Abstract
Images and videos, which have always had a huge impact upon the way people perceive the world and form their convictions, are pervasive in today’s reality more than ever. Even in the forensics scenario, evidences are more and more often composed by multimedia in general and visual data in particular. Since the new meaning of “original data” in this digital world requires new approaches to ensure the admissibility of these elements as evidence in a trial, starting from the first years of this century the need to prove the authenticity of a digital evidence became crucial. This work introduces the sub area of Digital Forensics, which has the aim to define and develop the procedures devoted to help operators in this challenging research area. After an introductory part, the topic of this paper was introduced, starting from the meaning of digital evidence, and following with the definition of Image / Video Forensics as a branch of the forensic sciences. Then some methods allowing the extraction of significant information from the images when it is not readily available are examined in detail. Finally, a list of free and non-free software devoted to face the daily challenges coming from processing images and videos for forensic purposes is provided. The work ends with a list of publications containing the Best Practices in the field.

Keywords: Image/Video Forensics, Image/Video Tampering, Digital Forensics, Image Authentication
The impact of images in today’s reality

Nowadays our whole life is becoming increasingly more reliant upon images. Virtually all our visual memories are stored in real-time in our devices, on the cloud (often without even realizing it), and possibly shared through the web. The amount of multimedia data created each day on the Internet is massive and impressive. According to (Schultz, 2017), in 2017 more than 4 million hours of content have been uploaded to YouTube, with users watching 5.97 billion hours of YouTube videos, 200,000,000 photos have been uploaded on Facebook and 67,300,000 pictures have been posted on Instagram. This enormous pervasiveness of images has a lot of consequence in all aspects of our everyday life. If it is true that “a picture is worth a thousand words” (Brisbane, 1911), it is straightforward asking ourselves how many times we form our own conviction about an event, simply looking at the relative image or footage presented to us by the media. In most of the cases, simply there is no time to investigate if a visual information is true or false, so people often trust what sometimes is a fake. The danger in this behavior lies in the fact that once an opinion is rooted in this way is very hard to remove it (Nash et al., 2009; Sacchi et al., 2007). The lack of human ability to distinguish between tampered and original images (Schetinger et al., 2015), helps to increase the risk for humankind to be fooled by malicious agents. The overall feeling for the importance of the issues connected with the Integrity Verification in Multimedia is constantly increasing.

In the forensics scenario, a natural consequence of this pervasiveness of visual sources of what is called “liquid knowledge” is that, always more often, one (or more) image(s) or video(s) could become fundamental evidence in legal trials, and one of the main steps in the investigations is devoted to ascertain the originality of these evidence. In addition, like all the findings used as evidence, images and footage become valid and therefore admissible, only if they had been acquired, processed and stored according with the prescribed procedures. How can we trust an image or footage in a forensic environment? How can we be sure about the source from where they are supposed to come and, most of all, how can we prove that the visual content that we would like to validate as an evidence (possibly a primary one) has not been altered? To all these questions we will try to answer on the following pages.

Image tampering: from handmade retouches to deepfakes

Despite what one might imagine, the first documented examples of image manipulation (Figure 1) date back to 1860, only a few decades after the birth of photography (about 1830). Although the motivations of this photo-editing have never been clarified, it is thought that the reason of this first version of “cut-and-paste” forgery was the best physi-
cal appearance of the politician John Calhoun compared to the one of president Lincoln. From that episode, there had been thousands of cases in which more or less important images have undergone to substantial changes, most of them available on the famous website http://pth.iziru.com/.

Figure 1: On the left, the picture known as the first photographic counterfeiting (circa 1860), is obtained by combining the head of American president Abraham Lincoln with the body of the southern politician John Calhoun (right). Images from http://pth.iziru.com/.

In the first decades of 20th century, image tampering methods began to be classified and listed in papers and manuals, as the one showed in Figure 2 (Wardell, 1946), although this practice, from a technical point of view, remained virtually unaltered and limited to a small group of experts during all of the analogical era. This is a fundamental issue that needs to be highlighted, since nowadays, instead, the wide spread of acquisition devices (every smartphone embeds a camera, often provided with a powerful software suite able to modify the acquired images on the fly), and a huge number of manipulation software, often downloadable for free from the web, allow everyone to obtain unbelievable results in images manipulation. These instruments, and in general the different concept of “originality” that applies to digital and analogic worlds, heavily impact the reliability of a digital visual content when it is presented as an evidence in a trial.
During 2004 Presidential primaries, as Senator John Kerry was campaigning for the Democratic nomination, the image at the right of Figure 3 appeared, showing Kerry and Jane Fonda sharing a stage at an anti-war rally. Its caption was: "The actress and anti-war activist Jane Fonda speaks to a crowd of Vietnam as activist and former Vietnam vet John Kerry (LEFT) listens and prepares to speak next concerning the war in Vietnam (AP Photo)."

The picture was later determined to be a fake. Indeed, it was composed by a picture of Senator Kerry captured in June 1971, while he was preparing to give a speech at the Register for Peace Rally in Mineola, New York, and an image of Jane Fonda which has been shoot while she was speaking at a political rally in Miami Beach, Florida in August 1972. The aftermath on the campaign of the candidate Kerry were enormous.
In Figure 4 (left) is showed an image published in 2011 by the Saudi-owned English news website Al-Arabiya, under the headline “Russia refuses to recognize Libya rebels as legitimate government, clashing with West”. The fighter jets were digitally inserted as appears checking the original photo (by Marco Longari for AFP/Getty), that shows Libyan rebel fighters near a checkpoint on the outskirts of Ras Lanuf.

Figure 4: In the upper image showed at http://pth.zitru.com/2011_07_01.html we can see an image published in 2011 by the Saudi-owned English news website Al-Arabiya, under the headline “Russia refuses to recognize Libya rebels as legitimate government, clashing with West”. The fighter jets were digitally inserted as appears seeing the original photo below (by Marco Longari for AFP/Getty), that shows Libyan rebel fighters near a checkpoint on the outskirts of Ras Lanuf.

In a shocking TED speech titled Fake videos of real people — and how to spot them, in April 2018 Supasorn Suwajanakorn, an American expert of Computer Vision and AI, presented his work (Supasorn, Seitz & Kemelmacher-Shlizerman, 2017) about how producing an artificial video. They started from an audio track of the President Obama’s voice, a database of his previous footages, modeled the mouth shape at each instant, and composed it with proper 3D pose matching the input audio track. Their approach was then compared (see Figure 5) with the real video from where the audio was extracted, and the results were amazing.

What would have been the outcomes of John Kerry’s election campaign without the circulation of the manipulated image? Which are the social and geopolitical consequences among the Arab population when tampered images similar (or worst) to the one in the left side of Figure 4 appear? What would happen if a fake video of the president of the United States, artificially built with a Neural Network algorithm, nowadays known as deepfake (Verdoliva, 2020) would announce an unexpected change on the US economic policy? Nobody really knows the answers, but the underlying message is that, now more than ever, every image or video before being considered a witness of the real world, must undergo to an authenticity verification process. If this validation is required in a forensic scenario, the applied methods are known as Image/Video Forensics techniques. To these approaches, and to the related issues, is devoted the following of this paper.
Figure 5: A frame of the 2018 TED by Supasorn Suwajanakorn, where the researcher exposed a comparison between an original footage of a speech by Barak Obama, and its synthetic copy modeled with Artificial Intelligence approaches using the real audio track and a database of footages of president’s speeches. The mouth, face and body movements are reproduced and coordinated with the audio of a talk that really happened, but what about if these techniques were used to generate a fake footage where a politician pronounces some dangerous statements? Screenshot taken by the author from the TED video [https://www.youtube.com/watch?v=o2DDU4g0PRo](https://www.youtube.com/watch?v=o2DDU4g0PRo)

Image/Video Forensics as a part of the forensic sciences

A Forensic Science (often shortened to Forensics) is the practical application of science to matters of the law, and in particular the use of scientific methods for obtaining probative facts from the so called scientific evidences. These are defined as: evidences that are provided by some scientific-technical tool with the addition of specific technical skills, possibly with the intervention of an expert in the specific field (AA.VV., 2008).

One of the forensic sciences becoming more and more relevant nowadays is the one known as Digital Forensics. Its earliest notion came when the Federal Rules of evidence (US), first started to discuss digital evidence in the 1970s, even if real Digital Forensics investigations started in the mid-to-late 1980s, when federal agents had to start figuring out ways to search for digital evidence inside computers. This “home-grown” bottom-up approach continued until the late 1990s, when security researchers at universities and labs started to figure out that this problem was big enough to warrant investigation. First research groups started around 2000 or 2001. At present time, Digital Forensics includes many subareas, as exposed in Figure 6, and can be described in two different ways, with respect to different important aspects:
Image/Video Forensics: Theoretical background, operational approaches and best practices

• its purposes: the use of scientifically derived and proven methods towards preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (Beebe, 2009).

• the need of the intervention of an expert: the science of locating; extracting and analyzing types of data from different devices, which are interpreted by specialists in order to be used as legal evidence (Fenu & Solinas, 2013).

The emergence and rapid growth of Digital Forensics spawned the need to define the “new” entities that needed to be addressed. In accordance to the still defined “scientific evidences”, these entities took the name of digital evidences, defined as: digital data that can establish, or negate, that a crime has been committed and can provide a link between a crime and its victim, or between a crime and the perpetrator. From a practical point of view, a digital evidence is composed by a digital content, often stored in a file of whatever format or kind, and it is characterized by the following attributes:

• Volatility, such as residues of gunpowder. As an example, let us imagine the artifacts left by a chat with an Internet browser set on a private browsing mode: once the device is shutting down, that data are likely to disappear forever;

• Latency, such as fingerprints or a DNA evidence. This is the case of data that have been erased or hidden;

• Easy to modify or to spoil, since reliability of digital data are intrinsically fragile. Indeed, with a simple copy-paste operation is possible to modify the strength of a digital evidence.

As shown in Figure 6, one of the main subareas that compose the Digital Forensic universe is the one devoted to the analysis of images, also known as Image/Video Forensics, a forensic science carried out since the very first photos were made. We can find a formal definition of this set of approaches on the FBI website, where we can read that “Forensic Image Analysis is the application of image science and domain expertise to interpret the content of an image or the image itself in legal matters”. From this sentence it is possible to identify the main aspect that should characterize every forensic approach to the analysis of an image: it must be provided by someone both with adequate technical skills, able to extract from a digital file (or device) the requested information, and with a solid experience in the forensic environment, thus with such an approach that allows him/her to look at the digital data as digital evidences.

1 Definition proposed by Carrier in 2003 and slightly modified by the author of this paper.
Figure 6: An example of possible division of Digital Forensics in sub areas. It is very difficult to separate these components, since often they are closely connected. As an example, if we have to extract a chat session made using WhatsApp stored inside a smartphone (a Portable Devices Forensics’ issue), we surely must use Computer Forensics’s rules, adding some attentions related to the fact that information in that kind of device may changes during the analysis (if the cell phone is connected to the net). The extracted information is then examined according to DataBase Forensics.

Classification of Image/Video Forensics approaches

Since the variety of questions that could arise in a trial, or in the various steps of an investigation, facing Image/Forensics topics requires a wide experience in different areas of Computer Science. In the following, we give some examples of queries, preceded by the specific area of interest:

- **Image Enhancement**: Is it possible to improve the image/video quality in order to extract the license plate?
- **Image Authentication**: Did the images/videos undergo some alteration or are they authentic?
- **Camera Ballistic**: Can we state that an image/video come from a certain device?
- **Source Identification**: Do the images/videos come from a real scene, or are they artificially created using Computer Graphics (CG) methods?

The above argumentation, justifies a deeper insight into the categories that compose the entire Image Video/Forensics approaches. Among the various classifications in literature,
we decided to expose in the following one proposed by Redi, Taktak and Dugelay (Redi, Taktak and Dugelay, 2011), since widely accepted by the scientific community.

**Image Forgery Detection/Image Authentication.**

These methods include the various approaches that try to discover malicious modification in an image or a footage. This allows to highlight the physical, geometric, or statistical regularities (also named as patterns) that are inserted during the creation of a fake. Although Image Forgery Detection and Image Authentication can be viewed as two sides of the same coin, since if we found a forgery on a media, this can be claimed to be not original, the opposite it is absolutely not true and this fact has a huge impact in the forensic scenario. Indeed, even after the negative response given by all known methods, we cannot state that “*the image or video is authentic*”, but only that “*there are no visible traces of tampering*”.

The approaches can be classified according to several criteria. A first discrimination can be done with regards to the way the tampering is obtained:

- fake images created by using Computer Graphics (e.g. artificially generated/modified objects or details), or Machine Learning approaches (e.g. deep fake videos);

- alteration of the image semantics without modifying subjects or objects contained (e.g. color variations and/or brightness, resizing);

- alteration of the image semantics by the insertion (e.g., copying and pasting) or elimination (e.g. cropping or deleting) of significant parts.

A subclassification of this sets of methods (Farid, 2009; Piva, 2013), starting from the pipeline of all the steps that characterize the creation of a digital image inside a camera, takes into account and leverages the irregular patterns that a forgery leaves on the picture:

- **Pixel Based** methods, were we search for the artifacts appearing at the border of neighboring blocks as horizontal and vertical edges. In some cases, when an image is manipulated, these blocking artifacts, or correlations, may be altered;

- **Statistical Based** methods. Apart its semantic meaning, an image is basically an $n \times m$ table of values, from which many statistical properties can be inferred. Some of them have been proved to give useful insights in case of tampering;

- **Format Based** methods. The knowledge of the particular artifacts introduced in the image formation procedure of the lossy JPEG compression scheme, allows to distin-
guish between single or multiple compressed images and, in the latter case, understand if different parts of the image possess traces of different quality factors;

- **Camera Based** methods, that specifically model artifacts introduced by the various stages of the imaging process (i.e., lens, colour filter array, sensor);

- **Physics Based** methods, that leverage the inconsistencies in the estimated position of the source of light, obtained with proper mathematical models. Indeed, if the image is a copy-paste made with parts of different scenes, the source of light that illuminates the various objects will result with high probability as inconsistent;

- **Geometric Based** methods, aimed to find inconsistencies caused by the geometrical model that describes the formation of the image inside the camera.

### Source Camera Identification

The aim of this important group of approaches is the identification of the device (when its ID is available we can find the exact one, more often we can only identify its brand) that first shot the image. Sometimes the first step is devoted to discriminate between natural or artificial (also known as computer-generated) images. In general, the methodology switches to the identification of the source that generated the image, ascertaining the type of device (scanner, camera, copier, and printer) and then trying to determine the particular device.

### Image Reconstruction/Restoration/Enhancement

Restoration and improvement of quality of deteriorated images in order to identify, even partially, the original content and/or retrieve useful information (Gonzalez & Woods, 2002). About these issues, that represent very common needs in nowadays investigations, we want to highlight an important principle, even if the risk to seem too trivial is high: such methodologies of information retrieval can be used to extract the requested information only if this data is actually present in the examined footage or image. An example in this sense (unfortunately still very common) concerns images acquired by video surveillance devices. Indeed, in many cases, although able to record a criminal event, the footage is useless due to the poor quality of the images captured by the video camera: it is not possible to enhance an interesting detail, since the wanted data simply does not exist, and should not be artificially created.\(^2\)

---

\(^2\) Clear examples of what an Image/Video Forensics will not ever be able to do, is the so-called “CSI effect”: impossible zooms, 3D reconstructions without any scientific basis, and so on, well represented online by video as the one available at the URL: https://www.youtube.com/watch?v=Vxq9yj2pVWk. Due to the popularity of these fictions, the number of citizens and colleagues asking us to use the same “magic powers” is still very high. Even if, sometimes, a kind of miracle seems to be feasible, as exposed in Figure 8.
Steganalysis
Sometimes, information is hidden within an image with steganographic techniques, e.g., by changing the least significant bit in the binary number that defines the color of a pixel in a RGB representation, known as LSB approach (Battiato & Moltisanti, 2012). Steganalitical methods allow to understand if this kind of techniques was used, that is itself an important alert, and sometimes to recovery the covered data (Fridrich et al., 2002).

2D/3D Reconstruction and Comparison
The methods belonging to this group are devoted to bi/three-dimensional information extraction, to derive measures or reference values (e.g., the height of an individual) and for the comparison between images (e.g., to compare the identity of a subject with the known offender from a footage taken by a video surveillance system). Since this information can be very precious, although, surprisingly, the underlying theory comes from a century ago (the pinhole camera model), and even from before the Italian Renaissance (the principles of the perspective theory), two approaches belonging to this group are going to be exposed in some detail in the next Section.

Reconstruction of 2D and 3D scenes from images
Although every Image/Video Forensics approach leans on a strong theoretical back- ground, it is impossible to fully illustrate in this paper all the cited methods, together with the corresponding underlying theory. So, as anticipated at the end of the previous section, we made a choice, giving details on two situations often arising during an investigation. In the first one, the information is already present in the picture, even if not clearly visible, and can thus be derived. In the latter case is necessary to go back on the location where the image was shot. Both approaches have in common that it would be impossible to tackle them without knowledge of perspective and its applications to computer vision.

The classic Pinhole Camera model
According to (Criminisi, 2002) when a photo is taken, every $X$ point in the 3D world is pro- jected (mathematically, "mapped") in the two-dimensional plane of the image in a corre- sponding point $x$. The latter is the intersection of the image plane with the line segment that joins the optical center $O$ of the camera and the $X$ point of the shot scene (Figure 7). The algebraic interpretation of this projection is summarized by (1), where

$$x = PX \quad (1)$$
Figure 7: The formation of the image can be mathematically modeled as an operation that transports (maps) 3D real points into a 2D plane (the camera sensor) that matches the image. In red the position of the pinhole camera.

$P$ is a mathematical operator called “projection matrix”, a table whose coefficients define the rules for the transformation of the real points into image points. If we are able to know (or at least reconstruct in some way) the matrix $P$, we have the possibility of reversing this transformation. In other words, starting from a point on the image, we can determine its position within the real scene that the image reproduces. In practice, unfortunately, complete rebuilding the projection matrix might not always be possible.

Rectification of plates
Under certain conditions, or when it is possible to find information on the camera that shot the image (step known as Calibration) and/or some measures of the objects portrayed in the image, the number of unknowns needed to define the matrix is greatly reduced. An example of this, one of the most frequent questions made by colleagues, is the so-called Rectification: if we assume that a region that is first manually defined (corner points of the plate) in the left image is a planar rectangle, we “only” have to compute a 2D set of transformation parameters. In the example exposed in Figure 8 we see that is possible to transform the skewed object into a proper rectangle, thus being able to highlight the numbers of a car license plate.

Estimation of heights
With three-dimensional objects, if we need to estimate the height of a subject, it is necessary to first retrieve the real measurements of some other objects or elements present in the image (which can be recovered also afterwards). As an example, Law Enforcement operators could return to the place where the photo was taken to manually detect the measure of a door, a window, or part of a house.
Figure 8: Example of Rectification. It can be appreciated how, in case of planar surfaces, the perspective transformation highlights the information relative to the car license plate.

Otherwise, this information can be derived from appropriate documentation, if present. The second step to be taken consists in extracting from the image a series of characteristics known as vanishing points and lines (Figure 9). In the literature there are many algorithms allowing to estimate these geometric entities directly from the image, without knowing the intrinsic parameters (concerning the internal settings of the camera) or extrinsic ones (concerning the positioning of the camera relative to the scene) (Criminisi, 2002; Szeliski, 2010).

Figure 9: Estimating the size of a subject in an image or footage requires the calculation of vanishing points, horizontal and vertical. In the figure, the height of the person is obtained using a known dimension (the height of the column), the horizontal vanishing points ($p_1$ and $p_2$) and vertical points ($v$) as well as the vanishing line (or horizon line).
Searching for information in images, sometimes we can go far beyond the simple extrapolation of single measures, like heights of people or objects. Indeed, increasing the number of “real” measures detected, it is possible to extend the above methods up to reconstructing the entire 3D scene from which the image is taken, as well as the position of the camera at the time of shooting, an information that could be very useful in an investigation. An example of an implementation of the aforementioned theory is shown in Figure 10, where the height of the object in the background was used as reference dimension for estimating the height of the person in the image using Amped FIVE software.\(^3\)

We want to point out that, like all estimation methods, the processes described above are subject to errors that may derive from multiple sources: the incorrect collection of reference measurements, an incorrect set of pixels selected as a reference distance, an (even light) distortions of the image (e.g. lens distortion, blurred, poor definition), or if the subject is not perfectly in vertical position, etc. For this reason, the percentage of error must always be indicated together with the estimation of the requested data.

**Figure 10:** Example of estimation of the height of a person from a single image: on the left of the image the reference height of an object, that is necessary to take manually. Screenshot taken by the author from the web page of the commercial software Amped [https://ampedsoftware.com/it/five-samples](https://ampedsoftware.com/it/five-samples).

\(^3\) See [https://ampedsoftware.com/it/five-samples](https://ampedsoftware.com/it/five-samples).
Solutions to practical problems arising in the everyday scenario

After a theoretical introduction and a list of some approaches in Image/Video Forensics, and before the conclusions, we think it may be useful giving a list of “tips and tricks” for the daily use. This because, in our personal experience, investigators and police officers “on the battlefield” rarely face problems like “reconstruct the 3D scenes of a crime”, whereas, as an example, quickly determining a car’s plate, or extract “the good frame” from a footage, or enhance an image, are questions that are much more likely to be addressed. For this reason, we inserted the following list of “how to”, hoping to cover the most important questions arising in an everyday scenario. For every single goal to be achieved we suggest a free software, which, in our experience, can help to solve the problem. The premise is that, for every listed need, every given solution could in general be achieved by more than the suggestion provided here.4

• Extract EXIF data from an image: As already pointed out, an image or a video are not only bearers of a visual message, but also of a plethora of further useful information, especially for an investigation, stored in an image file saved in jpeg-format. The ability to extract details as GPS-coordinates, time and date of shooting, the (sometimes exact) model of the devices that took the image, and other interesting features, could sometimes determine the outcome of a trial. Jpegsnoop5 is a good software for this purpose.

• Find 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 some website. With the “Reverse Image Search” provided by Google6, it is possible to upload an image from a memory location, or giving the url of its location on the web, to locate, if any, the website(s) where to find the same image.

• Eliminate the fisheye effect from an image: Very often the footage or images coming from a CCTV-system inside a bank, or from a surveillance system which has to cover large areas with a single camera, are affected by this distortion. VLC7 includes a filter that allows to eliminate it.

• Eliminate the effect of an interlaced video: Interlacing consists in the transmission of images by alternating their odd and even lines, since persistence of vision makes the eye perceive the two fields as a continuous image. Although allowing an high

---

4 A more exhaustive list of software can be found at https://s-five.eu/Related_software_and_tools.htm and https://s-five.eu/Software_and_tools.htm.
5 https://www.impulseadventure.com/photo/jpegsnoop.html
6 (https://images.google.com/)
7 (https://www.videolan.org/vlc/index.it.html) includes a filter that allows to eliminate it.
level of band saving, it unavoidably leads to losing quality in the video. Again, the free software VLC incorporates a function which allows to de-interlace the video sequence.

- **Extract single frames from a video sequence:** Occasionally 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\(^8\) allows extracting all or part of the frame of a footage, saving them in a proper folder.

- **Rotate or cut a video sequence:** Again, a functionality owned by VLC.

- **Clean an audio track:** Sometimes this operation could be necessary after extracting the audio from a footage. The best free and open source software for this need is Audacity\(^9\). 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, and so on.

- **Extraction the audio track from a video:** As above, VLC offers this feature.

- **Enhance the general aspect of an image:** An enormous list of filters for this purpose is given by Irfanview.

There is of course, a variety of commercial software available for the purpose of forensic image and video analysis.

### Best Practices

Up to now we showed some theoretical approaches, practical methods, and software which in general allows to an expert acquiring more knowledge upon an image, a video and (even if only marginally) an audio file. In section entitled "Image/Video as a source of evidence", and in the subsequent, we briefly tried to define what does it means facing a “digital” evidence. We started to point out which are the precautions that an expert has to keep in mind in an investigation, which essentially come from the fact that, in the digital era the ideas of “original” and “copy” are very different from the classical ones. For this reason, together with the need of standardization belonging to the forensic world, the new approaches that the operational experience certifies as robust define the so-called

---

\(^8\) ([https://www.irfanview.com](https://www.irfanview.com))

\(^9\) ([https://www.audacityteam.org/](https://www.audacityteam.org/))
“Best Practices” in this challenging forensic science. Regarding the specific field we want to mention:


- All the Best Practices and guidelines from SWGIT/SWGDE site ([https://www.swgde.org](https://www.swgde.org)).

- All the Best Practices and guidelines from NIST/OSAC site devoted to Digital Forensics ([https://www.nist.gov/topics/digital-evidence](https://www.nist.gov/topics/digital-evidence)).

**Conclusions**

The use of images as a source of evidence, in police investigations and in general in a judicial proceeding, is a practice which dates back from the analog era and greatly increased with the advent of digital devices. At the same time, the ability to provide this type of documents without alterations that could compromise their usability in the process is increasingly put at risk by the diffusion on the market of devices and programs capable of altering the output of an acquisition device. Indeed, if about twenty years ago only a few people could manipulate images or videos, as this practice was reserved to few professionals with the necessary experience and equipment, today anyone connected to the web can access a huge number of tools and knowledge that allow him, in a short time and with few resources, to obtain results that are virtually indistinguishable from those of an expert. This situation endangers the success of many legal proceedings and, consequently, the need to develop, formalize and catalog the methods to contrast these malicious practices has become increasingly concrete and unavoidable. These approaches, born starting from the early years of this century, are known as Image/Video
Forensics methods and were the subject of this work. The provided overview, far from being exhaustive, should be used, in the author’s opinion, as a reference in this multidisciplinary science, whose knowledge, at least at a basic level, cannot be missing from the cultural background of a professional who works in the forensic environment, whether investigator, lawyer, judge or prosecutor. In the future we believe that researches in this field will lead to important steps forward, mainly in faces identification and recognition, as well as in the analysis of images and videos for fakes detection purposes.

This paper has been made possible by the fact that the author, in parallel with 3 decades of experience as a law enforcement agent, has had the good fortune to get in close contact with researchers from the academic world. This multiple experience, allows him to be aware that very often academia doesn’t know which are the need of law enforcement agencies, and at the same time law enforcement agencies don’t know what academia could be able to do for their needs. The increasing attention towards Multimedia Forensics, and in general to every IT approach to a real forensic scenario, requires to multiply efforts to finally reach a situation in which academia and law enforcement operators could talk each other more efficiently.

References


