Forensic Science International 289 (2018) 268–269

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

Commentary

Digital forensics in a post-truth age

Hany Farid

Department of Computer Science, Dartmouth College, 6211 Sudikoff Lab, Hanover, NH 03755, United States

ARTICLE INFO

Article history:
Received 10 May 2018
Accepted 26 May 2018
Available online 6 June 2018

Nearly two decades ago, I was idly waiting in line at the library when I noticed an enormous book on a cart: The Federal Rules of Evidence. As I was thumbing through the book, I came across Rule 1001 of Article X Contents of Writing, Recordings, and Photographs, which outlined the rules under which photographic evidence can be introduced in a court of law. The rules seemed straightforward, until I read the definition of original:

> *An "original" of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, "original" means any printout – or other output readable by sight – if it accurately reflects the information. An "original" of a photograph includes the negative or a print from it.*

I was struck that the definition of "original" included such a vague statement as " . . . or other output readable by sight."

At the time, the Internet, digital cameras, and digital editing software were still primitive by today's standards. The trajectory, however, was fairly clear and it seemed to me that advances in the power and ubiquity of digital technology would eventually lead to complex issues of how we can trust digital media in a court of law.

This serendipitous event led me on a two-decade journey of developing techniques to authenticate digital content. These forensic techniques work in the absence of any type of digital watermark or signature. Instead, these techniques model the path of light through the entire image-creation process, and quantify physical, geometric, and statistical regularities in images that are disrupted by the creation of a fake.

During this time, I applied techniques in digital forensics to a wide range of criminal and civil proceedings, as well as occasionally helping law enforcement agencies, news organizations, and private citizens authenticate digital content. During this time, I considered the primary application of our academic field to be in the areas of criminal justice (the term forensics, after all, means "pertaining to, connected with, or used in courts of law.")

Today, however, the applications of digital forensics have shifted dramatically, as have the consequences of failing to quickly and reliably authenticate digital content.

The past few years have seen a startling and troubling rise in the fake-news phenomena in which everyone from individuals to state-sponsored entities produce and distribute mis-information which is then widely promoted and disseminated on social media. The implications of fake news range from a mis-informed public to an existential threat to democracy, and horrific violence.

All indications are that fake news is a serious threat to our society and democracy. We in the digital forensic community must continue to develop and refine techniques that will allow individuals, media outlets, and governments to quickly and accurately authenticate digital videos, images, and audios. This task has recently been made even more difficult by rapid advances in machine learning that have made it easier than ever to create sophisticated and compelling fakes. These technologies have removed many of the time and skill barriers previously required to create high-quality fakes. Not only can these automatic tools be used to create compelling fakes, they can be turned against our forensic techniques in the form of generative adversarial networks (GANs) that modify fake content to bypass forensic detection.

We as a scientific community face many challenges that require immediate and aggressive action. I outline below five calls to action to our scientific community and beyond.

1. **Funding**: The field of digital forensics is relatively new and therefore also relatively small. Our field needs to grow and this requires, at a minimum, more funding from government, foundation, and industry funders. The DARPA MediFor program, for example, is a model for how significant resources can bring together a large number of diverse academics to push our field forward. I encourage other agencies and organizations to support the field of digital forensics.

E-mail address: farid@dartmouth.edu (H. Farid).

https://doi.org/10.1016/j.forsciint.2018.05.047

2. **Scaling**: Forensic techniques that are validated again a dataset of a few hundred or thousand videos/images tend to break-down when evaluated against a dataset on the scale of hundreds of thousands. Similarly, techniques validated against a dataset of hundreds of thousands tend to break-down when evaluated against a dataset on the scale of millions, and so on. When developing forensic techniques, it is important to evaluate them against large (on the order of tens to hundreds of millions) and diverse datasets. This means that we as a community must develop and freely share our datasets to better ensure that the techniques we develop can be deployed, and be effective, at internet-scale.
3. **Balancing**: In the field of forensics, there has always been some tension between the goal of scientific openness and ensuring that our techniques are not easily circumvented. Today, this tension is only exasperated with the introduction of GANs which are being turned against our forensic techniques. Without necessarily advocating this as a solution for everyone, when students are not involved on a specific project, I have held back publication of new techniques for a year or so. This approach allows me to always have a few analyses that our adversaries are not aware of. We as a community will have to contemplate how best to balance the contradictory goals of scientific openness with that of fueling our adversaries.
4. **Responsibility**: The social media giants must take more responsibility for seeding and fueling the proliferation of fake news (look no further than the devastating violence in Myanmar and Sri Lanka which has been fueled by fake news stories and calls to violence on Facebook). This will entail a fundamental re-thinking of the perverse incentives of promoting sensational and controversial content because it simply engages users. We as a community and public should continue to pressure social media companies to rein in the abuses on their platforms.
5. **Legislating**: As countries around the world are wrestling with the serious and at times, deadly, consequences of fake news, many legislative bodies are contemplating legislation on how to contend with this phenomena. In Malaysia, for example, a new law would outlaw fake news and punish publishers of fake news with up to six years in prison and fines in the hundreds of thousands of dollars. We in the forensic community should engage with the public and with our legislators in helping them to understand the technical issues surrounding both the creation and detection of fake content. This will help to ensure that any proposed legislation is considered with an accurate understanding of the underlying technological issues.

While issues of digital authentication and verification have always been important, we have entered a new age in which the implications of digital fakery are impacting everything from our trust in news and democratic elections, to threatening the lives of our citizens. The responsibility for reining in these abuses falls on us as a scientific community, funding agencies, the social media giants, and legislative bodies. The past few years have given us a glimpse into the consequences of what happens when these issues are left unchecked and so it is with some urgency that we as a community and society should be addressing these pressing problems.