Don't be fooled by fake images and videos online

February 20 2019, by Hany Farid

Nope, not a real news report from Hurricane Irma. Credit: Snopes

One month before the 2016 U.S. presidential election, an "Access Hollywood" recording of Donald Trump was released in which he was heard lewdly talking about women. The then-candidate and his campaign apologized and dismissed the remarks as harmless.

At the time, the authenticity of the recording was never questioned. Just

two years later, the public finds itself in a dramatically different landscape in terms of believing what it sees and hears.

Advances in artificial intelligence have made it easier to create compelling and sophisticated fake images, videos and audio recordings. Meanwhile, misinformation proliferates on social media, and a polarized public may have become accustomed to being fed news that conforms to their worldview.

All contribute to a climate in which it is increasingly more difficult to believe what you see and hear online.

There are some things that you can do to protect yourself from falling for a hoax. As the author of the upcoming book "Fake Photos," to be published in August, I'd like to offer a few tips to protect yourself from falling for a hoax.

1. Check if the image has already been debunked

Many fake images are recirculated and have previously been debunked. A reverse image search is a simple and effective way to see how an image has previously been used.

Unlike a typical internet search in which keywords are specified, a reverse image search on Google or TinEye can search for the same or similar images in a vast database.

Reverse image search engines cannot exhaustively index the vastly expansive, ever-changing content on the internet. So, even if the image is on the internet, there is no guarantee that it will have been found by the site. In this regard, not finding an image doesn't mean it's real – or fake.

You can improve the likelihood of a match by cropping the image to

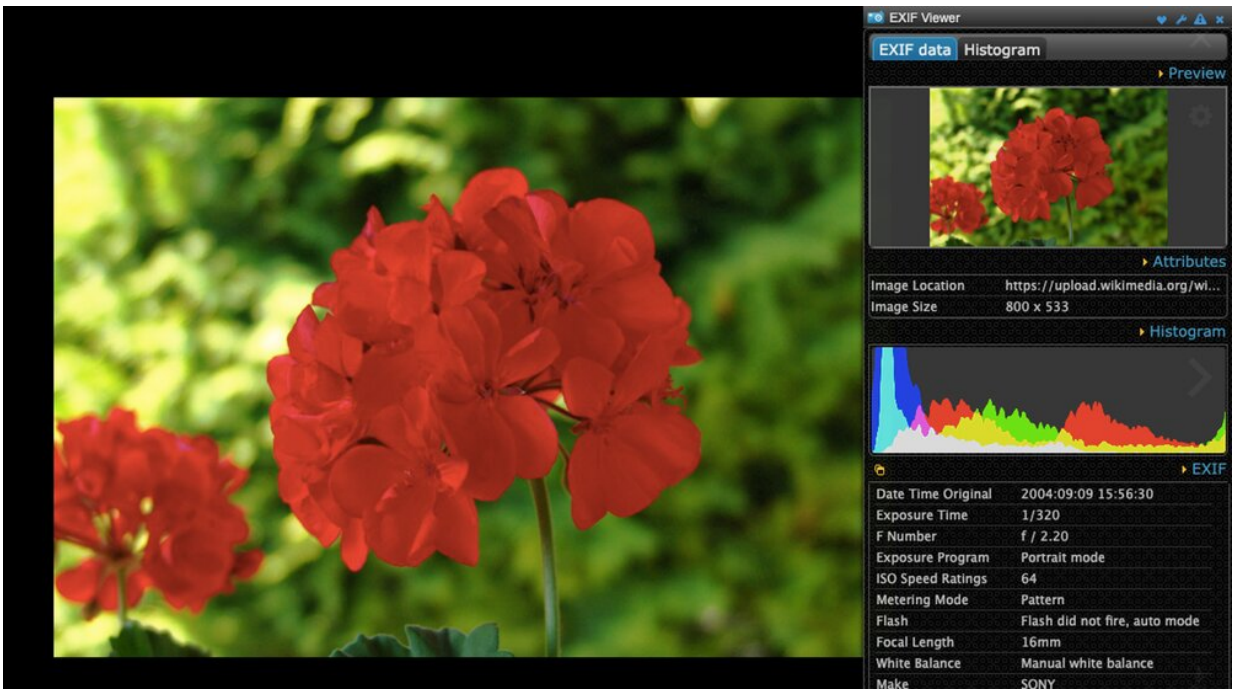
contain only the region of interest. Because this search requires you to upload images to a commercial site, take care when uploading any sensitive images.

2. Check the metadata

Digital images often contain rich metadata that can provide clues as to their provenance and authenticity.

Metadata is data about data. The metadata for a digital image includes the camera make and model; camera settings like aperture size and exposure time; the date and time when the image was captured; the GPS location where the image was captured; and much more.

The importance of the date, time and location tags is self-evident. Other tags may have a similarly straightforward interpretation. For example, photo-editing software may introduce a tag that identifies the software, or date and time tags that are inconsistent with other tags.



EXIF data offers clues about this photograph of a flower. Credit: Original image from Andreas Dobler/Wikimedia, CC BY-SA

Several tags provide information about camera settings. A gross inconsistency between the image properties implied by these settings and the actual properties of the image provides evidence that the image has been manipulated. For example, the exposure time and aperture size tags provide a qualitative measure of the light levels in the photographed scene. A short exposure time and small aperture suggest a scene with high light levels taken during the day, while a long exposure time and large aperture suggest a scene with low light levels taken at night or indoors.

The metadata is stored in the image file and can be readily extracted with various programs. However, some online services strip out much of an image's metadata, so the absence of metadata is not uncommon. When the metadata is intact, however, it can be highly informative.

3. Recognize what can and can't be faked

When assessing if an image or video is authentic, it is important to understand what is and what is not possible to fake.

For example, an image of two people standing shoulder to shoulder is relatively easy to create by splicing together two images. So is an image of a shark swimming next to a surfer. On the other hand, an image of two people embracing is harder to create, because the complex interaction is difficult to fake.

While modern artificial intelligence can produce highly compelling fakes – often called deepfakes – this is primarily restricted to changing the face and voice in a video, not the entire body. So it is possible to create a good fake of someone saying something that they never did, but not necessarily performing a physical act that they never did. This, however, will surely change in the coming years.

4. Beware of sharks

After more than two decades in digital forensics, I've come to the conclusion that viral images with sharks are almost always fake. Beware of spectacular shark photos.

5. Help fight misinformation

Fake images and videos have led to horrific violence around the globe, manipulation of democratic elections and civil unrest. The prevalence of misinformation also now allows anyone to cry "fake news" in response to any news story with which they disagree.

I believe that it's critical for the technology sector to make broad and deep changes to content moderation policies. The titans of tech can no longer ignore the direct and measurable harm that has come from the weaponization of their products.

What's more, those who are developing technology that can be used to easily create sophisticated fakes must think more carefully about how their technology can be abused and how to put some safeguards in place to prevent abuse. And, the digital forensic community must continue to develop tools to quickly and accurately detect fake images, videos and audio.

Lastly, everyone must change how they consume and spread content online. When reading stories online, be diligent and consider the source; the New York Evening (a fake news site) is not the same as The New York Times. Always be cautious of the wonderfully satirical stories from The Onion that often get mistaken for real news.

Check the date of each story. Many fake stories continue to recirculate years after their introduction, like a nasty virus that just won't die. Recognize that many headlines are designed to grab your attention – read beyond the headline to make sure that the story is what it appears to be. The news that you read on social media is algorithmically fed to you based on your prior consumption, creating an echo chamber that exposes you only to stories that conform to your existing views.

Finally, extraordinary claims require extraordinary evidence. Make every effort to fact-check stories with reliable secondary and tertiary sources, particularly before sharing.

Provided by The Conversation