Ground Truth – the missing link in digital/multimedia forensic science

by Jim Hoerricks

A survey of the research on digital/multimedia forensics (as it's generally known in the US) or digital visual media forensics (as it's described by Singh), will yield a treasure trove of techniques that address a single forgery/hoax type. (...) Following the publication history on this topic illustrates the fatal flaw; forgers create a new variant of a forgery and then scientists arrive at a valid detection method (hopefully). Society, and the courts, will always be one or more steps behind. In the age of so-called deep fakes, we are left to wonder if we can trust any type of multimedia. Thus, the path forward is not necessarily a new tool or technique, but a return to the fundamentals of jurisprudence. This path necessarily requires something that isn't always found or available in the retrieved evidence – *ground truth*. *Ground truth* means different things within different disciplines. As regards this paper, it can generally be thought to refer to "*information provided by direct observation (i.e. empirical evidence) as opposed to information provided by inference (Wikipedia, 2019).*"

Abstract

A problem of trust exists within society. Not long after technology is created to record events, nefarious actors emerge to create purposeful deceptions utilizing this new technology. Zhang (2012) describes the first ever hoax photo that was created in France in 1840. Tattersall & Névraumont catalog over 5,000 years of hoaxes in their 2018 book on the history of deception. As forgers and hoaxsters discover

new ways to create and disseminate their nefarious works, society is always one step behind in creating detection methods. In this paper, the author moves beyond detection methods and technological advances and suggests the answer to this problem lies not in science but in the law and in reason.

Introduction

In *The art and science of digital visual media forensics*, Singh (2018) succinctly documents the use of visual media to aid in the investigation of criminal activities throughout the last 150 years. She illustrates the current methods for contextual authentication of this vital evidence type utilizing active/passive and blind/non-blind techniques. The paper is well researched, and the sources are available to practitioners who may choose to replicate the featured techniques. Indeed, many of us have found the solution to novel technical problems in such research papers.

A survey of the research on digital/multimedia forensics (as it's generally known in the US) or digital visual media forensics (as it's described by Singh), will yield a treasure trove of techniques that address a single forgery/hoax type. Bianchi 2011, Das 2012, Decarlo 2012, Gironi 2014, Gupta 2012, Jing 2006, Johnson 2005, Kee 2011, Mondaini 2007, Pandey 2014, Shanableh 2013, Singh 2017, Wang 2007, 2009 all document specific techniques whilst Fontani 2011, 2013, Gloe 2007, Hu 2009, Schetinger 2017 illustrate frameworks that may guide an inquiry. Following the publication history on this topic illustrates the fatal flaw; forgers create a new variant of a forgery and then scientists arrive at a valid detection method (hopefully). Society, and the courts, will always be one or more steps behind. In the age of so-called deep fakes, we are left to wonder if we can trust any type of multimedia. Thus, the path forward is not necessarily a new tool or technique, but a return to the fundamentals of jurisprudence. This path necessarily requires something that isn't always found or available in the retrieved evidence – *ground truth*. *Ground truth* means different things within different disciplines. As regards this paper, it can generally be thought to refer to "*information provided by direct observation (i.e. empirical evidence) as opposed to information provided by inference (Wikipedia, 2019).*"

Ground truth becomes important as many practitioners do not realize that they're relying wholly upon information derived from inference - a guess or opinion that comes from the information that one has on hand (link). Further complicating the matter, in the best of cases, analysts often rely upon *abductive reasoning*, eliminating implausible explanations and retaining the most plausible explanations for the

(limited) available facts and traces, drawing analogies from past experience (Eco & Sebeok 1983, Lipton 2004), rather than engaging in actual experimental science. For those unfamiliar with the term, abductive reasoning can be thought of as *taking your best shot*. In the hierarchy of reasoning types, it's the lowest and least reliable. This is opposed to deductive reasoning where a conclusion is guaranteed, or inductive reasoning where a conclusion is merely likely. A lack of understanding of the *ground truth* of the case, or that they're simply taking their best shot, analysts may not realize just how far from science they've strayed. In the worst of cases, analysts rely upon supposition based in expediency, not science (Hak, 2019). In doing so, the course of justice is perverted by asking the accused to prove innocence against the weight of the prosecution's *claims*, in the absence of the analyst's affirmative ability to prove the investigation's theory of the case. Along the way, analysts trust in the collection methods used to obtain the evidence, especially when the analysts are not the ones who have actually collected the evidence. The analysts trust in their tools to deliver accurate and valid results, often without validating the tools generally or in their case specifically. Finally, the justice system, as a whole and around the world, trusts that the evidence that it receives is an accurate and valid depiction of the events under consideration. The issue thus becomes, *says who*? The answer to this question is part of our path forward.

Forensic Science Defined

In *A framework for harmonizing forensic science practices and digital/multimedia evidence*, the US-based Organization of Scientific Area Committees for Forensic Science (OSAC) notes *"[t]he value of forensic science as a whole is that it uses scientific reasoning and processes within the framework articulated in this document to address questions – specific to an event or a case – for legal contexts, to provide decision-makers with trustworthy understanding of the traces in order to help them make decisions. (OSAC, pg. iii)."* Further to the point, the authors place forensic science in context, *"[the above referenced document] proposes a broad definition of forensic science, not limited to legal problems in civil and criminal justice systems (courtroom contexts), and describes the different types of reasoning that play a significant role in forensic science. Then it defines five core forensic processes, seven forensic activities, and three operational techniques. The formalization of forensic science reasoning processes and outcomes in this work leads to increased reliability, repeatability, and validation in forensic results. This, in turn, gives decision-makers increased confidence in and*

understanding of forensic results. (pg. iii)." A broad definition of forensic science is then proposed by the authors: forensic science is "*the systematic and coherent study of traces to address questions of authentication, identification, classification, reconstruction, and evaluation for a legal context (OSAC, pg.1).*"

It is the *systematic and coherent study* that is often missing from inquiries, replaced instead with haste and expediency as well as fallacious appeals to authority. Let's examine what a *systematic and coherent study* of digital/multimedia evidence would look like when based in *ground truth*.

Ground Truth and the Retrieval of Evidence

When considering digital/multimedia data as evidence, there is always some contextual reason for its acquisition. The usual reason for retrieving or collecting such evidence involves the requested information either proving or disproving a theory of the case. In this sense, the preservation of the data is of vital importance. Guidance for a proper and thorough retrieval and preservation of the data has been available for decades. The UK's Police Scientific Development Branch (now the Home Office Scientific Development Branch - link) created numerous publications informing its consta-bularies and police services as to the proper procedures for such tasks (Blain, 1979). Likewise, in 2006, the US federal government sponsored the creation of the *Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems* (CTTSO, 2006) guidebook (*in terms of disclosure, I was a contributor to that effort, which included subject matter experts from US federal, state, and local agencies, as well as help from the UK*). Other countries have made similar efforts.

Since that time, these original documents have been refined and updated. The CTTSO guidebook is now working its way through the standards process at the ASTM. Other groups, like the US' Scientific Working Group on Digital Evidence (SWGDE), have produced guidance on this topic. In its guidance towards establishing the *ground truth* of retrieved evidence files, the *SWGDE Best Practices for Data Acquisition from Digital Video Recorders* (SWGDE, 2018) advises those conducting the retrieval to create a hash value for any video retrieved (SWGDE, pg. 12.). The hash of the storage container (in the case of *evidence seizure*) or the evidence files (in the case of *evidence retrieval*) establishes *ground truth* and provides a reference that can be utilized in any subsequent inquiries as to the integrity of the evidence.

According to Goodin (2020), "*a hash is a cryptographic fingerprint of a message, file, or other type of digital input that, like traditional fingerprints, looks unique. Also known as message digests, hashes play a vital role in ensuring that software updates, cryptographic keys, emails, and other types of messages are the authentic product of a specific person or entity, as opposed to a counterfeit input created by an adversary. These digital fingerprints come in the form of a fixed sequence of numbers and letters that are generated when the message is inputted into a hash algorithm or function*."

Accompanying the hash calculation in the integrity verification of the data is the person who retrieved the files. This person must attest, *under penalty of perjury*, that they are the one who performed the retrieval and generated the cryptographic hash. This attestation, along with the hash value, provides the *ground truth* of the evidence's provenance. It also puts a face to the data – someone who will lay the foundation for how the evidence happened to be entered into the system. Adding the jeopardy to the process, *the penalty of perjury,* ensures that the person that begins the chain of custody by entering the evidence into the system (*or anyone else who subsequently accesses the file*) understands the gravity of the situation, as well as the consequences for attempting to perpetrate a fraud on the process. From a quality assurance standpoint, this high level of accountability also helps to assure that only properly qualified staff are involved in the retrieval process, and that appropriate procedures are in place and followed.

Alongside the evidence files, once properly retrieved and accounted for, a separate data set is often needed. Consider a case involving the speed of a vehicle depicted in the recordings from a DVR. Did the recorder accurately record events? Was it in an error state at the time the evidence files were recorded? Did it drop frames during the creation of the evidence files? If so, does it always drop frames, rarely, or randomly? How does it handle motion, or lack of motion in uninvolved cameras? How do you, the analyst, know these things? You extract an appropriate sample of data from the DVR (or direct suitable staff to do so).

The calculation of the number of recordings needed for the task, the sample, should follow the acceptable rules within the statistical sciences. Often, as in the case of DVR performance, there are multiple variables to control. Thus, a sample size would be calculated relative to the variables as well as the eventual tests to be performed. In the case of speed as captured by a DVR, a sample size

calculation would look like Figure 1. At under 60 samples, you have more chances of being wrong than being right. In the world of the *abductive*, having a few samples or even a sample size of one becomes unfortunately acceptable. In relying upon previous results and eliminating the implausible, the analyst is left with the plausible (they think) – which is *accepted* (*not proven*) as fact. But, in such a case, the *ground truth* remains to be discovered – and may actually disprove the analyst's findings. In addition, the overreliance on abductive reasoning speaks to the problem of wrongful convictions, and the work of groups like the US-based Innocence Project.

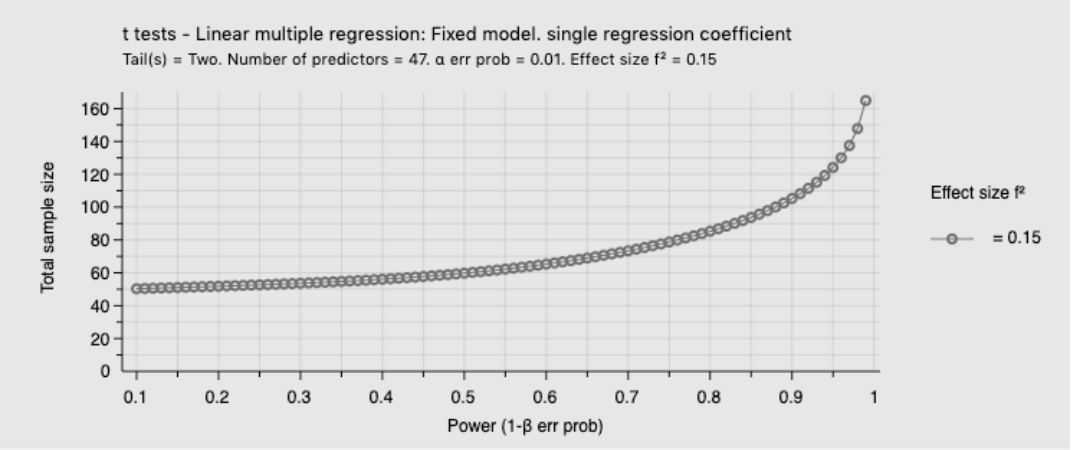

Figure 1 - Sample Size Calculation for Linear Multiple Regression

Ground Truth and the Analysis of Evidence

The US National Research Council's scathing report on the state of forensic science in the US, Strengthening Forensic Science in the United States: A Path Forward (2009), outlined some of the problems in the analysis of digital/multimedia evidence. "*Digital evidence has undergone a rapid maturation process. This discipline did not start in forensic laboratories. Instead, computers taken as evidence were studied by police officers and detectives who had some interest or expertise in computers. Over the past 10 years, this process has become more routine and subject to the rigors and expectations of other fields of forensic science. Three holdover challenges remain: (1) the digital evidence community does not have an agreed certification program or list of qualifications for digital forensic examiners; (2) some agencies still treat the examination of digital evidence as an investigative rather than a forensic activity; and (3) there is wide variability in and uncertainty about the education,*

experience, and training of those practicing this discipline." More than ten years later, these problems remain. These challenges are particularly relevant to the idea of establishing *ground truth*.

The analysis of DNA, for example, is a complex and costly process. Specific college programs and degree paths are oriented towards preparing the analyst for such a career. Accredited laboratories, recognizing the complexity of the task, insist upon a standard set of qualifications and entry skills for those that will work with this evidence type. The analysis of video evidence, on the other hand, does not generally follow the same protocol in requisite skills and hiring. Many agencies still consider the analysis of digital/multimedia evidence to be an investigative or intelligence gathering function, as opposed to an exercise in forensic science. An example of this can be found in my former agency's organizational map. My former unit, where the retrieval and analysis of multimedia evidence is typically performed, is not positioned in the Forensic Science Division, but in the Technical Investigation Division. The examination of digital evidence (e.g. computers) happens typically in the Commercial Crimes Division. I say typically because there are also more than a dozen units scattered throughout the Department responsible for the collection and analysis of digital/multimedia evidence related to specific crime types (e.g. Use of Force, Professional Standards, Major Crimes, etc.). But, again, none of these small units function within the auspices of the LAPD's accredited crime laboratory, with the majority of the analysts in these units coming from the commissioned peace officer ranks, not directly hired subject matter experts. All of this requires us to ask, are commissioned staff – steeped in the world of the abductive and biased towards a side and an outcome (Kincaid, 2015) – the appropriate staffing choice in establishing *ground truth*?

Having addressed, in brief, the problem of staffing and placement of analysis units within the government service, let's turn now to the problems presented by the tools that are on offer to the analyst.

For the analysis of digital/multimedia evidence, tools exist in two distinct classes – commercial off-the shelf (COTS)/free and open source software (FOSS), and purpose built tools. The COTS/FOSS tools are by far the most dominant in the marketplace. The problem with this, and the relation to *ground truth*, is that the tools on offer are generally repurposed from other industries. For example, when I entered into the discipline in 2001, there were only COTS/FOSS tools available. For some image restoration and

clarification tasks, Adobe's Photoshop (a product developed for photographers) was my tool of choice. But, as good as Photoshop is at clarifying the visual information in images and (now) videos, it's completely unfit for purpose in conducting a 3D photogrammetric analysis. Yet, there are cases today where Photoshop is still used for this purpose, often leading the analyst to the wrong conclusions.

Standing between COTS and FOSS is MATLAB. There is an initial cost to acquire and deploy the basic platform, but many image and video processing scripts can either be downloaded for free or created from work found in academic / scientific papers. This serves as a potential problem as the modifications might not be available to both sides of a case should the author choose to restrict distribution, as was a problem in a recent case in which I was involved. In US v Wells (2019, US District of Alaska), the government retained an academic to resolve an issue in the case. The academic utilized MATLAB to perform the work, but did not want to disclose the scripts used (or information about their methodology) to the court. This decision on the academic's part contributed to that work product not being utilized in the presentation of the case. In a much older case (People v Payton, 2010, Ventura County Superior Court), I was asked to authenticate an image from a bank's ATM. Utilizing MATLAB at the time, I presented a complete package to the process, including the documentation of my processing and custom scripts. The opposing counsel's objection to my use of MATLAB was sustained, as the judge accepted the argument that the cost of MATLAB was prohibitive to the defense. I then had to devise, test, and validate a solution utilizing FOSS tools. In that case, I used ImageJ with a set of plug-ins to accomplish the task.

On the FOSS side, tools like Fiji / ImageJ2 for images and VideoCleaner and R for images / videos offer analysts a no-cost way to work on files. The benefit of FOSS tools is the ability to modify them to suit one's needs. These tools share the same limitations as noted above when the developer of any customizations refuses to share or distribute their work product.

Modern tools for the analysis of video are mostly based upon FFMPEG (link), a collection of freeware tools from France. According to the developers, "*FFmpeg is the leading multimedia framework, able to decode, encode, transcode, mux, demux, stream, filter and play pretty much anything that humans and machines have created. It supports the most obscure ancient formats up to the cutting edge. No matter if they were designed by some standards committee, the community or a corporation* (FFMPEG,

2020)." It's an impressive statement, with one glaring omission as relates to *ground truth*; the word "accurately."

The two dominant vendors in the video analysis tool market, Input-ACE and Amped, SRL, both base their tools on FFMPEG, modifying FFMPEG and the associated libraries to suit their customers' needs. The problem with FFMPEG as it relates to *ground truth* can be seen in a blog post by Amped SRL's founder and CEO, writing about the purpose of FIVE's Change Framerate Filter, "*Sometimes it may happen that a video has a wrong frame rate set, either because of a problematic codec or a wrong capture. With the new filter Presentation > Change Frame Rate , the frame rate can be adjusted as needed, either from a set of standard values or by user submitted input* (Jerian, 2014)." Why would his tool not discover and present the *ground truth* of a video file's frame rate; such an important piece of information? How would the analyst know if the submitted evidence conforms to a standard value for frame rate given the analysis tools in FIVE? How would an analyst determine the appropriate, or *ground truth* frame rate? These questions are not meant to belittle or disparage Amped, SRL, its founder, or its tools (indeed, I am one of the US' original users of FIVE and continue to use it in my casework). The questions are meant to illustrate the need for a proper scientific workflow, as well as the need for sample sets of recordings from the DVR that generated the evidence under analysis. The range of values for frame rate can be determined from the sample data. Nevertheless, this filter's presence in the tool underscores the problem with modifying freeware that was not specifically designed to be used in the way it's currently being employed in support of science and justice.

In addition to employing FFMPEG, both Input-Ace and FIVE are able to work within the Windows video playback environment to utilize installed codecs for the processing of evidence files. Each has vendor relationships that allow their tools to process proprietary files without conversion or transcoding. Input-Ace, for example, can process Genetec's native file formats (Fredericks, 2019), whilst FIVE can process Milestone's (Jerian, 2013) and HIKVISION's (Spreadborough, 2017) native formats. But, as noted above with each tool's FFMPEG processing, the analyst is left with a choice of either trusting the results returned by the tool or attempting to arrive at *ground truth* via experimentation. Unfortunately, the former is more often true given the massive caseloads facing most agencies.

On the other side of the spectrum lies the purpose-built tools, like those from Pasadena, CA's Cognitech (link). Whilst Input-Ace and FIVE both employ modified versions of FFMPEG and associated libraries for processing video, the tools from Cognitech initially rely upon a video file's native codec for processing. This can present its own challenges, to be sure, but illustrates the point that getting to the *ground truth* of video evidence is partially dependent upon one's tool set – and one's validation of that set of tools relative to the evidence under examination – and partially dependent on an analyst being willing and able to perform valid experiments to arrive at *ground truth*.

As with retrieval, the presentation of results, findings, and/or conclusions to the court puts the analyst, their tools, and their procedures on the spot. Their work will be examined not only by the opposing side's analyst(s), but the greater community of analysts and attorneys. In commenting on a recent ruling in the US, *Melton v. Klee, 2019 WL 1315723, the United States District Court, Eastern District of Michigan, Southern Division*, Canadian attorney and blogger Jonathan Hak, observed of the analyst in the case, "*When the analyst himself states that the exercise is "not a scientifically accurate experiment," that is an indication that the opinion proffered is subjective in nature and perhaps ought not to have been given. Opinions offered by an expert should be objectively verifiable as that is a hallmark of scientific reliability. The further subjective opinion that someone trying to hide from the police would keep his face out of camera view has no place in forensic video analysis. Experts owe a singular critical duty to the court to assist in the discovery of the truth, even if doing so does not further the interests of their client. These issues understandably caused concern for the federal court and led to the rejection of the opinions tendered.*" Reporting on the court's findings, he quotes, "*The Court noted that no curriculum vitae or other evidence of the analyst's qualifications or expertise were provided to the Court. Allowing leeway on that point, the Court stated, "Even assuming [the analyst] is qualified as an expert in video analysis, the report is largely based on conjecture and speculation"* (Hak, 2019)." In other words, no legitimate attempt to arrive at the *ground truth* of the incident was offered in the case.

Conclusion

This article has been offered as an attempt to move away from tool reviews, feature sets, and explorations of new and novel techniques. As Singh (2018) has illustrated rather artfully, there are a plethora of those types of papers available in the marketplace. Given the diversity of legal systems and

the availability/affordability of tools across the world, I wanted to take a step back from the technological arms race to focus on a fundamental aspect of our work – the pursuit of *truth*.

American attorney and technology advocate Ralph Losey noted in 2013 that "*justice is based on truth, on what really happened. That is a basic problem in law because facts are usually contested. Each side has their own story. The truth is out there, but requires [a proper inquiry] to discover… Truth in the law means objective, reliable facts that may be admitted as evidence in a trial. The truth is out there, but requires [an effective] search to discover.*" The pursuit of truth, or the attempt to establish the *ground truth* of an event, is thus of vital importance in the cause of science and justice. A valid, reliable, and reproducible search for *ground truth* is absolutely necessary if we are to be engaged in forensic science - "*the systematic and coherent study of traces to address questions of authentication, identification, classification, reconstruction, and evaluation for a legal context (OSAC, pg.1).*"

Thank you.

References

1. Bianchi, T., & Piva, A. (2011). Detection of non-aligned double JPEG compression with estimation of PRIMARY Compression parameters. *2011 18th IEEE International Conference on Image Processing*. doi:10.1109/icip.2011.6115848

2. Blain J. (1979). Home office police scientific development branch. Journal of Physics E: Scientific Instruments, 12(7), 560-562. doi:10.1088/0022-3735/12/7/201

3. Bump, P. (2020). Analysis | How to spot a Photoshopped image, or, The Problem with the Internet. Retrieved from https://www.washingtonpost.com/politics/2020/01/07/how-spot-photoshopped-image-or-problem-with-internet/

4. CTTSO. (2006). Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems (DCCTV Guide) [PDF]. Washington, DC: Combating Terrorism Technical Support Office.

5. Das, S., Darsan, G., L, S., & Devan, D. (2012). Blind detection method for video inpainting forgery. *International Journal of Computer Applications, 60*(11), 33-37. doi:10.5120/9739-4290

6. Decarlo, & Metaxas, D. (1996). The integration of optical flow and deformable models with applications to human face shape and motion estimation. *Proceedings CVPR IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. doi:10.1109/cvpr.1996.517079

7. Eco U, Sebeok TA (1983) The Sign of Three: Dupin, Holmes, Peirce (Advances in Semiotics). Bloomington, IN: Indiana University Press

8. Faul, F., Erdfelder, E., Buchner, A., Lang, A. (2009). Statistical power analyses USING G*Power 3.1: Tests for correlation and regression analyses. Behavior Research Methods, 41(4), 1149-1160. doi: 10.3758/brm.41.4.1149

9. Faul, F., Erdfelder, E., Lang, A., Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. Behavior Research Methods, 39(2), 175-191. doi:10.3758/bf03193146

10. FFMPEG. (2020). About FFMPEG. Retrieved from https://www.ffmpeg.org/about.html

11. Fontani, M., Bianchi, T., Rosa, A. D., Piva, A., & Barni, M. (2011). A Dempster-Shafer framework for DECISION fusion in image forensics. *2011 IEEE International Workshop on Information Forensics and Security*. doi:10.1109/wifs.2011.6123156

12. Fontani, M., Bianchi, T., Rosa, A. D., Piva, A., & Barni, M. (2013). A framework for DECISION fusion in image Forensics based on Dempster–Shafer theory of evidence. *IEEE Transactions on Information Forensics and Security, 8*(4), 593-607. doi:10.1109/tifs.2013.2248727

13. Fredericks, A. (2019). ACE version 2.5 is here. Retrieved from https://input-ace.com/input-ace-version-2-5/

14. Gironi, Fontani, M., Bianchi, T., Piva, A., & Barni, M. (2014). A video forensic technique for detecting frame deletion and insertion. *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. doi:10.1109/icassp.2014.6854801

15. Gloe, T., Kirchner, M., Winkler, A., & Böhme, R. (2007). Can we trust digital image forensics? *Proceedings of the 15th International Conference on Multimedia - MULTIMEDIA '07*. doi: 10.1145/1291233.1291252

16.Goodin, D. (2020). PGP keys, software security, and much more threatened by new sha1 exploit. Retrieved from https://arstechnica-com.cdn.ampproject.org/c/s/arstechnica.com/information-technology/2020/01/pgp-keys-software-security-and-much-more-threatened-by-new-sha1-exploit/?amp=1

17.Gupta, S., Cho, S., & Kuo, C. J. (2012). Current developments and future trends in audio authentication. *IEEE Multimedia, 19*(1), 50-59. doi:10.1109/mmul.2011.74

18.Hak, J. (2019). Federal court Rejects evidence of forensic video analyst as Opinion "Largely based on conjecture And speculation". Retrieved January 09, 2020, from https://www.jonathanhak.com/2019/12/10/federal-court-rejects-evidence-of-forensic-video-analyst-as-opinion-largely-based-on-conjecture-and-speculation/

19.Hoerricks, J. (2008). Forensic Photoshop: A comprehensive imaging workflow for forensic professionals. San Francisco, CA: Blurb Publishing.

20.Hoerricks, J. (2019a). Evaluating research. Retrieved from https://forensicphotoshop.blogspot.com/2019/03/evaluating-research.html

21.Hoerricks, J. (2019b). Review: Forensic science. the importance of identity in theory and practice. Retrieved from https://forensicphotoshop.blogspot.com/2019/09/review-forensic-science-importance-of.html

22.Hoerricks, J. (2019c). First, do no harm. Retrieved from https://forensicphotoshop.blogspot.com/2019/08/first-do-no-harm.html

23.Hu, D., Wang, L., Zhou, Y., Zhou, Y., Jiang, X., & Ma, L. (2009). D-S evidence theory based digital image Trustworthiness evaluation model. *2009 International Conference on Multimedia Information Networking and Security*. doi:10.1109/mines.2009.154

24.Jerian, M. (2013). Amped milestone integration and photo authentication AT NATIA. Retrieved from http://blog.ampedsoftware.com/2013/04/14/amped-milestone-integration-and-photo-authentication-at-natia/

25. Jerian, M. (2014). Amped five Update: Annotations and frame rate adjustments. Retrieved from http://blog.ampedsoftware.com/2014/12/02/amped-five-update-annotations-and-frame-rate-adjustments/

26. Jing, W., & Hongbin, Z. (2006). Exposing digital forgeries by detecting traces of image splicing. *2006 8th International Conference on Signal Processing*. doi:10.1109/icosp.2006.345714

27. Johnson K., & Farid, H. (2005). Exposing digital forgeries by detecting inconsistencies in lighting. *Proceedings of the 7th Workshop on Multimedia and Security - MM&Sec '05*. doi: 10.1145/1073170.1073171

28. Kee, E., Johnson, M. K., & Farid, H. (2011). Digital image authentication from jpeg headers. *IEEE Transactions on Information Forensics and Security, 6*(3), 1066-1075. doi:10.1109/tifs.2011.2128309

29. Kincaid. (2015). The Sherlock Holmes conundrum, or the difference Between deductive and inductive reasoning. Retrieved from https://medium.com/@daniellekkincaid/the-sherlock-holmes-conundrum-or-the-difference-between-deductive-and-inductive-reasoning-ec1eb2686112

30. Lipton P (2004) Inference to the Best Explanation. (2nd edition). London: Routledge

31. LAPD. (2019). Los Angeles Police Department Organization Chart [PDF]. Los Angeles: Los Angeles Police Department.

32. Losey, R. (2013, April 05). There can be no justice without truth, and no truth without search. Retrieved from https://e-discoveryteam.com/2013/03/31/there-can-be-no-justice-without-truth-and-no-truth-without-search/

33. Mondaini, N., Caldelli, R., Piva, A., Barni, M., & Cappellini, V. (2007). Detection of malevolent changes in digital video for forensic applications. *Security, Steganography, and Watermarking of Multimedia Contents IX*. doi:10.1117/12.704924

34. National Research Council. (2009). Strengthening Forensic Science in the United States: A Path Forward. Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf

35.OSAC. (2019). A framework for harmonizing forensic Science practices and digital/multimedia evidence [PDF]. Gaithersburg: The Organization of Scientific Area Committees for Forensic Science, OSAC Task Group on Digital/Multimedia Science. http://dx.doi.org/10.29325/OSAC.TS.0002

36.Pandey, R. C., Singh, S. K., & Shukla, K. K. (2014). Passive copy-move forgery detection in videos. *2014 International Conference on Computer and Communication Technology (ICCCT)*. doi:10.1109/iccct.2014.7001509

37.Schetinger, V., Oliveira, M., Silva, R., & Carvalho, T. (2017, August 25). Humans are easily fooled by digital images. Retrieved January 08, 2020, from https://www.sciencedirect.com/science/article/abs/pii/S0097849317301450

38.Shanableh, T. (2013). Detection of frame deletion for digital video forensics. *Digital Investigation, 10*(4), 350-360. doi:10.1016/j.diin.2013.10.004

39.Singh D. (2018). The art and science of digital visual Media Forensics. Forensic, Legal & Investigative Sciences, 4, 1-6. doi:10.24966/flis-733x/100021

40.Singh, R. D., & Aggarwal, N. (2017). Detection and localization of copy-paste forgeries in digital videos. *Forensic Science International, 281*, 75-91. doi:10.1016/j.forsciint.2017.10.028

41.Singh, R. D., & Aggarwal, N. (2017). Detection of upscale-crop and splicing for digital video authentication. *Digital Investigation, 21*, 31-52. doi:10.1016/j.diin.2017.01.001

42.Singh, R. D., & Aggarwal, N. (2017). Optical flow and prediction residual based hybrid forensic system for inter-frame tampering detection. *Journal of Circuits, Systems and Computers, 26*(07), 1750107. doi:10.1142/s0218126617501079

43.Singh, R. D., & Aggarwal, N. (2017). Video content authentication techniques: A comprehensive survey. *Multimedia Systems, 24*(2), 211-240. doi:10.1007/s00530-017-0538-9

44.Spreadborough, D. (2017). Amped five Update 9223: New Hikvision Loader, new tool, new functions. Retrieved from http://blog.ampedsoftware.com/2017/05/15/amped-five-update-9223-new-hikvision-loader-new-tool-new-functions/

45.SWGDE. (2018). SWGDE Best Practices for Data Acquisition from Digital Video Recorders [PDF]. Washington, DC: Scientific Working Group on Digital Evidence.

46.Tattersall, I., Névraumont, P. N. (2018). Hoax a history of Deception: 5,000 years of fakes, forgeries, and fallacies. New York, NY: Black Dog & Leventhal.

47.Wang, W., & Farid, H. (2006). Exposing digital forgeries in video by detecting double mpeg compression. *Proceeding of the 8th Workshop on Multimedia and Security - MM&Sec '06*. doi: 10.1145/1161366.1161375

48.Wang, W., & Farid, H. (2007). Exposing digital forgeries IN interlaced and DEINTERLACED VIDEO. *IEEE Transactions on Information Forensics and Security, 2*(3), 438-449. doi:10.1109/tifs.2007.902661

49.Wang, W., & Farid, H. (2007). Exposing digital forgeries in video by detecting duplication. *Proceedings of the 9th Workshop on Multimedia & Security - MM&Sec '07*. doi: 10.1145/1288869.1288876

50.Wang, W., & Farid, H. (2009). Exposing digital forgeries in video by detecting double quantization. *Proceedings of the 11th ACM Workshop on Multimedia and Security - MM&Sec '09*. doi: 10.1145/1597817.1597826

51.Wikipedia. (2019, December 06). Ground truth. Retrieved from https://en.wikipedia.org/wiki/Ground_truth

52.Ying, C., & Yuping, W. (2008). Exposing digital forgeries by detecting traces of smoothing. *2008 The 9th International Conference for Young Computer Scientists*. doi:10.1109/icycs.2008.448

53.Zhang, M. (2012, November 16). The first hoax photograph ever shot. Retrieved January 08, 2020, from https://petapixel.com/2012/11/15/the-first-hoax-photograph-ever-shot/

About the Author

Jim Hoerricks, PhD AVFA, is a Certified Audio/Video Forensic Analyst (AVFA) in private practice, is the author of the best-selling book Forensic Photoshop (available on Amazon.com), is a co-author of Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems (DCCTV Guide), published by the Combating Terrorism Technical Support Office (CTTSO), is retired from police service where his unit (LAPD's Electronics Unit) was responsible for the collection and analysis of multimedia evidence (audio, video, images, and metadata from digital CCTV systems and mobile devices), and currently serves the Organization of Scientific Area Committees on Forensic Science (OSAC) as the Video/Image Technology and Analysis (VITAL), Video Task Group lead.