. related to NEXUS).

5. Video-based identification of cargo containers (related to RADNET)
6. Video-based statistics measurements.

- Intra-departmental camera working group (CWG) created (Mar 2008),
- Plans to create a new LSSD section on Video Technology to guide and support VT deployment and usage by the agency (inc. Biometric Surveillance technologies)

- TC: extensive funding for VT announced in 2007, released CCTV manual.
- RCMP: extra funding for VT, focus on Media Management System, face recognition in video
- DRDC: face recognition from video biometrics RFP

- **While VT of the past was primarily concerned with video capture and storage, VT of the future is more concerned with Video Data Management, Video Analytics and its integration with other sensor systems.**
- IARPA (DTO-VACE): conducts evaluation and selection of the next-generation video analytics technologies. A history of relationship with IARPA (DTO-VACE) since 2005.
- The first VT4NS meeting was organized by NRC-IIT Video Recognition Systems, held in June 2007.

Goals:

The VT4NS workshops bring together project leaders and principle investigators working on deploying and using Video Technology (VT) within the government of Canada. The workshops consist of several invited oral presentations, followed by focus-group discussions on the raised issues.

Objectives:

1. To synchronize the effort in developing solutions for Video and related (Audio, and Biometrics) Technologies for the new century.
2. To connect VT users and VT experts with each other .
   - VT experts present SOTA (state of the art) in the area;
   - VT users present Pilot projects, case studies, wish list and Action items.
3. To populate a list of interests and expertise, and to create a common knowledgebase.
4. To address action items and specific technical issues from the following topic list.

Topics:

1. Quality of video capture (equipment internal & external factors)
2. Camera locations and applications: Port Runner vs. Port Integrity
3. "Procedural" adjustments to ensure proper and efficient use of VT
4. Video data retention and storage (inc. review, disclosure and destruction)
   1. Video data viewing rights, sharing and transfer.
5. Video for person identification (with iris and face recognition)
6. Use of visual data in courts as evidence.
7. Automated video recognition and analytics:
   1. In real-time: alert enhancement, and meta-data insertion
   2. In post-event investigation: video data analysis and content retrieval.
8. Combining video surveillance systems with audio and other sensors
9. Selecting video management systems

Participants:

- IARPA / Computer Vision section (formerly, DTO-VACE)
- DHS / Science and Technology Directorate / Suspicious Behavior Detection Programs
- CRIM (Computer Research Institute of Montreal), L'equipe Vision et Imagerie
- CRC (Industry of Canada, Communications Research Centre)/Advanced Video Systems
- CBSA / LSSD / Advanced (Surveillance & Biometric) Technologies, Electronics and Computer Systems, Network and Computer project
- CBSA / Architecture division / Concepts and Consultations
- CBSA / Travelers Projects and Systems, People Systems
- CBSA / Operations / Professional Standards
- CBSA / Camera Working Group (inc. Enforcement, Corporate Security, Regions)
- RCMP / Surveillance Technology Section / Covert Vide(CV), Remote Sensing Technologies (RST) and Special Purpose Vehicle (SPV) units
- RCMP / Video/Audio Analysis Unit, Technical Investigation Services Branch
- RCMP / Technical Security Branch
- Transport Canada / Security Technology / Security and Emergency Preparedness
- Office of the Privacy Commissioner of Canada
- DRDC / Automated Intelligent Systems/UAV
- DRDC / Network Information Operations Section
- DND / Forces

In total, 45 people representing over 30 different federal groups/departments participated in the workshop. The participants contact information can be requested from the workshop coordinator.

List of participants [**PDF**]

Program and Proceedings

See also **PDF files for printing**

23 October (Thusday) CENTURION CONFERENCE & EVENT CENTER

8:30-9:00 Breakfast, Coffee/Tea*

9:00

- Welcome message from CBSA-LSSD Director General [**PPT**, **5-year strategy**]
- Foreword from workshop chair [**PPT**]
- Round table introduction names/groups and related projects/interests [**PPT**]]

9:45

- Introduction to related DHS and IARPA activities and interests:
  - DHS: "Behavior-Based Surveillance" [PDF]
  - IARPA: "Overview of the IARPA Computer Vision Program" [**PPT**]

11:15 Break*

11:30

- CRC: "Overview of CRC Advanced Video Systems activities" [**PPT**]
- DRDC: Automated Intelligent Systems projects [**PPT**, **demos**]
- DRDC: Video-based Facial Verification System for Information Security [**PDF**]
- RCMP: "Overview of the RCMP Audio & Video Analysis Section" [**PPT**]

12:30-13:30 Lunch Buffet*

13:30

- LSSD: "Intelligent Surveillance: examples, myths and lessons" [**PPT**,**demos**]
- CRIM: CRIM projects related to Video (and Audio) Analysis [**PDF**]
- RCMP: Video Management Software Evaluation Project [**PPT**]

15:00 Break*

15:15

- VT at CBSA and discussions [**PPT**]
  - Related projects, activities, action items:
    - vision statement, survey, policy issues, RFPs and Regional requests, interim recommendations / Best Practices documents.
  - Cameras for physical security at CBSA
  - Criminal Investigations Program
    The relationship between Access to Information, Privacy (ATIP) and Disclosure Policy Division and Video Technology

17:00 Adjourn

* Breakfast, lunch, snacks courtesy of CBSA-LSSD.

24 October (Friday) Laboratory and Scientific Services Directorate

9:00-11:00 LAB TOUR (Address: 79 Bentley Ave, Ottawa, ON, K1A 0L5)

Repository of related documents

See also **Repository directory**

- IARPA : **http://www.iarpa.gov**
- **DNI InfoX, VACE programs**:
  - vace_brochure.pdf, DNI-VACE Presentation at NRC (August 2006).
  - infox_brochure.pdf, DNI-InfoX Presentation at NRC (June 2007).
- **NRC Video Recognition Systems** (2002-2007):
  - bilingual brochure, Presentation for VACE (2006)
  - Papers on ACE Surveillance, Face Recognition from video technologies
- Evaluation of Intelligent Video solutions: from SAWER, VACE, **UK Home Office**
  - **Home Office CCTV and Imaging Technology i-LIDS dataset** (copy available from LSSD)
- CBSA:
  - **"Automated video surveillance: challenges and solutions. ACE Surveillance (Annotated Critical Evidence) case study"** (D.Gorodnichy, T.Mungham, NATO symposium "Sensor and Technology for Defence Against Terrorism", April 2008).
  - **Port Runner Cornwall Pilot project: Report, Recommendations & Images** (August 2008).
  - CBSA Camera Working Group (CWG) interim documents and drafts (May-Nov 2008):
    - Policy drafts,
      - List of identified issues (for broad policy)
    - Recommendations for regions.
    - Survey questions
    - Video Surveillance Vision statement
  - CBSA Physical security:
    - Guides:
      - Security Design of CBSA Facilities, Ch11, Appendix A, "Closed Circuit Television", Comptrollership Manual (Protected A).
      - RCMP Threat and Risk Assessment (TRA).
    - Doctrinal sources
      - Government Security Policy (GSP)
      - Operational Standards for Physical Security
      - RCMP Technical Services Branch
      - CSE Information Technology Security Guides
      - Professional organizations and testing bodies for some elements (ASIS, CSIS, ULC, etc)
    - Concrete Sources
      - Results of a Threat and Risk Assessment then baseline requirements if no additional threat or risk identified above general environment
- From RCMP AVAS: Useful References on Video Evidentiary Requirements:
  - Scientific Working Group on Imaging Technology (SWGIT) **www.theiai.org/guidelines/swgit/index.php**
  - Technical Support Working Group (TSWG) **http://tswg.gov/**
    - Flipbook "Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems" (2007). Email: Pubs@TSWG.gov
- Related PWGSC RFPs:

    - DRDC "Video-based Facial Recognition: Algorithm and Demonstration." (Dec. 2008)
    - CBSA "Advanced Video Management System" (Sep. 2008)
    - CBSA "Access Control & Video Management" (Nov. 2008)
- Standards:
    - UL 2044 standard, Commercial Closed Circuit Television Equipment,
    - IS23000-10 2008 (Copyright) Video Surveillance Application Format
    - **ONVIF (Open Network Video Interface Forum)**
    - **PSIA (The Physical Security Interoperability Alliance)**
- Media on Video Surveillance:
    - **< L'Actualite > (Oct. 15, 2008, p.14) article : "Big Brother est aveugle" ("Big Brother is blind")**
- Related links:
    - **http://ipvideomarket.info/companies**
    - **www.canadiansecuritymag.com**
    - Video analytics:
        - **CRV International Workshop on Video Processing for Security (VP4S'06)**.
        - IEEE-published Workshops on Video Processing and Recognition, research forums and labs in Canada: **www.computer-vision.org**

Follow-up items:

- Create a common Repository of Documents/references
    - Share the Workshop Presentations
    - Create on-line site for sharing the unclassified, public domain documents and links
    - Interim internal documents (List of Issues, Survey Question etc) can be sent by request
- Create an Interdepartmental Working Group (or Council) on Video Technology (based on the parties presented at the workshop)
- Contact Interdepartmental Working Group on Biometrics.
    - Suggest organizing a similar academia-meets-operations workshop on Biometrics/Pattern Recognition.
- Establish closer relationship with DRDC Center for Security Science
- Have follow-up close-group focused meetings
    - Video Management System process at RCMP
    - Interim Recommendation documents/Criteria by CBSA
    - Share comments/experience on currently used equipment (RCMP/CBSA)
    - Face Recognition from Video (with DRDC,RCMP,CBSA)
- Prepare for next VT4NS workshop
    - Within SSC-PSTP
    - US FBI Video Surveillance section, UK Home Office expressed interest in participating.

Last updated: 22.XII.2008

Intelligent Surveillance: examples, myths and lessons

Dr. Dmitry Gorodnichy

Laboratory & Scientific Services Directorate
Canada Border Services Agency

VT4NS'08 Meeting
23 October 2008
Ottawa

Outline

- Problems with status-quo Video Surveillance
  - Real-time and archival problems
  - Operational considerations
    - Demo
- Next generation solution - Video Analytics based
  - "Motion detection" myth and problem
  - "Object detection" as example of real intelligence
    - Demos
  - Special interest - Faces
- Conclusions
  - Other myths
  - What you can do with Faces

2

How it started: Surveillance System = CCTV system

- Basic architecture:

  Camera + TV monitor (+ storage) + Agent

  → Hence, the name *Closed Circuit Tele-Vision*

- 3 modes of operation:
  1. Active - personnel watch video at all times
  2. Passive - in conjunction with other duties
  3. Archival - for post-event analysis
- Actively Used for:
  - monitoring protected/strategic areas (by Physical Security, Enforcement, Infrastructure)
  - Demo

3

Problems in real-time modes

1. An event may easily pass unnoticed .
   - due to false or simultaneous alarms,
   - lack of time needed to rewind and analyse all video streams.
2. No time to react in real-time (efficiently)
   - Because no intelligence is available (until Agent extracts it from video data)

4

Problems in Archival mode:

Due to temporal nature of data:

1. **Storage space consumption problem**
   - Typical assignment:
     2-16 cameras, 7 or 30 days of recording, 2-10 Mb / min.
     ➔1.5 GB per day per camera / 20 - 700 GB total !
2. **Data management and retrieval problem**
   - London bombing video backtracking experience:

"Manual browsing of millions of hours of digitized video from thousands of cameras proved impossible within time-sensed period"

[by the Scotland Yard trying to back-track the suspects] [L'Actuality, 15 oct. 2008]

5

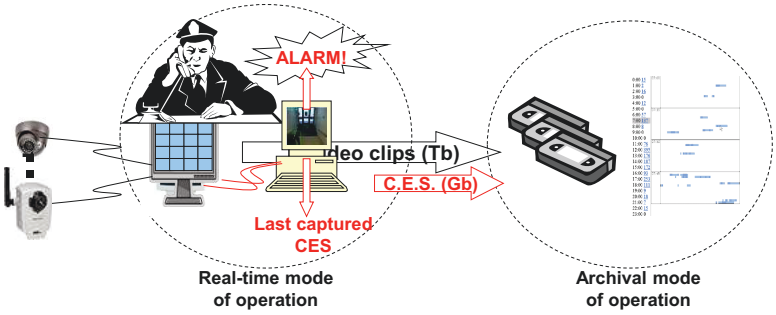
The only solution to these problems – computerize Agent's work!

- Known as
  - **Intelligent Video**,
  - Video Analytics
  - Video Recognition,
  - Smart Cameras
  - Video Analysis & Content Extraction
  - Intelligent Filters / Adds-on / Modules

6

Key idea – Computer/Software is added to do the job

Main condition – to be able to tap into video signal:
Both a) at capture time, and b) to archived data.



Capture filters / modules

Retrieval modules / software

What exactly we can do?

- Some results from NRC Video Recognition Systems project (2002-2007)
- Demo - Lets connect our TV to a laptop !

More demos

Something which is quite possible:

- Better alarms, response
- Automated summary / annotations
- Detection/Recognition of specific objects, directions, events
- Face extraction / archival / tagging
- Automated tele-operator
- Stored quality/quantity depends on the content
  - High-Res snap-shops or video only when needed
- And many more for archived tones of data…

…but this is on Research side.

On operational side…

- Video data/cameras became appreciated …
  - not only for triggering alarms or remote viewing
  - but also providing source of intelligence (useful data)
  - + it is Publicly accepted

➔Explosion (“Tsunami”) of

- video technology projects (see presentation in PM)
- infrastracture build-ups, and
- captured and stored data

➔ Consultants/Providers are contacted for advise … and this is what we get.

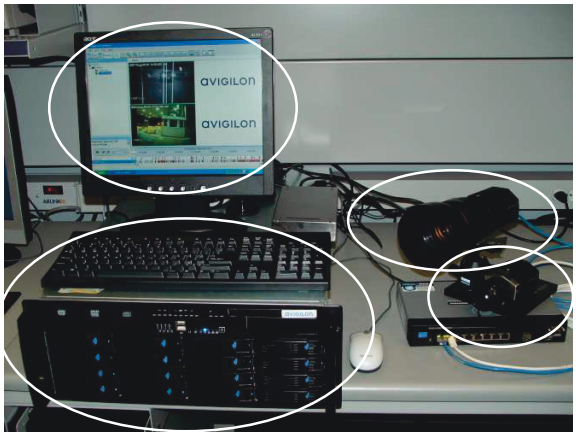
Better equipment, BUT the same mentality

Camera + TV monitor + storage + Agent!

Avigilon - From Port Runner Pilot project (2007, LSSD)

Similar, solutions:

Covi, IndigoVision, and many others…



And the problem is…

If …

- a system doesn’t support Open Architecture, and
- transmits and stores video data using proprietary formats,

you …

- won’t be able to add Intelligent Video processing / modules of your own.
- will have to rely entirely on the provided “Intelligent” options, … which in many cases are far from being “Intelligent”.

Besides, you can’t easily replace/upgrade components…

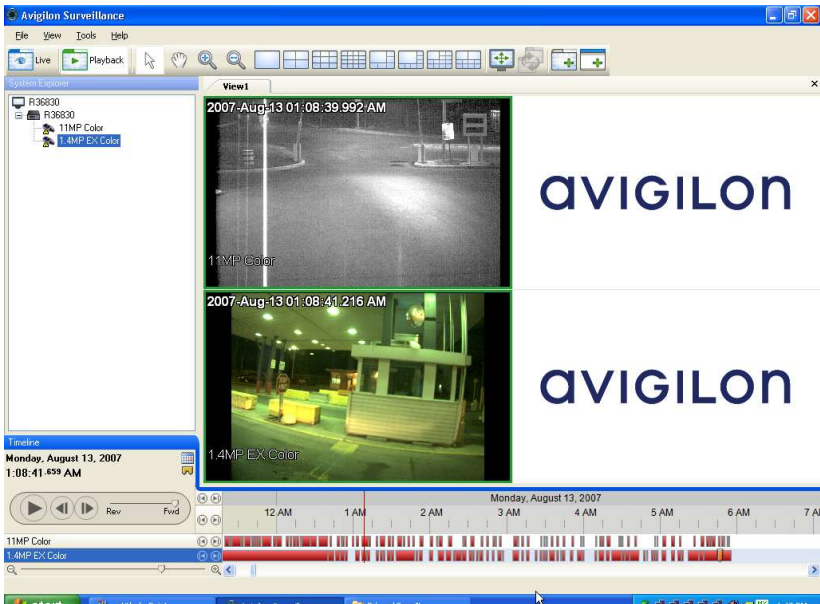
… and it is left to Agent

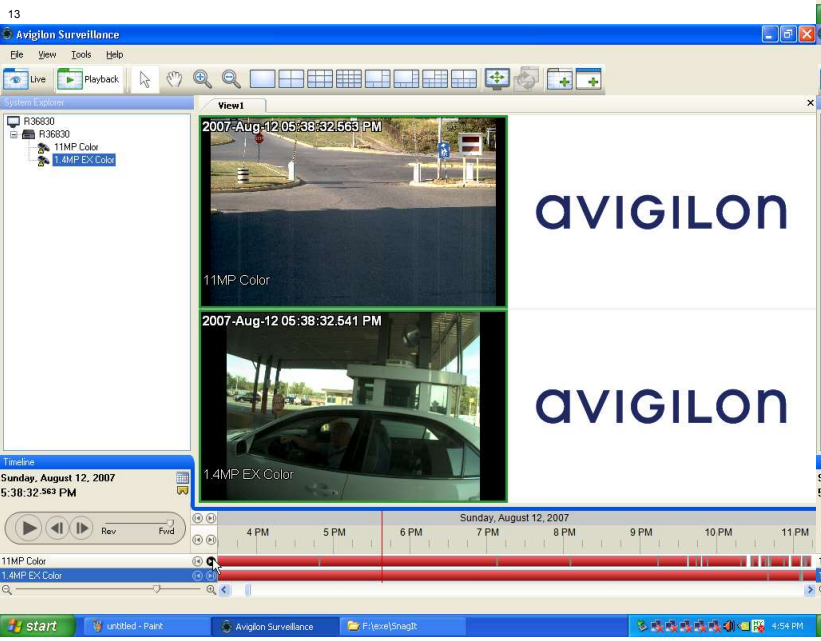
In real-time mode,

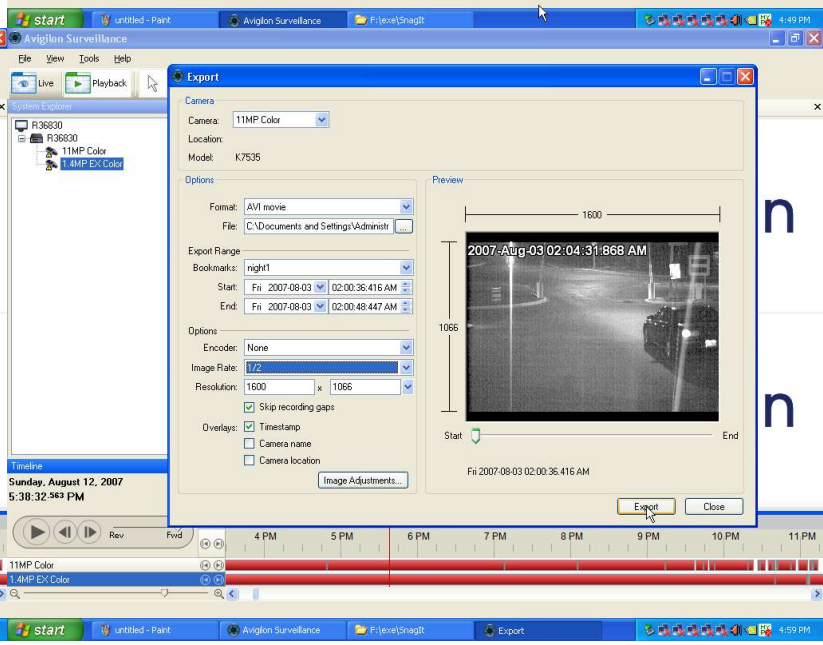
- to figure out what happened (or didn't happen) in , which may take long – demo
  - …because of limited "motion detection"
  - …no annotations / meta data (or possibility to add them)

In Archival mode,

- to convert each "potentially useful" clip from proprietary to standard format.
  - You can't just take HD. – You need Provider's software!







Status-quo "video intelligence"

Transport Canada CCTV Reference Manual for Security Application .

Australian Government National code of practice for CCTV applications in urban transport

USA Government :recommended security Guidelines for Airport Planning, Design and Construction.

…. refer to "Motion-based" capture as *Intelligent Surveillance* Technology, and make their recommendations based on thereon.

More on "Motion-detection" myth

- Term "Motion-based" is coined to make people believe that video recognition is happening, which is not!
- It's actually illumination-change-based, as it uses simple *point brightness comparison*: $| I(\text{pixel at } t) - I(\text{pixel at } t+1) | > T$

- Which often happens not because of motion!
  - Changing light / weather (esp. in 24/7 monitoring)
  - Against sun/light, out of focus, blurred, thru glass
  - Reflections, diffraction, optical interferences
  - Image transmission, compression losses

"Object-detection" is intelligent …

… but few can do it, since necessary advances in video recognition theory became possible only recently (>2002).

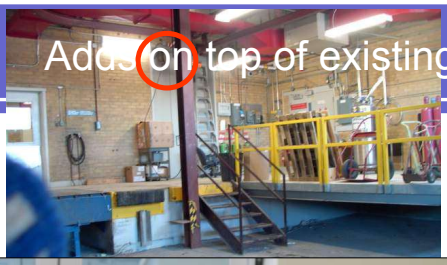
Example:

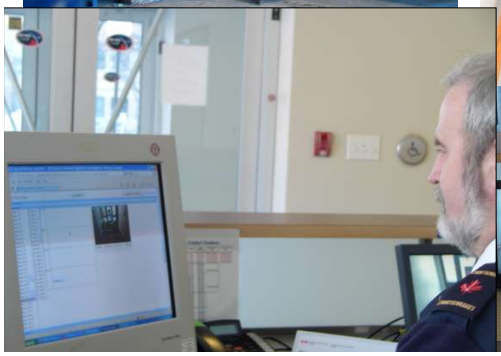
A 7-hour activity from day to night (17:00 - 24:00) is summarized into 2 minutes (600Kb) of Annotated Critical Evidence snapshots.

Note illumination changes! - Watch tree shadows and sun light.

19

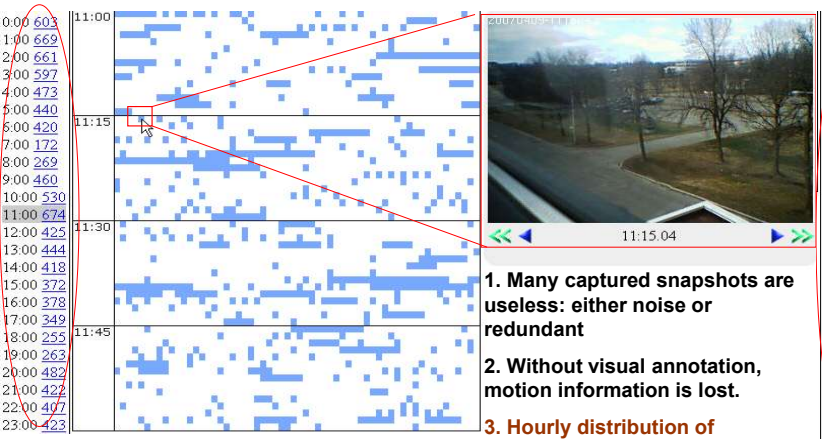
Adds on top of existing infrastructure





Status quo "Motion-based" capture

(Courtesy: NRC-IIT Video Recognition Systems project)



1. Many captured snapshots are useless: either noise or redundant

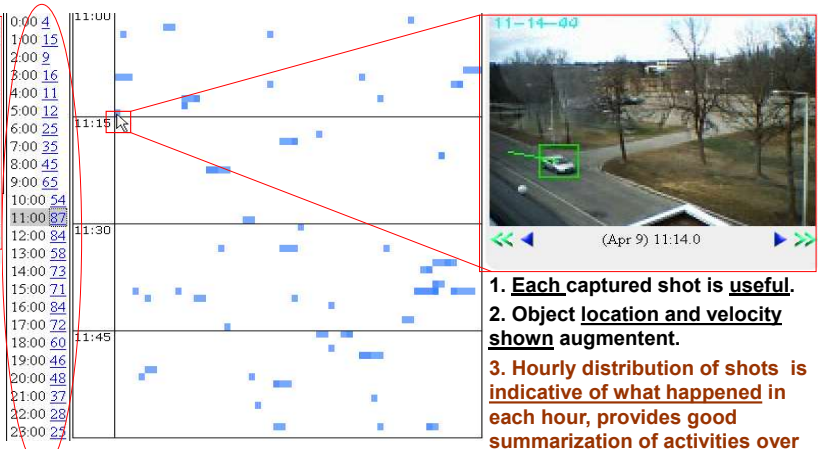
2. Without visual annotation, motion information is lost.

3. Hourly distribution of snapshots is not useful

21

ACE Surveillance "Object-based" capture

(Courtesy: NRC Video Recognition Systems project)

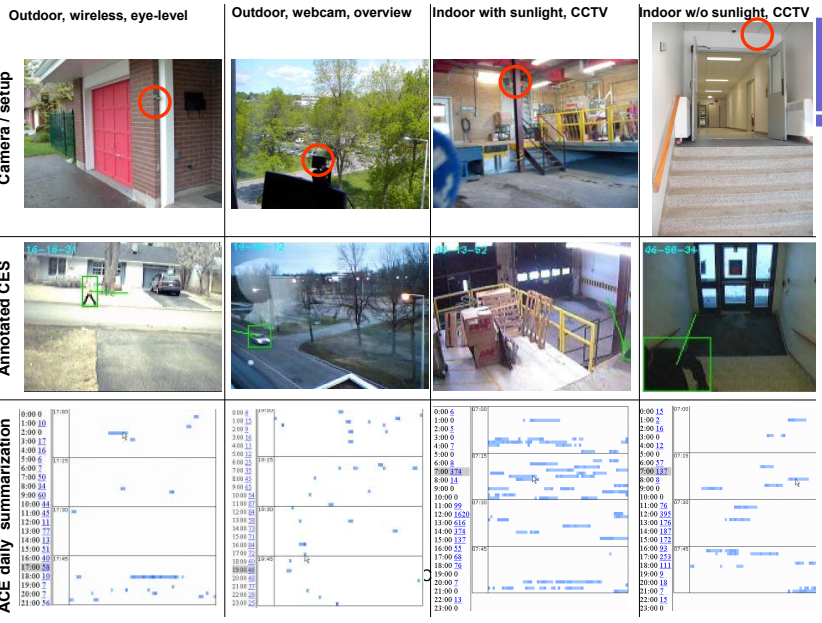


1. Each captured shot is useful.

2. Object location and velocity shown augmentent.

3. Hourly distribution of shots is indicative of what happened in each hour, provides good summarization of activities over long period of time.

22



23

Conclusions

- **Affordable Intelligent Video Surveillance (IVS) is possible!**

However:

- It is possible, only if Video data can be directly accessed by 3rd party software (module)

Other:

- Requires extra training from security officers.
- Requires new protocols to handle automatically extracted evidence.
  - - From forensic prospective, data that are not original and have been processed by a computer can not be considered as evidence.
- Requires new privacy policies.
  - - Surveillance data are normally not kept for a long period of time (<1 month), due to their size. AVS allows to store on local machine many months (even years) of evidence data.

24

Common myths

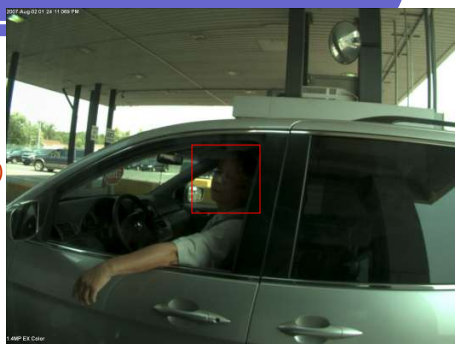
- Naive “Motion detection” not to confuse with Object Detection and Object Tracking.
- The “one-fit-all” myth.
  - Extra video analytics expertise will always be required to set and operate IVS.
  - Solutions are to be provided with SDK / API which allows to customize them.
- The more (data), the better.
  - “30 days or more, but it’s the data quality and ability to efficiently retrieve the desired data that is also very important!”

Special Interest – Face in Video

Video:

Taken in unconstrained environment.

(in a “hidden” camera - like setup)



Result from Pilot Project at Cornwall (2007)

- People
  - don’t not look into camera
  - even don’t face camera
- Poor illumination
- Blurriness, bad focus
- Individual frames of poor quality

Video can also be MPEG compressed (for storage & transmitting)

Conclusions wrt Face Recognition

- Inner square part of the face is most important
- 12 i.o.d. , which is most frequent case, is sufficient for recognition!
  - These face can be automatically extracted.
- If less 10 i.o.d., body/gait biometrics should be used instead.
- Technology is (almost) ready for
  - For limited number of faces (limited access premises)
  - Multiple-camera tracking
- Can be combined with hi-res photo-camera capture

Bottleneck:

- angle of view, quality of video
- 1 to Many is still a problem

- Demo

What is possible – best applications

1. Automated Recognition from ICAO-conformed passport photographs - as good as finger or iris recognition.
2. Human assisted Recognition From Video (not biometrics): Face is automatically extracted from video (e.g. to be linked with boarding pass or vehicle plate number)
3. Face image and geometry automatically extracted from video is used together with other modality (eg. Iris) recognition.
4. Automated Recognition From Video only – is possible, if procedural constraints are imposed (to make video snapshot image quality closer to that of passport image

Currently, no business case is made. But we’ve collected enough data/expertise (inc. from Pilot projects) to be ready!

Appendix E: “Recognition in Video”, The Identity, Privacy and Security Institute, University of Toronto Public Lecture Series, November 30, 2009.

By Dmitry Gorodnichy

Canada Border Services Agency | Agence des services frontaliers du Canada

Recognition in VIDEO

The Identity, Privacy and Security Institute
University of Toronto Public Lecture Series
November 30, 2009

Dr. Dmitry O. Gorodnichy
Video Surveillance and Biometrics Section
Applied Research and Development Division
Science and Engineering Directorate

Canada

Outline

Part 1. History & Background
- Video, Recognition, in GoC
- Recognition taxonomy & main dilemma
- [How brain does it]

Part 2. Surveillance Recognition
- Objectives and Modes of operation
- Problems & Solutions
- Faces in Video: where Surveillance meets Biometrics

Part 3. Biometric Recognition
- Five Biometric Recognition Tasks
- Key Issue: Recognition Confidence →Performance Evaluation

Discussion on Privacy Issues

Part 1. History and Background: Video, Recognition, in GoC

Main Entry: [1]sto·ry

Etymology: Middle English *storie,* from Latin *historia*

Date: 13th century

narrative: a message that tells the particulars of an act or occurrence or course of events;

tale: a piece of fiction that narrates a chain of related events;

history, account: a record or narrative description of past events; "a history of France"; "he gave an inaccurate account of the plot";

report: a short account of the news; "the report of his speech";

Invention of Movie(Video) made Story-telling much easier!

What makes a story ?

- NOUNs
- VERBs

But how do you know that the story is true ?!

Is what you see on TV all true?..

Is what you see on CCTV sufficient to put someone in jail?..

Recognition taxonomy & dilemma

Recognize what?	Automated	By Human	**Requires:**
Noun (Identity)	**Biometrics**	Forensic examination	**Spatial details →Photo**
Verb (Activity)	Video Analytics	CCTV surveillance	**Temporal details →Video**

Heisenberg's uncertainty principle:

Mother Nature does not allow both – temporal & spatial detail !

What is Video?

→ A sequence of still images

→ Continuous stream

→ Captured/Displayed "fast"

→ > 12 frames per second

→ From the same point of view

Continuity in time – this is what VIDEO is all about.

7.

Main Entry: vid·eo, mov·ie

Main Entry: **[1]vid·eo**

Etymology: Latin *vidēre* to see + *-o* (as in *audio*)

Date: 1937

Main Entry: Etymology: *moving picture*

Date: 1911

Main Entry: **motion picture**

Function: *noun*

Date: 1896

1 : a series of pictures projected on a screen in rapid succession so as to produce the optical effect of a continuous picture in which the objects move

2 : a representation (as of a story) by means of motion pictures

8.

History of Video Technology

- ***Video Analytics:* Computational Analysis of Video Data and Extraction of Intelligence from Video.**
- *Better quality, more affordable*
- ***IP cameras***
- ***Digital***
- ***Analog***

21st c.

20th c.

←Animated image example:
The entire 17:00- 24:00 activity is summarized into a few annotated snapshots.

(with our VAP technology)

- 21st c: VIDEO RECOGNITION became possible
- 20th c: MOTION PICTURE (VIDEO) became possible

9.

Demand for Video Surveillance

In the context of enhancing security, Video Surveillance is one of the most demanded technologies in the 21st century.

- Many federal departments (Canada & worldwide) announced major funding for expanding Video Surveillance capacity
- Several projects & initiatives currently at CBSA…

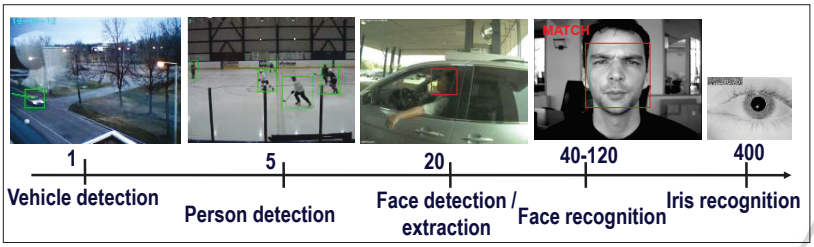
As a result:

"Tsunami" of camera infrastructure build-up and video data that need to be recognized – to create a TRUE STORY!

10.

From Video Analytics to Biometrics

As resolution increases (pixels between the eyes)…

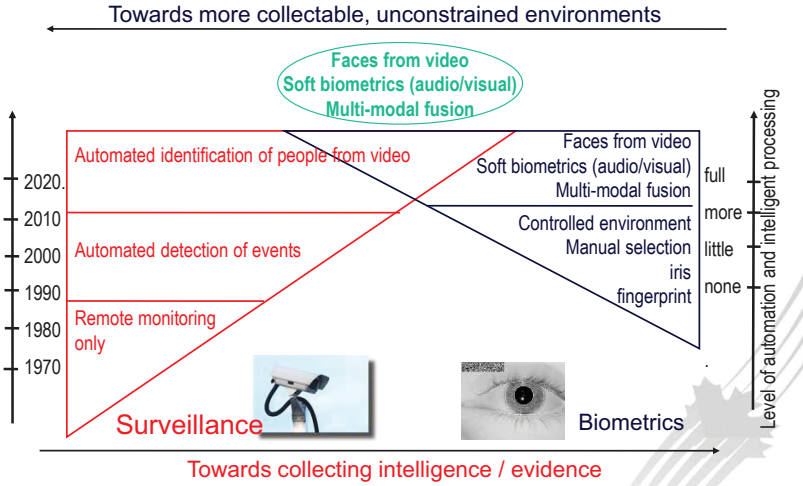


Best synergy & impact is achieved by treating Video Surveillance together with Biometrics.

- … because most Biometrics are image-based.
- Same unique set of skills:
  Image Analysis (CompSci) AND Pattern Recognition (Math).
- Face Recognition – is approached by both

11.

Merge of Biometrics and Surveillance



12.

CBSA-VSB Section

That"s how Video Surveillance and Biometrics Section was created (Jan 2009) -

to support agency"s Portfolios in Video Surveillance and Biometrics

with expertise in Image Analysis & Pattern Recognition (Overlap of Comp.Sci. AND Math)

13.

Canada Border Services Agency

•CBSA was created in December 2003 as one of six agencies in the **Public Safety** (PS) portfolio
  –RCMP is another PS agency

•Integrates „border" functions previously spread among 3 organizations:
  –Customs branch from the former Canada Customs and Revenue Agency (CCRA)
  –Intelligence, Interdiction and Enforcement program of Citizenship and Immigration Canada (CIC)
  –Import inspection at Ports of Entry (POE) program from the Canadian Food Inspection Agency (CFIA)

•***Mandate***: to provide integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods

14.

Three foci of our R&D work:

Our objective: To find what is possible and the best i

- **in Video Analytics, Biometrics, Face Recognition**
- **For LAND (Outdoor) and AIRPORT (Indoor)**

to be in a position to recommend solutions to CBSA & OGD.

Focus 1: Evaluation of Market Solutions

Focus 2: In-house R&D

Focus 3: Live Tests/Pilots in the Field

15.

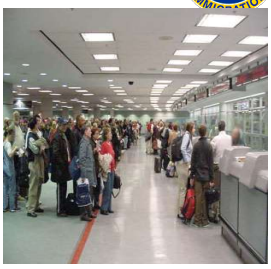
Cameras at CBSA

Cameras are used:

- Either for Photo capture
- Or for Video capture

16.

NEXUS Iris Recognition



Cross often? Make it simple, use NEXUS.

NEXUS is designed to expedite the border clearance process for low-risk, pre-approved travellers into Canada and the United States.

17.

NEXUS Iris Recognition (cntd)

Fully operational at:

Vancouver International Airport
Halifax International Airport
Toronto- L.B. Pearson International Airport
Montréal – Trudeau International Airport
Calgary International Airport
Winnipeg International Airport
Edmonton International Airport
Ottawa-MacDonald Cartier International Airport

More about NEXUS:
1-866-639-8726, www.nexus.gc.ca, CBSA Travellers Systems Team.

NB: Number of members is growing!

Recognition performance deteriorates as more templates are stored…

18.

Cameras at Airports

: many installed …

19.

Many faces seen in cameras

One camera can be used for both:

- For identification, and
- For storytelling
- 0.5 Mp (800x600) camera data is manageable : 4 TB for 90 days

20.

Cameras at Points of Entry (Land)

: several installed

21.

Two types of cameras needed

- One – for storytelling:
  - Court requires: Continuity in time
  - Resolution does not matter (can be low)

- One – for identification:
  - Court requires: Sufficient visual detail
    - License Plates
    - Faces
  - Resolution must be high

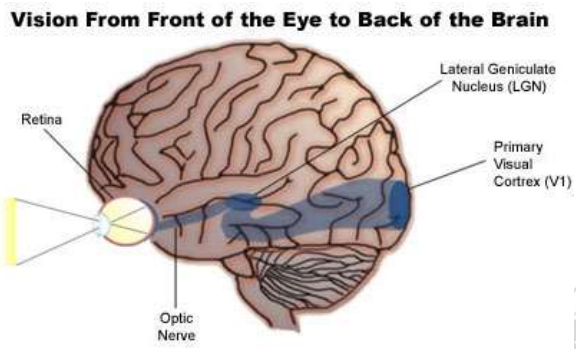
Trying to do both tasks with one camera is WRONG !

- 11 Mp (4000x750) at 30 fps makes data unmanageable (1Tb/day)

22.

How do we see and recognize?

How we (humans) do it:
A few lessons from Mother Nature



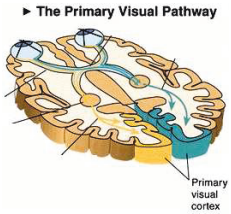
Human brain is a complicated thing …

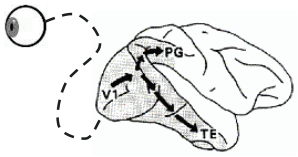
… but a lot is known and can be used.

23.

24.

Where vs. What / Saliency vs Goals





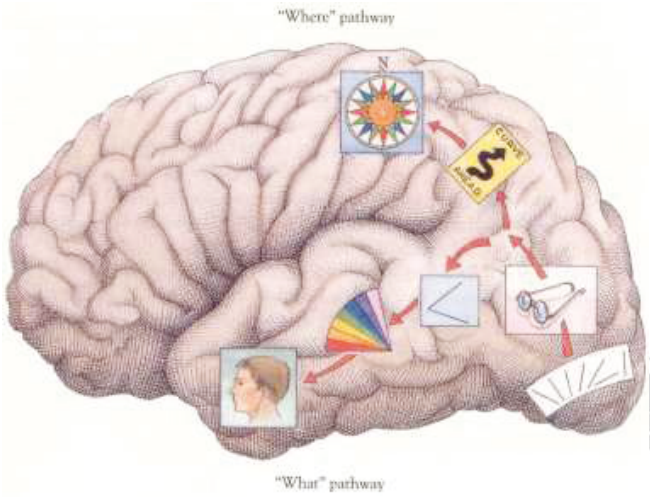
Localization vs recognition - in different parts of brain: Dorsal ("where") vs Ventral ("what") stream)

Visual saliency-driven vs goal-driven localization (25ms vs 1sec)

Refs: Perus, Ungerleider, Haxby, Riesenhuber, Poggio …

25.

Visual pathway



26.

Lesson 1: order of recognition tasks

Try to recognize this face →

Detection
↓
Tracking
↓
Recognition

Note how you scan the image with your eyes and accumulate evidence over time

27.

Lesson 2: Colour vs intensities

You can detect a face in any colour inverted space →

You can recognize a face in BW just as well as in colour:
(Even for visa purposes !)

Colour, motion - for localization
Intensity - for recognition

28.

Lesson 2a: four modalities

Pendulums for my daughters (for 1-3 months olds)

Detection by saliency
in a) motion, b) colour, c) disparity, d) *intensity.*
•These channels are processed independently in brain
(Think of a frog catching a fly or a bull running on a torero)
•*Intensity* is not raw values, but: frequencies, *orientations*, **gradients** .

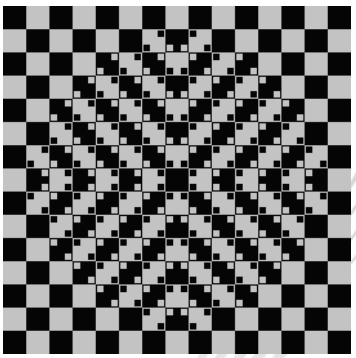
29.

Lesson 3 & 4

For us: all video data are of low quality (except a fixation point) : Saccadic eye motion, Fovea vision

Accumulation over time:

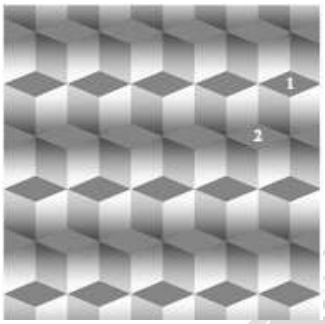
- **We don't need high res**
- **Data are accumulated over time**



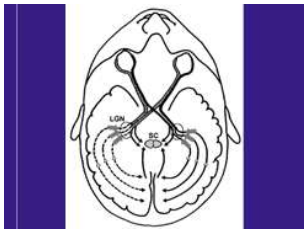
30.

Lessons 5 & 6

- **Local processing**
- **Non-linear colour perception**



Lesson 7



- **We recognize associatively**
- **Associative memory allows us to accumulate (tune) data (knowledge) over time**

Part 2. Video Surveillance

Recognition taxonomy & dilemma

Recognize what?	Automated	By Human	**Requires:**
Noun (Identity)	Biometrics	Forensic examination	**Spatial details →Photo**
Verb (Activity)	Video Analytics	CCTV surveillance	**Temporal details →Video**

Why ?

… to improve national security, program integrity and officer and public safety.

- CBSA is a major user of Video Surveillance at Land and Air POEs
- Significant volumes of Video Data captured and stored at CBSA

External drivers:

- "Complete monitoring of customs controlled areas" (2006, Senate Committee on National Defence and Security)
- "Face recognition and other biometric technology at border crossings and ports of entry" (2007, Federal Election Platform)

Consistent with Lab Strategy"s areas of technical focus:

- Advanced Analysis and Analytics; and
- Sensor development/testing and Integration

Where ?

In all critical infrastructures esp. in high-risk zones:

- Extensive Coverage
- Complete coverage - no blind spots

Two main domains of application:

- to monitor within – violations by agency personnel
- to monitor without – violation by agency visitors

Objectives

Five security functions:

- Deter
- Detect (produce alarm)
- Respond (analyze in real-time causes and decide on actions)
- Investigate (after incident)
- Reassure community

Four operational objectives:

- observe
- Detect (abnormality/event)
- Recognize (sufficient detail to be stored as intelligence, to describe event/incident)
- Identify (sufficient detail to be used as evidence)

Real-time vs. Archival operation

Three modes of operation:

- **Active**
- **Passive** ← most common (in conjunction with other duties)
- Archival (thru recording)

Three components commonly to be integrated with:

- audio
- real-time video analytics software
- peripheral devices: heat sensor, fire-alarm, smoke/radio-activity detection etc.

Problems in real-time modes

An event may easily pass unnoticed .

- due to false or simultaneous alarms,
- lack of time needed to rewind and analyse all video streams.

No time to react in real-time (efficiently)

- Because no intelligence is available (until Agent extracts it from video data)

Table 1: Camera Solutions

Problems in Archival mode:

Due to temporal nature of data:

Storage space consumption problem

Typical assignment:

2-16 cameras, 7 or 30 days of recording, 2-10 Mb / min.

➔1.5 GB per day per camera / 20 - 700 GB total !

Data management and retrieval problem

London bombing video backtracking experience:

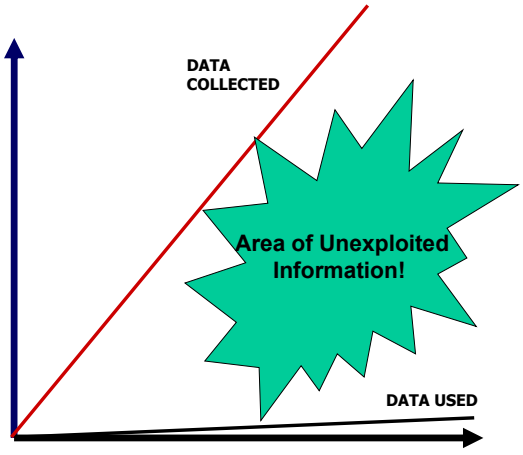
"Manual browsing of millions of hours of digitized video from thousands of cameras proved impossible within time-sensed period"

[by the Scotland Yard trying to back-track the suspects] [L'Actuality, 15 oct. 2008]

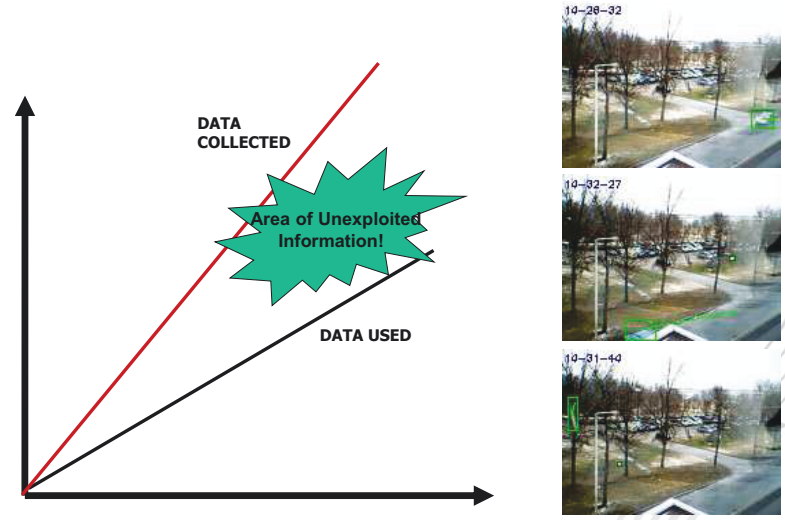
Video sources

	Image Frame size	MP	Storage requirements MJPEG in TB	Storage requirements H.264 in TB	Bandwidth MJPEG (MB/s)	Bandwidth H.264 (MB/s)
TV, webcam	320x240	0.08	0.64	0.08	0.08	0.01
VGA, USB2 webcam	640x480	0.31	2.55	0.16	0.33	0.02
DVD, 4CIF	720x480	0.34	2.87	0.16	0.37	0.02
SVGA ($800)	800x600	0.48	3.98	0.24	0.51	0.03
HDTV	1280x 800	1	7.72	0.4	0.99	0.05
Full HD	1920x 1080	2	17.36	0.96	2.23	0.12
3Mp ($3K)	2048x 1536	3	26.36	1.35	3.39	0.17
5MP	2600x 1950	5	42.44	2.23	5.46	0.29
11Mp ($20K)	4000x 2750	11	85	5	12	0.6

Without Video Analytics - as it is now



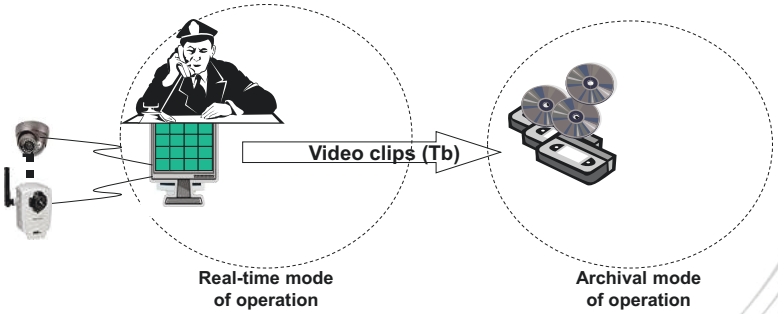
With Video Analytics - what we can do



43.

Monitoring Tasks Performed by Human (Status quo)

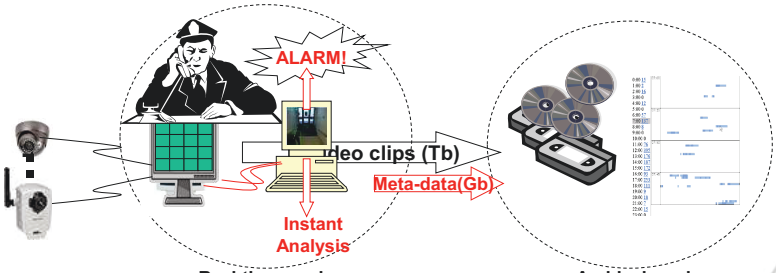
Two modes: a) real-time monitoring, b) post-event analysis



44.

Monitoring Tasks Performed by Human & Software

Two modes: a) real-time monitoring, b) post-event analysis



Real-time mode of operation
Capture filters / modules

Archival mode of operation
Retrieval modules / software

Main condition - Open Architecture:
To be able to tap into (video signal) input and (data) output.

45.

Video Analytics Technology Readiness

Traditionally performed by Humans, many of these Monitoring Tasks can now be facilitates with VA software

TYPE 1: Real-time monitoring tasks	Customization, testing req.-d	Technical readiness
1* - "Face extraction/tagging"	Little	5
2* - "Wrong direction detection (Run-away alarm)"	Little	5
3 - "Loitering alarm"	Major	4
4 - "Object-left behind or abundant object alarm"	Major	4
5 - "Tripwire (trespassing) alarm"	Little	5
6 - Other events (door opening, car parking etc) alarm	Major	4
General Tracking / Detection of people in multiple streams	-	1
TYPE 2: Post-Event (Archival) monitoring tasks		
1 - Summary of detected events & statistics (trends)	Little - Medium	5
2 - Searching for a object/person in stored streams	Little - Major	5
General Summary / Search in unstructured environment	-	1
Special case tasks		
LPR (License Plate Recognition)	None	5
Face Recognition	Little-Medium	1-4

5 – ready, 4 – requires Evaluation only, 3/2– requires further Refining/Exploration, 1 – not yet ready

46.

ACE Surveillance™ real-life tests [Gorodnichy, Mungham, NATO-2008]

Faces in Video

48.

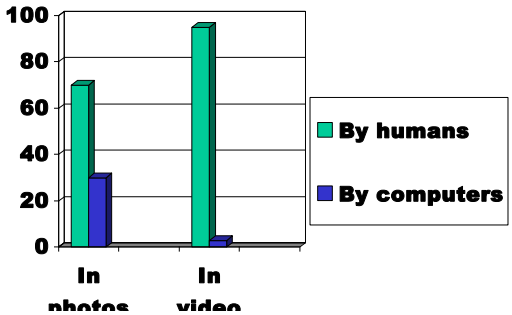
MAIN Peculiarity of Face Recognition

- The only Biometric modality that can also (and easily) be used by Humans:
  - High expectations
  - "Human + computer" approach should prevail

PLAY VIDEO

Current situation: computers fail, humans succeed

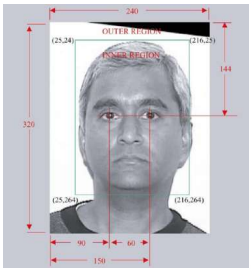
Face recognition* systems performance



* But there are different types of recognition

In Video vs in Passports

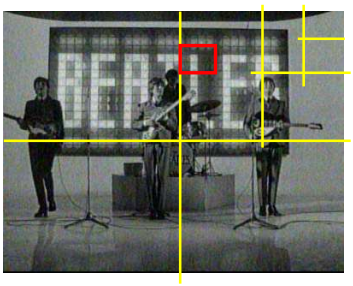
- Faces stored on documents are much easier to recognize than faces from videos. Photos taken in a controlled environment provide:
  - **Canonical face model adopted by ICAO'02 for passport-type documents**
  - high resolution - 60 pixels **i.o.d.** (intra-ocular distance)
  - high quality
  - face "nicely" positioned
- Videos taken in much less constrained/less controlled environment, e.g. "hidden" camera, where people do not usually face the camera, result in:
  - Poor illumination
  - Blurriness, bad focus
  - Individual frames of poor quality

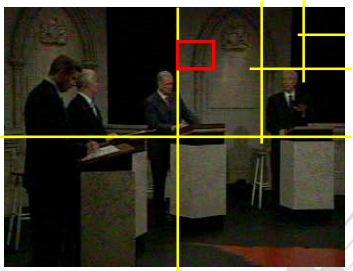


Constraint / requirement #2 – low resolution

In TV & VCD (e.g. in movies): 320x240

Faces often occupy not more than 1/16 of screen…

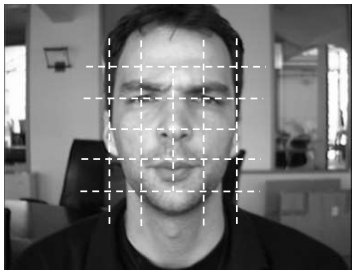




And that's OK for humans !

Head = 20-40 pixels **between eyes = 10-20 pixels**

Applicability of regular CCTV video(320x240) for Face Recognition tasks



Face size	¼ image	1/8 image	1/16 image	1/32 image
In pixels	80x80	40x40	20x20	10x10
Between eyes-IOD	40	20	10	5
Eye size	20	10	5	2
Nose size	10	5	-	-
FS	√	√	√	b
FD	√	√	b	-
FT	√	√	b	-
FL	√	b	-	-
FER	√	√	b	-
FC	√	√	b	-
FM / FI	√	√	-	-
Person detection	√	√	√	√

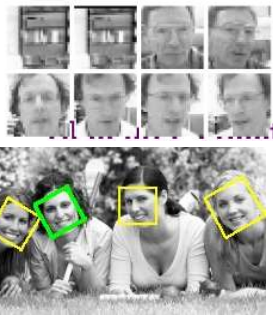
√– good
b – barely applicable
- – not good

Segment, Detect, Track, Localize, Expression, Classify, Memorize/Identify

Good news: Faces can be detected!

2002: computers can detect faces
with i.o.d >= 10 pixels
in poor illumination,
with different orientations: +/- 45°
different facial expressions

2007.



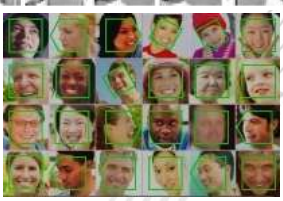


TABLE I
READINESS LEVEL OF FACE RECOGNITION TECHNOLOGIES
5 - ready for deployment, 4 -needs minor R&D, 3 – needs some R&D, …
0 - not ready at all

RL=5	Human-assisted Recognition From Video (not biometrics per se), where face is automatically extracted from video, e.g. to be linked with boarding pass or vehicle plate number or matched with passport photo.
RL=4	Face image and geometry automatically extracted from video is used together with other modality (eg. Iris) recognition.
RL=3	Automated Recognition from ICAO-conformed passport photographs - as good as finger or iris recognition.
RL=3	Automated Recognition From Video only – is possible, if procedural constraints are imposed (to make video snapshot image quality closer to that of passport image).
RL=3	Identification in small-size database, as in monitoring access-restricted areas applications.
RL=0.1	General unconstrained automated face recognition.

5.

Part 3. Biometric Recognition

56.

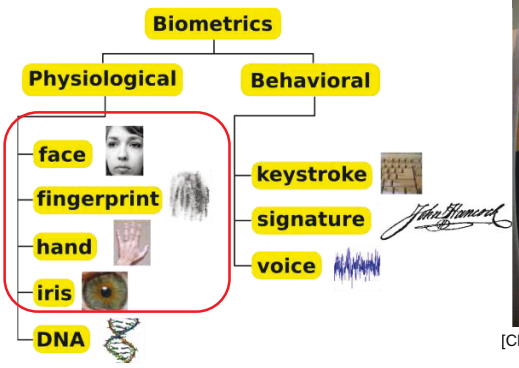
Recognition taxonomy & dilemma

Recognize what?	Automated	By Human	Requires:
Noun (Identity)	**Biometrics**	Forensic examination	**Spatial details →Photo**
Verb (Activity)	Video Analytics	CCTV surveillance	**Temporal details →Video**

57.

What is Biometrics?

Biometrics is an automated technique of measuring a physical characteristic (**biometric data**) of a person for the purpose of recognizing* him/her.




[CBSA NEXUS Iris Recognition system]

NB: Most biometric **modalities** are image-based!

58.

Five operational "recognition" tasks

1. Verification (1 to 1, aka Authentification)

Is it "John Doe" (name on his card) ?
(eg. RAIC Access Card)

2. Identification (1 to N, from "White List", **N is large and growing)**

Who is he? ➔ If not identified, follow SOP …
(eg. Pre-enrolled members)

3. Screening (1 to M, from "Black List", **M is fixed and not large)**

Who is he? ➔If identified, follow SOP …
(eg. Terrorists)

4. Classification / Categorization (1 to K, **K – small**)

What is his type (eg. Gender, Age, race) ? ➔ Soft biometrics

Whom of K people he resembles most ? ➔ tracking/matching

5. Similarity quantifier/filter (for forensic investigation)

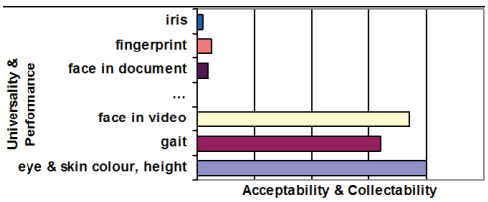
Final decision made by Forensic Analyst (ie decision is NOT automated)

In either case: No "magic bullet" – There will be False Positives and False Negatives!

59.

Biometric modality characteristics

Universality: each person should have the characteristic	g
Uniqueness: how well separates individuals from one another.	g
Permanence: how well a biometric resists aging/fatigue etc	g
Circumvention: ease of use of a substitute.	? m
Performance: accuracy, robustness of technology used.	? m-g
Collectability: ease of acquisition for measurement.	? m-g
Acceptability: degree of approval of a technology	? m-g



?

2001 - 2009

60.

CBSA NEXUS Iris Recognition

Cross often? Make it simple, use NEXUS.

NEXUS is designed to expedite the border clearance process for low-risk, pre-approved travellers into Canada and the United States.

Why iris? (not Fingerprint or Faces)

Must be easily accepted by public: not intrusive

Must not have a bad association

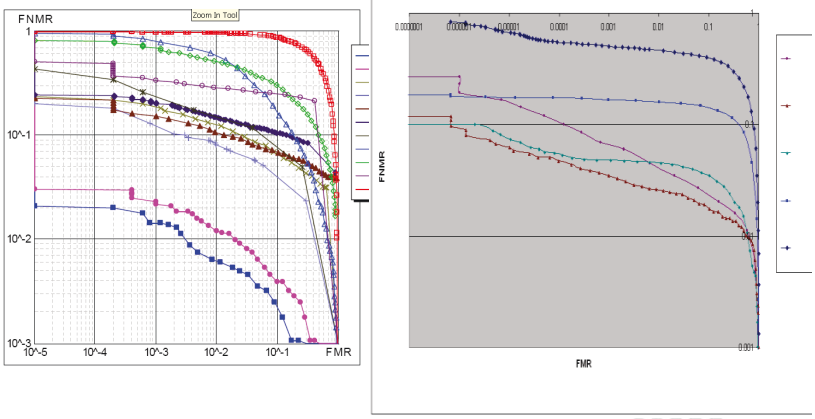
To take a fingerprint image – be treated like a criminal

To take a face (eyes) photo – be treated like a traveller

… so that people would voluntarily participate (and cooperate)

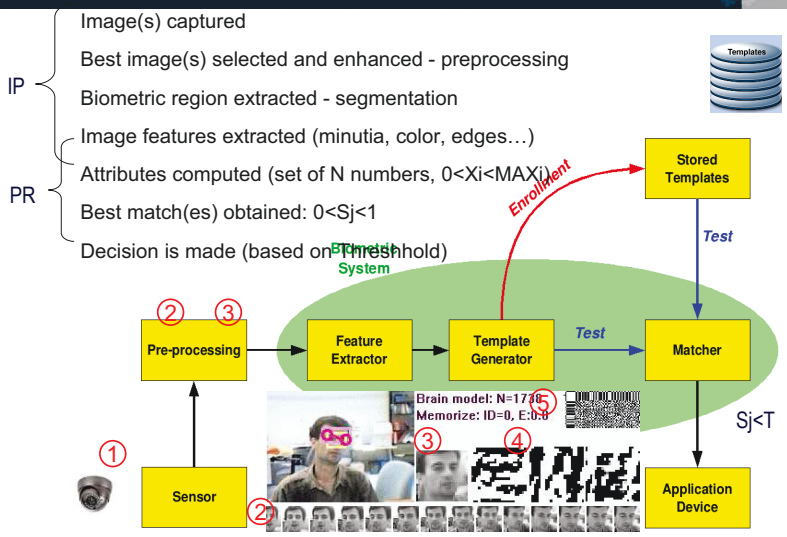
Yet, be well-performing…

Iris vs. Fingerprints



DETs of FVC2000 DB1 Competition Results (Various Algorithms)

Why Biometrics may fail?



Why technical evaluation is needed?

Only DNA match is (almost) perfect. Other biometric modalities will never be error-free.

However, critical errors can be minimized to the level allowable for operational needs - with proper performance evaluation and optimization strategy.

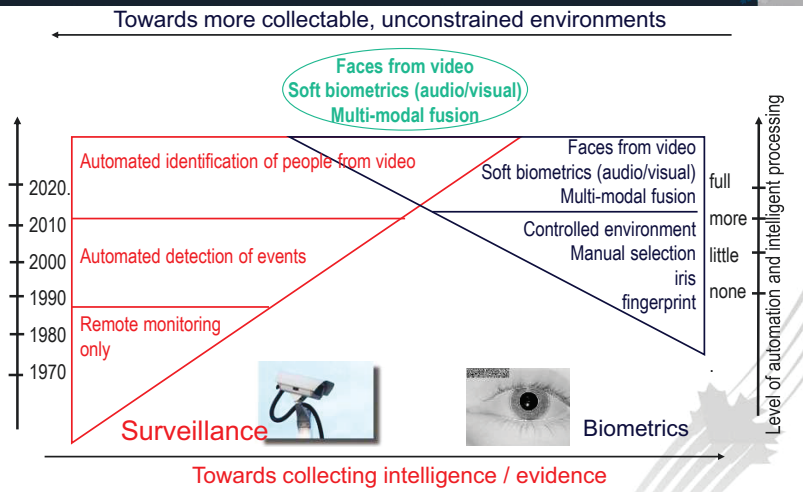
Many factors affect the performance (lighting, location etc)

+

Performance deteriorated over time (as number of stored people increases and spoofing techniques become more sophisticated).

However, there are also many ways to improve it (eg. more samples, modalities, constraints)

Merge of Biometrics and Surveillance



Merge of Biometrics with Video Surveillance

As a result of evolution, the arrival of such biometric technologies as

- *Biometric Surveillance*,
- *Soft Biometrics,*
- *Stand-off Biometrics*, also identified as *Biometrics at a Distance*, *Remote Biometrics*, *Biometrics on the Move* or *Biometrics on the Go*
- And an increased demand for *Face Recognition from Video*,
  - which is where Biometrics meets Video Surveillance and
  - which is seen as a golden solution to many operational needs.

67.

Important Conclusion

As computers become faster and more automated intelligent processing becomes possible…

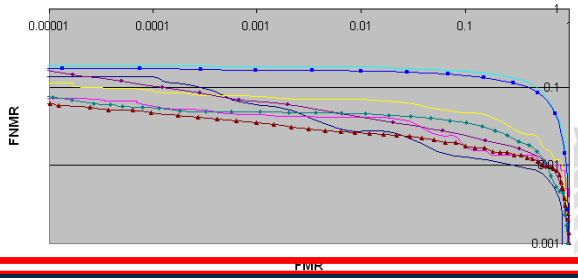
Biometric systems are increasingly applied to less intrusive, less constrained, free-flow surveillance-like environments, where biometric data can be acquired at a distance and possibly in inconspicuous (covert) manner.

As a result, for such systems to achieve reliable performance, the *recognition results may need to be integrated or fused over time and/or with results obtained from other biometric systems.*

68.

Status-Quo performance evaluation

- **False Match Rate (FMR)**
  (False Accept, False Positive, False Hit, Type 1 Error)
- **False Non-Match Rate (FNMR)**
  (False Reject, False Negative, False Miss, Type 2 Error)
- ***Detection Error Trade-off* (DET) curves** - the graph of FMR vs FNMR, which is obtained by varying the system parameters such as **match threshold**.



69.

Stereotype: Biometrics as a door opening device

Intelligence gathering is NOT just about counting binary events!

TABLE II
BIOMETRIC SYSTEMS VS. PROXIMITY SENSORS

	Biometric systems (for access control)	Proximity sensors
Application Task	Open the "door" for *the* person	Open the "door" for *a* person
Measurements taken	Similarity distance (match score): S	Distance to a person: D
Tasks achieved	when S < T	when D < T
Calibration done by	computing similarity distances of genuine and imposter data	measuring distances at different ranges
Performance metric	FMR, FNMR (ROC / DET curves)	FMR, FNMR (ROC / DET curves)

Best 5 scores:	Or:
0.61	0.51
0.59	0.38 *
0.36 ***	0.39 *
0.49	0.41 *
0.57	0.67

70.

Request for new ISO Biometrics standard

- Recent Canadian contribution (for meeting in Moscow, July 2009)
  - **CBSA's request for New Work Item Proposal (NWIP) for SC 37 WG 5: Biometric Performance Testing and Reporting - Testing Methodologies for Comprehensive Evaluation**

"There is a need for a comprehensive biometrics performance evaluation standard that would take into account not only the best matching scores, but also the "runner-up"matching scores.

Such standard would be most applicable for evaluation of stand-off identification systems, such as Face or Iris Recognition from Video. The standard however would also be applicable for verification systems, in particular to those that make the decision based on examining the entire database of enrolled identities."

71.

Beyond binary error trade-off curves ("door opening" counts)

Multi-order biometric performance analysis [Gor2009a]

Order 0:

- See ALLs scores distributions

Order 1:

- See the trade-off and FMR/FNMR as function of threshold

Order 2:

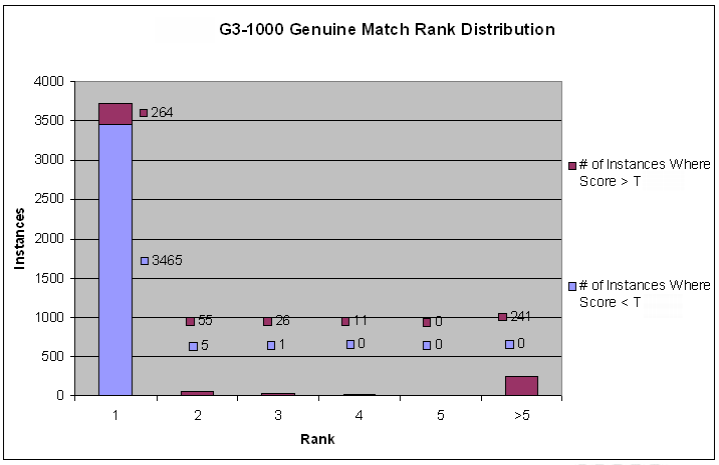
- Find best scores (Do they coincide with genuine images?)

Order 3:

- Find second best scores and ALL scores below threshold

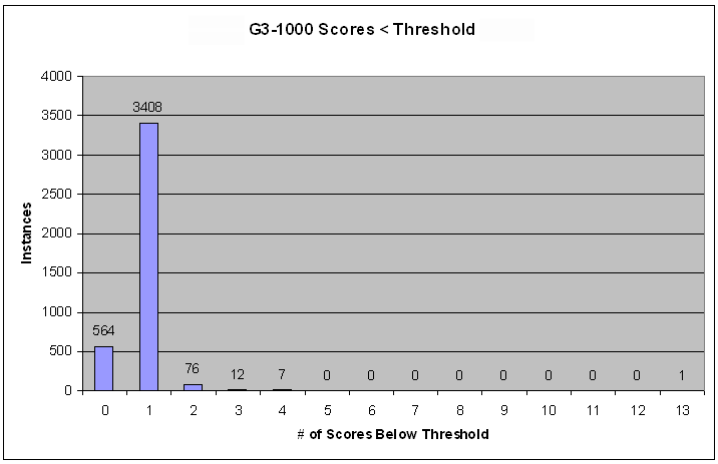
72.

Order 2. Do Genuine data have best scores ?



73.

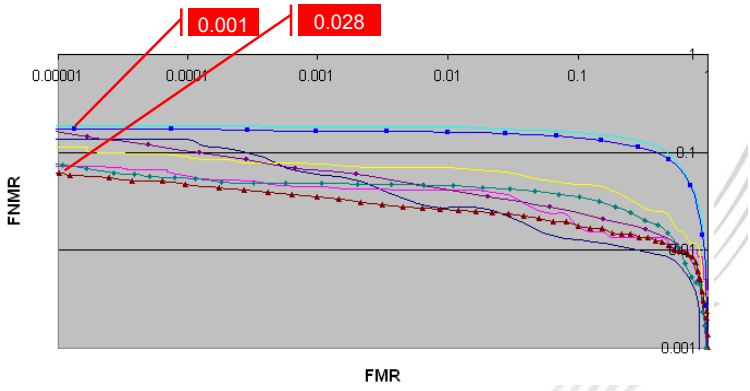
Order 3: Recognition confidence I



74.

Better Trade-off Curves: with FCR

DEFINITION: **Failure of Confidence Rate (FCR)** – the rate of incidences in which there are more than one match below threshold



75.

Better Performance Report Card

FTA=0.23	FMR	FNMR	FCR
	0.00067	0.0688	0.122
	0.00028	0.0854	0.059
	0.00012	0.1000	0.029
	0.000050	0.1195	0.013
	0.000017	0.1429	0.0048
	0.000007	0.1669	0.0008
	0.000001	0.1932	0.0004

Fig.8. All-inclusive biometric performance summary should report such information as FTA (Failure to Acquire rate) as well as FCR (Failure of Confidence Rates) in addition to commonly used False Match (FMR) / False Non-Match (FNMR) rates obtained by varying a match threshold.

76.

Privacy , Ethics & Cultural Questions

Is there an assumption of privacy?

- In access-controled areas
- In high(er) security zones
- In public places

Can you video-tape yourself at public places?

- With higher than human-eye resolution cameras?
- 24/7 ?

Can be recorded video data used for

- fun, R&D, testing
- collecting intelligence about someone

77.

Time for the show … and discussions

Enjoy the movie!

And as you watch it, ask yourself:

- What & whom do I recognize?
- How I do it?
  What my eyes are looking?
  What"s the resolution?
  What my brain is doing?
  What makes it so efficient for me?
- Can computer do it?
- What computer can do?
- Can it be used for evidence?
- …

THANK YOU!

78.