Open Access
Global Journal of Forensic Science & Medicine
Iris Publishers

Review Article

Forensics Usage of Video-Surveillance and Associated (Meta) Data

Franck Jeveme Panta, Jean François Sulzer and Florence Sedes*

Department of Forensic, France

***Corresponding author:** Florence Sedes, Department of Forensic, University of Toulouse III-Paul Sabatier, France.

Received Date: November 23, 2018
Published Date: December 10, 2018

Abstract

Forensic video analysis is the offline analysis of video aimed at finding video or digital evidence during an investigation. In order to find video evidence during an investigation (terrorism, kidnapping, homicide, ...), investigators need to analyze and watch large amounts of video data (equivalent to a high number of video hours). Despite the powerful existing techniques and algorithms for video processing, investigators are still facing many problems including the large volume of video data and time consuming. The correct interpreta-tion of videos requires a set of accurate miscellaneous data called the metadata. In this paper, we focus on the contribution that can come from the correlation between video surveillance, metadata and context infor-mation. Such a contribution can be demonstrated at the end of the projects we are currently working on in collaboration with the police services.

Keywords: Video-surveillance; Video evidence; (Meta)data

Abbreviations: CCTV: Closed-circuit television

Introduction

IP-based, SOA, IOT, IA, deep learning, etc. are today among the key buzzwords, which are supposed to radical-ly alter the business model of a number of sectors; in fact, they describe technologies and practices which are now in operational service for over a decade in video-surveillance (and other surveillance) applications! Accordingly, they already impact directly the forensic investigations which rely on such resources. The pre-sent article, concentrating on the IT-based investigations (excluding the cyber domain and the regulatory aspects), will focus on the relevance of metadata, contextual information and social media in an environment where video needs to be enriched in order to find video evidence during an investigation. Furthermore, espe-cially in dense/urban environments, the different spaces belong to many different organizations; each of them has made a risk assessment and has derived thereof security measures based on a variety of implementations (and vendors). Concretely, if a security incident happens in a city center at Christmas time, in a com-mercial mall or in a large station, there is a high probability that technical investigations call resources from up to half-a-dozen of independent systems, which have never been designed to interoperate. In this way, [1] presented analytical tools and initiatives for standardization with the aim of assisting the users of large-scale video surveillance systems and police forces for the purposes of a posteriori investigation. Even within a same system, legacy or need for video live monitoring may lead to significant discrepancies between the modes of communication and types of cameras, with the frequent situation of a Pan, Tilt and Zoom (PTZ) camera perfectly located near the scene, but looking in another direction...

More generally these lacks mentioned above show that collecting the videos themselves is not enough and that their proper interpretation requires a set of accurate miscellaneous data, called the metadata, which, as it will be detailed hereafter play a key role.

The Metadata and their Crucial Role

"Metadata" is a very generic term which defines support data, complementary to « data of interest » and that are provided to help in the interpretation or exploitation of the « data of interest ».

It is easily understandable that in video-surveillance systems, which carry a huge volume of information collected in varied conditions over a long period of time, metadata play a key role. As video-surveillance systems do not remain isolated and must share information with different systems (within a same organiza-tion or not), common understanding is crucial. Furthermore, metadata associated to the « data of interest » can be enriched at any time in their life cycle.

What makes video unique, is the fact that it is often not enough to attach the metadata to a file name; some metadata must be synchronized with the content and are then called "dynamic metadata"; as an example, absolute (and accurate) time of capture is the most generic one.

In fact, and more generally, the video-surveillance metadata divide into:

a. Descriptive: fixed data describing a camera, its installation and set-up, its location and orientation, etc. does not change over the time.

b. Dynamic "implicit": data associated to one or more videos, permanently produced and potentially changing over the time, like

- Relative to geo-location (GPS, orientation, PTZ, position between two stations, etc.)
- Events, alarms and miscellaneous sensors

c. Analytics results: products of analytics algorithms, mainly detections and characterizations, associ-ated to an estimated reliability level

➢ The process may be permanent with a fixed set-up and behave like dynamic implicit metadata

➢ The process can be activated or set-up on-demand, applying live or on pre-recorded contents

d. Annotations and comments: generally, in free text.

Some common-sense rules apply:

1) Unless a system is very specific, it is recommended to collect all relevant metadata and conserve them as long as the "data of interest" are preserved (and not more)

2) In video, the amount of metadata is not a big issue, as they represent less than 1/1000 of the total volume!

3) When a set of data is exported to another system, this must be done with their associated metadata, to allow common understanding and further processing; this applies to clips extracted from a longer sequence

4) Metadata being descriptions and characteristics, all the stakeholders must agree on common data definitions, representations, units used, …; this is the rationale for standards and dictionaries

The metadata have in practice a dual life; they are used both as

A. Streams in association with the video (and audio) streams, for display (live or post event), clip ex-port, further analytics processing, etc.

B. Indexes in data bases, for query answering and search activities (which can be very unpredictable!)

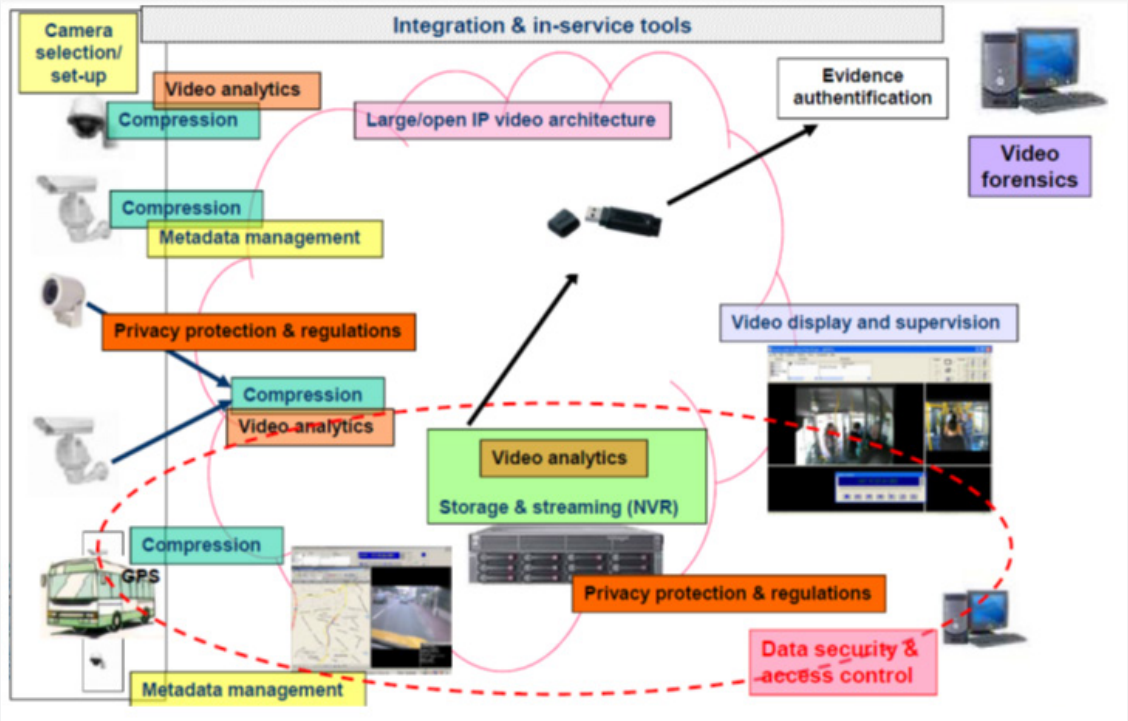

Figure 1: Generic functional block-diagram of a video-surveillance environment.

The two approaches normally cohabit consistently and a duplication (eventually with some filtering) is gen-erally the practical and future-proof approach. This applies to the different modes of use, as illustrated in Figure 1, i.e. inside a system or a set of subsystems, real-time or near-real-time, to prepare the content of export files, if required by police investigators and later on, when all the collected video evidence files are regrouped in a case-related data base.

In all cases a unique time reference (normally derived from GPS) is mandatory to allow correlations. It ap-pears from experience that only a small number of metadata types is of general usage (geo-location and events) and requires standardization, but

also that video-surveillance is only one of the resources usable in an investigation and that a correlation between context information (like interactions social media, devices-based geolocation, mobility information systems, open data, etc.) and video metadata data-base is often re-quired. Our recent researches address the collaboration between video-surveillance systems and spatio-temporal metadata [2,3,4,5].

Biometric Option

Many systems (sensors and applications) used for recognition, authentication and identification (Figure 2) are deployed on devices (e. g. smartphones) that are commonly used nowadays. Collecting data generated by these systems and integrating them with video-surveillance data can be helpful in an investigation. Let us remember that "Biometric data = Personal data".

Figure 2: Biometrics data.

Ethics and Privacy

Data collected from CCTV cameras and other information should comply with the legal and ethical rules defined by the law. The primary ethical issue invoked by surveillance activities in general is that of privacy.

Conclusion

In this paper, we present the utility of a correlation between video-surveillance, metadata (descriptive, dy-namic, analytics results, annotation and comments) and context information (social media, geo-location, mobility, open data) for the purpose of post-researching video evidence during an investigation. This correlation is being implemented in the different projects (project H2020 VICTORIA , ANR project FILTER2) we are currently working on with the police services. We also mentioned in this paper the biometrics opportunity while respecting the restrictions defined by law regarding the use of data.

Acknowledgement

None.

Conflict of Interest

No conflict of interest.

References

1. Florence Sèdes, Jean-François Sulzer, Denis Marraud, Christianne Mulat, Benjamin Cepas (2012) A Posteriori Analysis for Investigative Purposes. In: Jean-Yves Dufour (Eds.), Intelligent Video Surveillance Systems. Wiley, USA, 3: 33-46.
2. Dana Codreanu, André Péninou, Florence Sèdes (2015) Video spatio-temporal filtering based on cameras and target objects trajectories-Videosurveillance forensic framework. In: International Conference on Availability, Reliability and Security, Multimedia Forensic IEEE, Greece, pp. 611-617.
3. Dana Codreanu, Vincent Oria, André Péninou, Florence Sèdes (2016) Spatio-temporal metadata filtering and synchronising in video-surveillance. In : Ingénierie des Systèmes d'Information, France 21(3): 75-91.
4. Florence Sèdes, Franck Jeveme Panta (2017) (Meta-)Data Modelling : Gathering Spatio-Temporal Data for Indoor-Outdoor Queries. In: ACM SIGSPATIAL, ACM, Special issue Indoor Spatial Awareness 9(1): 35-42.
5. Franck Jeveme Panta, Geoffrey Roman Jimenez, Florence Sèdes (2018) Modeling metadata of CCTV systems and Indoor Location Sensors for automatic filtering of relevant video content. In: IEEE International Conference on Research Challenges in Information Science (RCIS), IEEE, Belgium, pp. 1-9.