Automatic surveillance systems against security threats

A. Zanasi[1] & M. Artioli[2]
[1]ZANASI Alessandro Srl, Modena, Italy
[2]Bridge 129 SPA, Reggio Emilia, Italy

Abstract

New threats to security have appeared in recent years: terrorism, organized crime, trafficking, smuggling, proliferation of weapons of mass destruction, the role of video and the Internet in spreading extremist propaganda is currently highlighted. The reaction to the new threats is slowed for the huge, unmanageable amount of available data about them. To contrast these new threats and their new "weapons", the research in automatic surveillance technologies (i.e.: able to detect criminal or suspect behaviour without human help) has quickly advanced. Intelligence analysts in their daily fights are profiting of these new surveillance technologies (e.g. advanced CCTV and crawlers, text and video mining) to automatically analyze the content of video data streams, suspected web sites containing videos, blogs, emails, chat lines, instant messages and all other digital media detecting links between people and organizations, trends of social and economic actions, topics of interest also if they are "sunk" among terabytes of information. Examples of application are here presented.

Keywords: surveillance, text mining, video mining, national security, intelligence.

1 Introduction

1.1 Security threats

1. New information technologies help to take profit of the *information* (often contradictory) *explosion* (information density doubles every 24 months and its costs are halved every 18 months [1]); open to the contributions of the best

doi:10.2495/SAFE090251

experts, also outside government [2], e.g. through a *public-private partnership* (PPP or P3: a system in which a government service or private business venture is funded and operated through a partnership of government and one or more private sector companies).

2. The role of *competitive intelligence* has assumed great importance not only in the corporate world but also in the government one, largely due to the changing nature of national power which rests to a significant extent on energy production control, industrial and financial power.

3. New terrorists are typically organized in small, widely dispersed units and coordinate their activities and organize attacks on line, (*Netwar* phenomenon [3]). Due to this growth of *virtual communities*, a strong interest towards the capability of automatic surveillance inside these communities is also growing.

4. The Internet provides an anonymous and low cost way for terrorists to filter through potential recruits and for potential recruits to take their first steps toward *radicalization*. Consequently the need to improve automatic Internet monitoring techniques to trace terrorist recruitment on the web is improving.

5. Since there are some 4,500 web sites that disseminate the al Qaeda leadership's messages [4], it makes more sense to leave those web sites online but watch them carefully and automatically capturing texts and videos, understanding terrorists' cultural backgrounds-skills [5], [6].

For an introduction to automatic intelligence: data mining: [7], text mining and its applications to intelligence: [8], video mining: [9].

1.2 Automatic surveillance as prevention solution

1. Currently we are all being surveilled. It is no longer possible to avoid cameras, DNA tests, identity chips, border crossing cameras, highway monitors, ATMs and other devices that record our movements, finances and even our health. Many people do not realize that their activities are catalogued and stored in a multitude of databases, many of which are accessible on the Internet without the surveillée's knowledge or permission. Examples of this trend are:

- Detailed information about people who have never logged onto the Net nor even used a computer is available to anyone with an Internet connection.
- Some hospitals now routinely take DNA samples of newborn babies.
- Nude photos of unwary victims are sold on the Internet without the knowledge or permission of the surveillée.
- Law enforcement agencies are consolidating their forensic and criminal databases and providing Internet access to authorized personnel from any part of the country.
- These surveillance activities provide a huge volume of openly available data which may be analyzed and understood only by using automatic techniques as data, text and video mining.

2. Today's *intelligence analysts* (either working in marketing, corporate or national security) must wade through an exponentially increasing amount of data (classified and open sources) to uncover potentially key nuggets of valuable information in time for them to be transformed into timely, actionable intelligence.

3. In *marketing* text mining helps in analyzing emails, chats, blogs [10] and video mining captures the movement of people through a shop, in order to spot shoplifting activity and /or observe the order in which people browse through the store.

4. *Competitive intelligence* [11] is still an area of strategic interest [8]: we can regard what competitors are doing and what they will do in the future easily analyzing automatically their patents, their executives' declarations, the press surveys.

5. From the London subway to the recent Mumbai bombing attacks, there were suspicious activities before the attack. Individually considered, each event does not exhibit sufficient significance to trigger an alarm, but if we combine the video evidence from all relevant sites, the unusual events become more obvious.

Video mining with capability of unusual event detection in high volumes of videos is a central technology not only to react to but also to prevent terrorist threats to *National Security* [12], [13].

1.3 Authors' organizations

1.3.1 Zanasi Alessandro Srl

ZANASI Alessandro SrL is a consulting and advisory company, incorporated in Italy and active internationally, serving security research market, focusing on surveillance technologies application, founded in 2006, appointed in 2007 ESRIF member.

1.3.2 Bridge129

Bridge 129 was founded in 2000 with HQs in Reggio Emilia (Italy) and branch offices in Rome and Modena, focused in developing advanced safety and security research (especially in computer vision, video management for security, data retrieval from video and from texts, chats, social networks.

2 Surveillance technologies

2.1 Text mining

Text mining (coupling data mining with linguistics) allows the user to extract the principal topics of interest to him among huge amount of text (e.g. organization and people names, email addresses, bank account, phone and fax numbers but also sentiments and feelings as they appear in the data set, lists of organizations working with a predefined technology or the journalists supporting an opinion or the key players of a political group).

2.2 Video mining

Video mining (coupling data mining with computer vision) seeks to automate what is now a very tedious, generally human-powered process of reviewing video for content that is potentially of intelligence value detecting, for example, anomalous behavior, bombings or beheadings.

The objects' extraction process usually involves modelling, segmentation of the movement and classification of objects.

2.2.1 Segmentation models of the movement

The segmentation of the movement aims to determine the regions where objects are (people or vehicles) in motion. We summarize briefly our different approaches to the segmentation of the movement.

- **Subtraction of the background**. We recognize the regions in motion by a subtraction pixel for pixel between the frame and image of the background.
- **Time difference**. This technique, to extract the motion, makes the difference between two or more consecutive frames in a sequence.
- **Optical Flow**. The methods based on optical flow can be used to determine moving objects in the context of camera-motion.

In addition to the basic methods previously cited we use several more complex background models. The most common is the Mixture of Gaussians.

2.2.2 Classification of objects in motion

The approaches to the classification of moving objects are grouped into two categories: classification based on shape, and classification based on movement. The first ranks regions of movement according to their geometric properties, while the second by comparing their movement with reference models, for example, a person who walks makes periodic movements, while not a vehicle in transit.

2.3 Text retrieval from video

Examples of text to be extracted include car plate numbers, headlines comments and text on objects.

The number plate recognition basically requires much more work and attention compared to headlines comments. On the other side the extraction of data within image/video is dependent to image environment and no often easy to extract. I.e. the plate of a car can be affected by light reflections, dust and so on. In this case text retrieval applicability really depend on video source quality.

2.4 Smoke and fire detection

We developed autonomous and automatic video surveillance system, capable of independently detecting the presence of smoke or flames in a video stream from a fixed camera by emulation of artificial processes of visual human observation.

This detection method does not use any kind of sensor and it is able to monitor open environment (power plants, cities, forests... where it is not possible to use electronic sensors) and large closed areas (where electronic sensor response is too slow). Detection time: 3-10 seconds. Detection rate: 100% after 10 seconds.

3 Current challenges

3.1 Outdoor scenario

There are many differences between indoor and outdoor scenario. Outdoor noise really affect the performance and an extended research activity must be done to cover aspects like scene vibrations, camera movements, noise in the signal, noise from weather condition and a combination of these aspects.

The goal is to reach a great robustness in image segmentation providing a near zero false extracted items.

3.2 Virtual communities surveillance

Most virtual community (e.g. blogs and chats [14]) members need to interact with a single individual in a one-to-one conversation or participate and collaborate in idea development via threaded conversations with multiple people or groups. This type of data is a usual source to be automatically mined looking for radicalization process traces and other dangerous behaviour.

4 Video mining theory/algorithm

4.1 Introduction

The proposed method consists of three stages: candidate text region detection, text region localization and character extraction.

4.2 Candidate text region detection

This stage aims to build a feature map by using three important properties of edges: edge strength, density and variance of orientations. The feature map is a gray-scale image with the same size of the input image, where the pixel intensity represents the possibility of text.

4.3 Text region localization

We use a morphological dilation operator with a 7×7 square-structuring element to the previous obtained binary image to get joint areas referred to as text blobs.

Two constraints are used to filter out those blobs, which do not contain text, where the first constraint is used to filter out all the very small isolated blobs whereas the second constraint filters out those blobs whose widths are much smaller than corresponding heights.

The retaining blobs are enclosed in boundary boxes. Four pairs of coordinates of the boundary boxes are determined by the maximum and minimum coordinates of the top, bottom, left and right points of the corresponding blobs. In order to avoid missing those character pixels, which lie near or outside of the initial boundary, width and height of the boundary box are padded by small amounts.

4.4 Character extraction

Existing OCR (Optical Character Recognition) engines can only deal with printed characters against clean backgrounds and can not handle characters embedded in shaded, textured or complex backgrounds. The purpose of this stage is to extract accurate binary characters from the localized text regions so that we can use the existing OCR directly for recognition.

5 Automatic surveillance exemples

5.1 APR –automatic plate recognition

Several cities administrations have installed Bridge129 visual surveillance systems that can read the license plates of vehicles passing a checkpoint, detecting the name of the car owner and automatically relay law enforcement information that may be relevant to the computer terminals of inspectors in nearby booths of buildings.

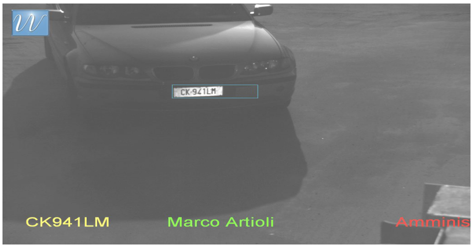


Figure 1: APR example.

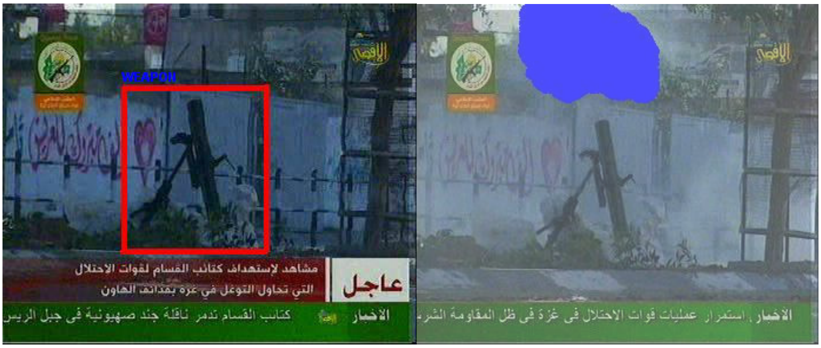

WEAPON
عاجل
مشاهد لإستهداف كتائب القسام لقوات الاحتلال
التي تحاول التوغل في غزة بقذائف الهاون
الاخبار
كتائب القسام تدمر ناقلة جند صهيونية في جبل الريس
الاخبار . استمرار عمليات قوات الاحتلال في غزة في ظل المقاومة الشر

Figure 2: Weapon and smoke detection.

The image shown refers to an outdoor camera installation in daytime with sun against.

The software acts like a plate detector and number plate recognition. The plate in effect is found and bounded via a blue rectangle. The algorithm searches inside this limited area the characters (segmentation process) and yields the plate read with the name of the owner of that plate (if connected to plates owners database).

5.2 Smoke

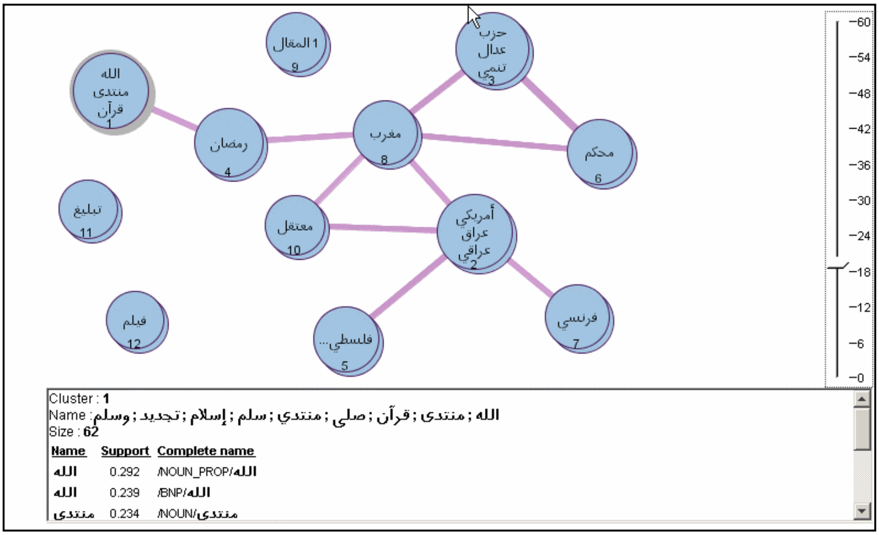
Left frame refers to a truck explosion showing the real image. The action and smoke propagation is very fast. In the right frame a blue mask show the algorithm detection. The detection speed is about one second.

Video analysis Al-Aqsa TV, January 6, 2009. Also this video is taken outdoors and shows different components: weapon, smoke, text. Applying different algorithms we can detect either smoke or text (images below).

5.3 Arabic texts

Applying the methods of text extractions we can filter from the scene the text on headlines comments.

Detection time is 1-3 seconds. Once the text is retrieved and collected from the web, it may be automatically analyzed thanks text mining, extracting key concepts and/or clustering thematically coherent pages.



Cluster : **1**
Name : **الله ; منتدى ; قرآن ; صلى ; منتدي ; سلم ; إسلام ; تجديد ; وسلم**
Size : **62**

Name	Support	Complete name
الله	0.292	/NOUN_PROP/**الله**
الله	0.239	/BNP/**الله**
منتدى	0.234	/NOUN/**منتدى**

Figure 3: Text clustering.

5.4 Weapons detection

The direction of algorithm implementation will follow the aim to support any intelligence activity. Keeping the Al Aqsa TV video as reference it is worthy to find the smoke source or investigate the presence of objects-weapons within the video source. Main limitations are based on real presence on video of the object to detect and noise due to overlapped features extraction in outdoor scenario.

5.5 Biometric: face detection with SRI (super resolution-imaging)

Techniques of Super resolution photographs are techniques that increase the resolution of an imaging system.

There are two approaches to these techniques: the passing of the diffraction limit of optics system or the trivial increasing of the signal-noise digital sensor.

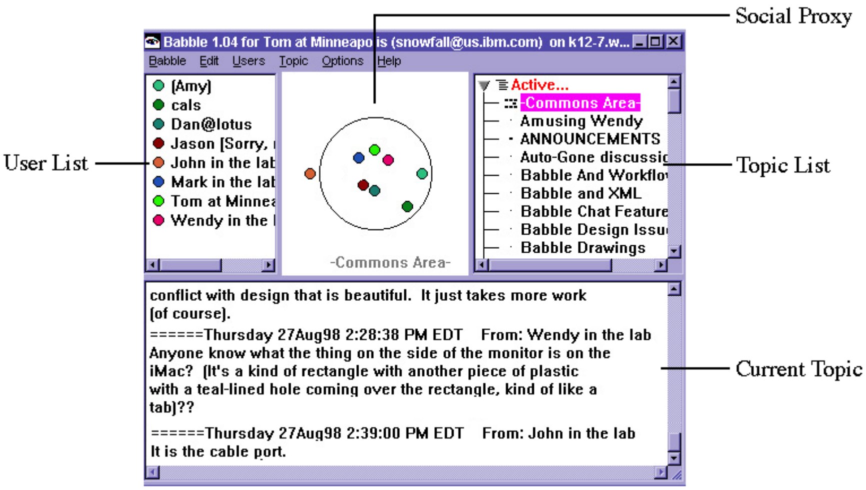
One way to get pictures to super-high resolution is to merge together multiple images captured from the same position in order to visibly reduce the amount of digital noise introduced from the amplifier.

5.6 Monitoring of specific areas/sectors

In business there are several examples of successful text mining solutions applied to competitive intelligence [11]. E.g. Unilever text mined patents discovering that a competitor was planning new activities in Brazil (which really took place a year later).

Telecom Italia discovered that a competitor (NEC-Nippon Electric Company) was going to launch new services in multimedia.

Total (F) mined Factiva and Lexis-Nexis databases to detect geopolitical and technical information.



```
conflict with design that is beautiful.  It just takes more work
(of course).
======Thursday 27Aug98 2:28:38 PM EDT    From: Wendy in the lab
Anyone know what the thing on the side of the monitor is on the
iMac?  (It's a kind of rectangle with another piece of plastic
with a teal-lined hole coming over the rectangle, kind of like a
tab)??
======Thursday 27Aug98 2:39:00 PM EDT    From: John in the lab
It is the cable port.
```

Figure 4: Chat surveillance.

5.7 Chat lines, blogs and other open sources analysis

The first enemy of intelligence activity is the “avalanche” of information that daily the analysts must retrieve, read, filter and summarize. The Al Qaeda terrorists declared to interact among them through chat lines to avoid being intercepted [15]: interception and analysis of chat lines content is anyway possible and frequently done in commercial situations [16].

Using different text mining techniques it is possible to identify the context of the communication and the relationships among documents detecting the references to the interesting topics, how they are treated and what impression they create in the reader. The coupling of text and video mining applied to intelligence issues directed against the growing terrorist activity on the web [17] is a new weapon in the hands of law enforcement agents.

Text mining is giving an important help in detection of social network hidden inside large volumes of text also detecting the simultaneous appearance of entities (names, events and concepts) measuring their distance (*proximity*).

6 European funded research

Today many threats to security are stateless in origin and transnational in scope. Terrorist groups have cells in multiple countries without the active support of any government but still capable of committing attacks with global impact. Potentially crippling attacks on the power grid or financial institutions could come from a computer anywhere in the world. Fighting elusive and transnational enemies requires international cooperation [18]. Technology has a central role in assuring protection of citizens: technology alone can't assure security but security without technology is not possible [19].

So an important aspect of fighting netwar terrorism is assuring international cooperation in developing new ideas and prototypes directed to protect populations against attacks.

European Union, through the action of European Commission, since 2005, with the inception of ESRAB and then of ESRIF and with the funding assured through 7FP and other initiatives, has been active in warranting this cooperation among its academic and private scientists and researchers.

6.1 ESRAB

One of the actions that the European Commission took was the creation, in 2005, of a 'European Security Research Advisory Board' (ESRAB) [19]. The Board included 50 high level strategists, nominated 'ad personam', from a broad spectrum of stakeholder groups including public and private users, industry, the European Defence Agency and research establishments.

ESRAB made recommendations to the Commission in defining the strategic missions, focus areas and priorities setting for security research programme and in defining the technological capabilities to be put in place among the European stakeholders, recommending a strategy to improve the European industry's technological base, so as to improve its competitivity.

One of its results was the definition of Security theme in 7FP.

6.2 7FP

The Seventh Framework Programme for research and technological development (7FP) is the European Union´s chief instrument for funding (through the mecanism of “Call for proposals”) research over the period 2007 to 2013 where a specific line dedicated to Security theme was launched for the 1st time in 2007. Security Research amounts to a total of about € 3 billion (including various EU funding lines).

The objective of the Security theme is to develop technologies to ensure the security from threats such as terrorism and (organised) crime, ensuring optimal and concerted use of available and evolving technologies to the benefit of civil European security and stimulating the cooperation of providers and users for civil security solutions and improving the competitiveness of the European security industry and delivering mission-oriented results to reduce security gaps.

New intelligence technologies (e.g. related to text and video mining) are expected to be developed principally for civil protection, bio-security, protection against crime and terrorism and to warrant intelligent surveillance and border security.

6.3 ESRIF

ESRIF stands for the "European Security Research and Innovation Forum" [20]. It is a European strategy group in the civil security research domain that was established in September 2007. Its main objective is to develop a mid and long term strategy for civil security research and innovation through public private dialogue by 2009.

ESRIF was set up and is supported by the EU Member and Associate States and the European Commission together. Its 64 members (including the author) represent four different interest groups ("stakeholders"):

- The security technology / solution demand side (Authorities and end users in charge of civil security from the 27 EU Member States). – Technology / solution supply side (Representatives of industry, research establishments and academia).
- Civil society representatives (Think-tanks, civil liberty organisations and other relevant experts).
- The European representatives (from European Parliament, European agencies as Europol, EDA, Frontex and from European Commission).

The main objective of ESRIF is the development of a mid and long term **Joint Security Research and Innovation Agenda** that will link security research with security policy making and its implementation.

It should create opportunities for more coherent research programming and funding that should lead to better innovation. It should also trigger the investment of funds by the private sector in research strategic priorities, thereby complementing public investments. Moreover, it corresponds to the general aim of building a true European Research Area, notably by promoting greater coherence between investments in research and development allocated at European, national and regional levels.

7 Conclusions

In this paper it has been shown that, although the current security threats are augmenting in volume and dangers, the possibilities of contrasting and preventing them and of protecting ourselves and our citizens are augmenting quicker thanks to information new technologies as text and video mining. Also European Commission, aware of that, has decided of investing huge resources in funding their developments. Special interest is growing especially in "exotic" (Arabic, Chinese, Japanese, Korean) language written communications analysis and in web video detection, retrieval and analysis (which are the areas of research of the authors).

References

[1] Lisse W., The Economics of Information and the Internet*, Competitive Intelligence Review*, Vol.9 (4), 1998.
[2] Treverton G.F., *Reshaping National Intelligence in an Age of Information,* Cambridge University Press, 2001.
[3] Ronfeldt, D., Arquilla, J., The *Advent of Netwar* –Rand Corporation, 1996
[4] Riedel, B., *– Al Qaeda Strikes Back –* Foreign Affairs, May/June 2007
[5] Kohlmann, E.- *The Real Online Terrorist Threat* – Foreign Affairs, Sept/Oct.2006
[6] Mueller, J., *– Is There Still a Terrorist Threat? –* Foreign Affairs, Sept/Oct 2006
[7] Cabena, P., .Zanasi, A., 1998. Discovering Data Mining. Prentice Hall
[8] Zanasi, A., (editor) *– Text Mining and its Applications to Intelligence, CRM and Knowledge Management –* WIT Press: Southampton, Boston, 2007.
[9] Rosenfeld, A., et al., *Video Mining,* Kluwer Academic Publishers, 2003.
[10] Zanasi A, Email, chatlines, newsgroups: a continuous opinion surveys source thanks to text mining. *Excellence in Int'l Research 2003 –* ESOMAR (Nl), 2003.
[11] Zanasi A., Competitive Intelligence Thru Data Mining Public Sources – *Competitive Intelligence Review,* Vol.9(1), John Wiley & Sons, Inc., 1998.
[12] Zanasi, A., *New forms of war, new forms of Intelligence: Text Mining –* ITNS Conference, Riyadh 2007.
[13] Steinberg, J., – in *Protecting the Homeland 2006/2007* – The Brookings Institution, 2006
[14] Rheingold, H., *The Virtual Community –* MIT Press, 2000.
[15] The Other War, The Economist March 8th Pag.26, 2003.
[16] Campbell, D., – *World under Watch, Interception Capabilities in the 21st Century* – ZDNet.co, 2001 (updated version of *Interception Capabilities 2000, A report to European Parliament* – 1999)
[17] Weimann, G., *Terror on the Internet,* US Institute of Peace Press, Washington, 2006
[18] Chertoff, M., *The Responsibility to Contain* -Foreign Affairs, Jan/Feb 2009

[19] Meeting the Challenge-The European Security Research Agenda – Luxembourg: Office for Official Publications of the European Communities, 2006

[20] European security research and innovation in support of European security policies: Report – Luxembourg: Office for Official Publications of the European Communities-2008