FAKING IT

David Spreadborough *explains why it's time to get real about fake imagery*

On one of the few warm sunny weekends this summer, I quickly took some photos at a family barbeque on my smartphone. Nothing too notable about this, but a few seconds and several finger swipes later I could edit the images and upload the finished product to my social media pages, for the benefit of friends and family from afar.

It has never been easier to do this. With Photoshop celebrating its 27th birthday this year, digital image manipulation has reached prime access and user operability. This allows me to manipulate the image to the point where I can change the story behind the image. Just a click of a mouse could crop out who was at the barbeque, the colour of their clothes, or the level of daylight present. According to my pictures, anyone could have attended and whether they did so at midday or sunset would also be at my discretion.

Most people would consider it fair game to make a few small cosmetic changes to enhance the photo for admirers on social media. However, were I to submit this image as an alibi for my whereabouts in a serious investigation then it would be a completely different matter.

My friends and family who weren't physically there would, of course, take the photos to be a true and accurate representation of the scene and be none the wiser. We harbour an innate instinct to trust what we see, given that visual stimulus is our primary means of interacting and assessing the world. The old mantra of "seeing is believing" means that it's easy to see how even minor changes can tell an entirely different story about what took place.

As technology has enabled mainstream, widespread image manipulation, it is not surprising that there has been a huge increase in the number of tampered images, which find their way into a wide spectrum of industries and sectors. Incidents of doctored images frequently appear in mainstream media where they incite cries of fake news.

DIGITAL FABRICATION

For example, a photo at the G20 summit this year featured a photoshopped president Putin, giving the impression that he was colluding with president Donald Trump. The photo proceeded to spread online, instigating huge political ramifications from a digital fabrication, which would have taken several minutes to create on a laptop. Last August showed our vulnerability to tampered photos, with the circulation of a doctored image of a shark swimming up the freeway during hurricane Harvey in the US, indicating a larger problem with major international news outlets spreading the image as genuine.

With a little know how and basic software it is easy to doctor an image to suit your purposes

Equally there is significant evidence of Photoshopped images being used to support fraudulent scientific research internationally. Doctored experiment results and images continue to rock the research industry with every new fraudulent revelation. For example, a prominent cancer research scientist in Italy has been under investigation for using a photography studio to manipulate images that are pivotal to the crux of the "ground breaking" research he is carrying out. Indeed, the journal *Nature* has suggested that up to one in five scientific papers contain evidence of some sort of image manipulation.

It is clear, therefore, that when the stakes are high enough, people will manipulate the truth and unfortunately given our tendency to trust photographic images, it seems that it is currently worth their while to do so. When the stakes are as high as imprisonment, it is easy to see just how tempting it can be to manipulate an image to support a fake alibi or a particular version of events.

UNVERIFIED EVIDENCE

Unfortunately, security investigations are by no means immune to this phenomenon either. In fact, given the increase in the sources of digital images, the integrity of evidence in such investigations is at its all-time most vulnerable. Body-worn cameras, smartphones and increasingly sophisticated CCTV surveillance means that investigators are now dealing with a fast-growing pile of unverified evidence.

Over the 12 years I spent in the police service investigating images, I have also seen a sharp increase in the amount of scanned images, screen captures and manipulated CCTV stills being analysed. One thing that had not changed over this period, however, is my surprise at how easy it still is to enter an image into evidence procedures, and for that image to then be relied on for the purposes of the investigation with very little verification procedures.

Thankfully, modern image authentication software allows users to ascertain the likelihood of whether an image has been tampered with or not. Digital images – which at first seem authentic at face value – are betrayed by the meta-data associated found in the file. By analysing the meta-data of a photograph, we can carry out a digital autopsy of the image to investigate signs of manipulation undetectable to the naked eye.

Choosing the right software for your investigations is important. It is a given that the software must be able to detect manipulation and inconsistencies in meta-data. Additionally, it is also useful to be able to process thousands of images without issue, given the high quantity of photos involved in multiple investigations. It is also possible to use the meta-data to identify that a specific camera has taken a certain photo. Being able to identify a camera's unique meta-data signature and the ability to reverse image search online for other photos taken by the device is a feature that would greatly aid security investigations.

As security investigators, we run the risk of convicting the wrong person if analysis results are unreliable. Speaking to different investigators internationally, there is a recurrent theme in the back of their heads that somebody's liberty may be at stake. Misinterpreting evidence could leave a criminal free to commit more crimes or an innocent person to lose their liberty. It is, therefore, of paramount importance to emphasise adequate training in using image authentication software, and for these methods to be based on strict scientific principles.

The origins of meta-data image analysis required a deep understanding of coding and mathematics, due to the algorithms, which need to be applied manually. This expertise bottleneck simply was not sufficient to deal with the widespread access that people have to intuitive and accessible photo manipulation software.

It is also, therefore, important that the software itself is easy to use, and proficient training is given to enable investigators with no prior advanced software skills to learn how to authenticate images in a matter of days. Before the advent of digital technology, analogue images and evidence were subject to strict rules on how to handle them. However since then, due to the complexity of the digital imagery world, many more processing variables have been added to the intricacy of an investigation. The nature of digital imagery also means that updates to both forensic software and photo manipulation software come fast and frequently, and investigators should, therefore, have a strong grasp on the foundations in order to build their skill sets as the world changes around them. This means that the importance of training cannot be understated.

MANIPULATED DIGITAL IMAGES CAN BE BETRAYED BY THE META-DATA THAT'S FOUND IN THEIR FILE

IMPORTANCE OF TRAINING

As a forensic video trainer I have seen first hand the empowerment that digital forensic training can give to investigative professionals around the world. However the training is carried out, though, the software being used must be intuitive enough to teach in just a few days. The students must be at the point where those learning are able to confidently apply the techniques to real situations in their line of work. Given the challenge they are facing, logistically this is the most realistic chance we have to fight the epidemic of manipulated images.

The "see one, do one, teach one" methodology so often practised in medical schools and engineering institutions is often recommended for such workshops. A hands-on approach tends to work best, as it is much easier to learn when applied in practice. Thankfully and perhaps paradoxically, the ease of manipulating images means that there are always plenty of practical materials for students to try their new skills on.

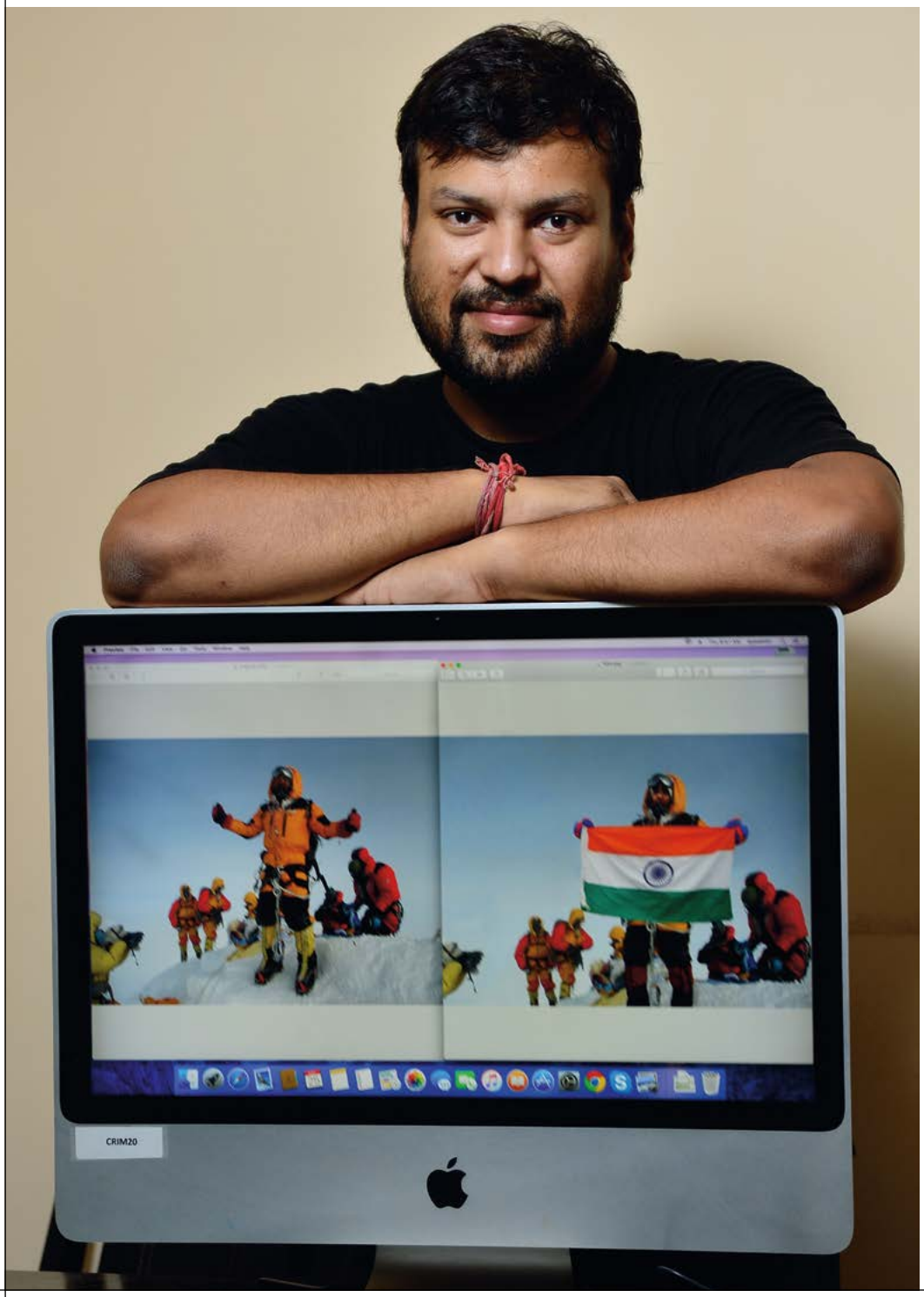
Training this way helps to build the muscle memory required to quickly authenticate digital

images at the speed required for complex investigations. Teaching this way also helps build the level of confidence necessary to testify for the results obtained, given the significant consequences of the nature of the investigation. At the end of the day, this line of work can significantly change someone's life, removing their liberty or in worse cases impose death penalty cases.

It is clear that image manipulation is a problem causing various issues in the world and security investigations are not invulnerable. The rise of digital imagery and imaging techniques means that proper software that can detect abnormalities in meta-data and proficient training is necessary in order to arm investigators with the tools and capacity required to address the issue. A mainstream uptake of this practice among security professionals although growing, is still is in its infancy. However with a newly gained scepticism of photographs – and an awareness of the significant consequences of ignorance – hopefully we can identify manipulated images and confine them to the realms of summer family barbeques ●

IMAGE SOFTWARE ALLOWS INVESTIGATORS TO SEE WHETHER AN IMAGE HAS BEEN TAMPERED WITH

David Spreadborough is Certified Forensic Video Analyst & International Trainer at Amped Software. He served as a UK police officer for 24 years and was the first LEVA-certified Forensic Video Analyst in Europe. He trains agencies worldwide on the use of Amped Software products.



Indian mountaineer Satyarup Siddhanta poses for a photograph alongside an image of himself on the summit of Mount Everest (L), and a doctored photograph of the same image used to make a fake claim of a summit

Picture credit: Getty