by Fausto Galvan and Sebastiano Battiato

IMAGE/VIDEO FORENSICS: THEORETICAL BACKGROUND, METHODS AND BEST PRACTICES

Part three – Tools for operational scenarios

Fausto GALVAN is a Warrant Officer at Arma dei Carabinieri, where he has been working since 1991. He received his degree in Mathematics in 2002 and his PhD in Computer Science in 2016, both at the University of Udine. His research area is Image/Video Forensics. He co-authored more than a dozen publications for scientific journals and international conferences, chapters of books and national magazines. He has been a member of the scientific and organizer committee, and he gave speeches, in national and international seminars and conferences regarding Computer Forensics issues. At the present time he works at the Public Prosecutor's office at the Court of Udine.

Sebastiano BATTIATO is a full professor of Computer Science He is currently the Scientific Coordinator of the PhD Program in Computer Science at the University of Catania. He is involved in research and directorship of the IPLab research lab (http://iplab.dmi.unict.it). He coordinates IPLab's participation on large scale projects funded by national and international funding bodies, as well as by private companies. His research interests include Computer Vision, Imaging technology and Multimedia Forensics. He is Director (and Co-Founder) of the International Computer Vision Summer School (ICVSS), Sicily, Italy. He is the recipient of the 2017 PAMI Mark Everingham Prize for the series of annual ICVSS schools. In 2016 he founded iCTlab (www.ictlab.srl) a spin-off company working on the field of Digital Evidence.

From the beginning of this century, Image/Video Forensics experts faced the need to extract the largest number of information from a digital visual content, developing a plethora of methods and algorithms. These approaches, which may concern the authentication of images or videos, the identification of the device in which the visual data was originated, or the alterations to which the document has been subjected, find applications both in the civil and criminal context. In a series of three papers, we provide first an introductory part about the powerful impact of images and videos in today's reality, followed by a section where we highlight the differences between the analog and digital age in the formation of an image. Then we will define what is a digital evidence, and we will introduce Image/Video Forensics as a branch of the forensic sciences, highlighting its potential and limits. In the following, we will examine in detail some methods allowing to retrieve information from images when they are not readily available, and finally will provided a list of free and non-free software to face the daily challenges coming from processing images and videos for forensic purposes. The work ends with a list of publications containing the Best Practices in the field.

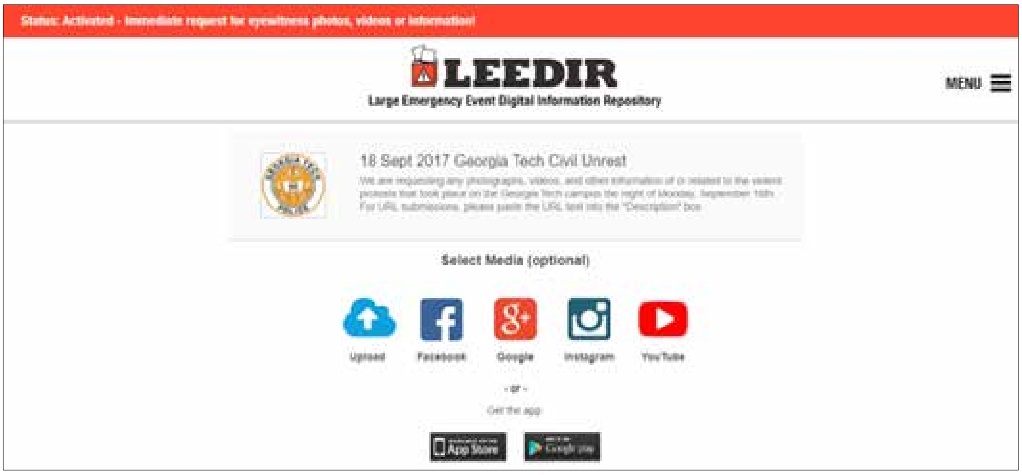
1. Unstoppable collection of multimedia data: not only a source of troubles

The state outlined in the two previous papers about Image/Video Forensics, does not seem to have a different address for the more general forensic area known as Multimedia Forensics (Battiato, Giudice and Paratore, 2016). On the contrary, in the future we will surely have more and more multimedia data to deal with (see Figure 1), collected by the different kind of sensors that will increasingly equip our devices.

At the same time, nowadays virtually every criminal behavior leaves behind digital clues, of whatever kind, in accordance with the Locard's Exchange Principle (Horswell and Fowler, 2004), which today is perhaps even more true than at the beginning of the 20th century. Consequently, the need to ascertain the originality of every sources of digital evidence in every investigation, forces law enforcements to face a huge amount of heterogeneous data, thus becoming an effort too wasteful in terms of time and human resources. The unstoppable advances in ICT technologies must be ridden in the right way, mostly by lawmakers. For this reason, police officers must have to be permanently in touch with the most up to date innovations in terms of software and hardware designed for digital forensics purposes. This is a big effort that could be difficult for a series of reasons, all of them connected with the increasing speed of technological innovations (Kurzweil, 2005).

Figure 1: in a not too distant future, shooting a picture or recording a scene with a video camera will mean collecting a huge amount of data. The ability to extract them from the acquisition devices and make them available for the forensic needs is a never-ending challenge for investigators, requiring constant research and updating. Image by https://blog.nikoneurope.com/en_GB/photography-2/the-future-of-imaging-part-1-contextualised-cameras/

These technical innovations, however, are not only a source of anxiety and worries, instead they bring with them also a lot of opportunities, that must be properly leveraged. As an example (see Fig.2), the american web platform LEEDIR (Large Emergency Event Digital Information Repository) is, as declared on https://www.leedir.com/, *a cloud based platform that can be* ***activated for FREE by law enforcement and relief agencies*** *during major emergency events to collect, manage, analyze and share virtually unlimited amounts of eyewitness photos, videos and text. When activated, (i) eyewitnesses can submit multimedia information via the LEEDIR mobile apps (iOS and Android) and the LEEDIR website and (ii) collaborating agencies can securely manage, analyze and share information rapidly. LEEDIR is built on expandable cloud server infrastructure in order to process massive amounts of data. This provides law enforcement agencies, relief agencies and eyewitnesses with an easy-to-use, end-to-end solution*.


Status: Activated - Immediate request for eyewitness photos, videos or information!

LEEDIR
Large Emergency Event Digital Information Repository

18 Sept 2017 Georgia Tech Civil Unrest
We are requesting any photographs, videos, and other information of or related to the violent protests that took place on the Georgia Tech campus the night of Monday, September 18th. For URL submissions, please paste the URL text into the "Description" box.

Select Media (optional)

Figure 2: LEEDIR web platform (http://www.leedir.com/) allows to any eyewitness to upload images and/or footages in case of events that happens in front of them and could be of some interest for law enforcement for any kind of reason. These media are then properly collected, fuse together and analyzed by Law Enforcement agencies, the only authority allowed to access them, which can consequently have a huge set of data useful for the purposes of investigations, or even just to plan an intervention as effectively as possible.

A similar approach, that is only an example of the use of new technologies for public safety purposes, would be highly desirable also for the European Law Enforcement Agencies, eventually enhanced with other similar emergency services.
In these set of three papers, after a theoretical introduction and a list of the main approaches in Image/Video Forensics, we think it may be useful giving a list of "tips and tricks" for the daily use. This because, in our personal experience, the majority of the police officers engaged in the daily investigations, rarely face problems like "reconstructing the 3D scene of a crime", whereas there are questions that more likely must be addressed on the fly, i.e. enhancing the number of a license plate of a car from an image, or extracting the "good" frame from a footage.

For this reason, we thought to insert a list of "how to", for the most important questions arising on an everyday scenario. The premise is that every solution can in general be achieved also by other approaches than the one provided here.

- **Extracting EXIF data from images or videos:** an image or a footage are not only bearers of visual messages, but also of a plethora of other useful information, especially for an investigation,. The ability to extract details as GPS coordinates, time and date of shooting, the brand, and (sometimes) the model of the device that took the image, and other interesting features, could sometimes determine the outcome of a trial.
  A good software for this purpose, in case of JPEG images or MPEG videos is *Irfanview* (https://www.impulseadventure.com/photo/jpeg-snoop.html).
- **Finding out if a given image has been taken from some source on the web**: sometimes, fake images, or part of them, are simply "copied and pasted" from a website. With the "Reverse Image Search" provided by Google (https://images.google.com/), is possible upload an image from a memory location, or give the URL of its location on the web, obtaining where is possible to find the same image on the web, if any.
- **Elimination of the *fisheye effect* from an image:** very often the footage or images coming from a cctv inside a bank, or from a surveillance system which has to cover large areas with a single camera, is affected by this distortion. The software v*lc* (https://www.videolan.org/vlc/index.it.html) includes a filter that allows its elimination.
- **Elimination of the effect of an interlaced video**: interlacing consists in the transmission of images by alternating their odd and even lines. Persistence of vision makes the eye perceiveing a continuous image. Although allowing an high level of band saving, it unavoidably leads to loosing quality in the video. Again, the free software *vlc* has got a function which allows to de-interlace the video sequence.
- **Extracting single frames from a video sequence:** sometimes this feature can be useful when we must decide the best frame to work with, i.e. to enhance a particular. A function provided by *Irfanview* allows extracting all frames by a footage, or part of them, saving them in a proper folder.
- **Rotation or cutting out of a video sequence**: Again, a functionality owned by *vlc*.
- **Extracting the audio track from a video**: As above, *vlc* offers this feature.
- **Cleaning an audio track**: One of the best free and open source software for this need is *Audacity* (https://www.audacityteam.org/). It allows enhancing the quality of an audio file affected by different source of noise, together with a lot of interesting function as cut and paste, volume increasing, ecc….
- **Enhance the general aspect of an image**: an huge list of filters for this purpose is given by *Irfanview.*
- **Authentication and forgery detection**: *Fotoforensics* (http://fotoforensics.com) by Hacker Factor, is a public, research-oriented web service that permits hands-on access to some digital photo analysis tools for free, but offers no privacy, since all uploaded content becomes part of a research archive. The same website provides also a more powerful commercial service, as described in the next Section.

At the end of this list of advices for operational approaches, all leveraging software that can be found for free on the web, we can't avoid to quit without mentioning the availability of commercial software for the forensic analysis of images and videos. The following is a non-exhaustive list of company, together with their software.

Amped Software (http://ampedsoftware.com/):

- *Amped Replay* is for investigators and frontline officers to conduct a first level analysis of their video evidence, with quick and easy conversion, enhancement and annotation functions.
- *Amped DVRConv* is for technicians tasked with converting a great number of surveillance videos in various proprietary formats, speeding up the triage in cases such as major investigations.
- *Amped FIVE* is for forensic lab experts to manage the complete image and video analysis workflow, with advanced and fully customizable processes for conversion, restoration, enhancement, measurement, presentation, and reporting, all in a single tool.
- *Amped Authenticate* is for digital forensic experts to exploit the data behind digital images, allowing the analysis of image integrity, authenticity, metadata, source and history, and detection of tampering prior to its use as intelligence and evidence.

Briefcam (https://www.briefcam.com/):

- *Synopsis* enables investigators to review hours of video in just minutes, and rapidly pinpoints people and objects of interest depending on their attributes (i.e. "a red car turning right", or "a man wearing a blue shirt on a bike"), thus avoiding to spend hours looking long parts of videos where nothing happens.

Kinesense (https://www.kinesense-vca.com):

- *KES* simplifies video processing with automatic search technology and template based workflows.
- LE enables time-efficient video retrieval, search and reporting from vast amounts of video evidence.

Hacker Factor (https://lab.fotoforensics.com/?show=tos):

- *FotoForensics Lab*: compared to its free version, it provides more analysis tools for evaluating digital pictures and more training materials. In addition, the content uploaded is not shared, not included in any research projects, and not added to the public archive.

2. *Best Practices*

At the end, according with the need of standardization belonging to every forensic science, we want to list the so-called "Best Practices" regarding the specific field of Image/Video Forensics, that represent the guidelines approved in the years by the scientific community:

- **ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidences** (https://www.iso.org/standard/44381.html).
- **ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidences** (https://www.iso.org/standard/44406.html).
- **ENFSI Best Practice Manual for the Forensic Examination of Digital Technology** (http://enfsi.eu/documents/best-practice-manuals/).
- **ENFSI Best Practice Manual for Facial Image Comparison** (http://enfsi.eu/documents/best-practice-manuals/).
- **ENFSI Best Practice Manual for Forensic Image and Video Enhancement** (http://enfsi.eu/documents/best-practice-manuals/).

3. *Conclusions*

In this set of three papers, we started showing some theoretical approaches to Image/Video Forensics, pointing out which are the precautions that a multimedia forensics expert must keep in mind in his analysis.

Then we briefly tried to define what does it means nowadays facing a "digital" evidence, in a forensic scenario where the ideas of "original" and "copy" are very different from the classical ones.

In this final paper, after exposing a possible use of multimedia data for public safety purposes, we proposed a list of free and commercial software used by multimedia forensics experts to acquire and analyze every kind of evidence content, together with a list of the Best Practices in the field. ©

REFERENCES

- ◊ Battiato, S., Giudice, O. and Paratore, A., 2016, June. Multimedia forensics: discovering the history of multimedia contents. In Proceedings of the 17th International Conference on Computer Systems and Technologies 2016 (pp. 5-16). ACM.
- ◊ Kurzweil, Ray. *The singularity is near: When humans transcend biology*. Penguin, 2005.
- ◊ Horswell, John, and Craig Fowler. "Associative evidence-the Locard exchange principle." *The Practice of Crime Scene Science, edited by Horswell, John* (2004): 45-56.