9. Sinitsyn, F. ‘Locky: the encryptor taking the world by storm’. SecureList, 6 Apr 2016. Accessed Sep 2017. https://securelist.com/locky-the-encryptor-taking-the-world-by-storm/74398/.
10. ‘Microsoft Security Bulletin MS17-010 – Critical Security Update for Microsoft Windows SMB Server (4013389)’. Microsoft, 14 Mar 2017. Accessed Sep 217. https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.
11. Cellan-Jones, R. ‘Ransomware and the NHS – the inquest begins’. BBC News, 15 May 2017. Accessed Sep 2017. www.bbc.co.uk/news/technology-39917278.
12. ‘Customer Guidance for WannaCrypt attacks’. Microsoft, 12 May 2017. Accessed Sep 2017. https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.
13. Goodin, D. ‘WannaCry ransomware spread widely because of Windows 7, not XP’. ArsTechnica UK, 22 May 2017. Accessed Sep 2017. https://arstechnica.co.uk/security/2017/05/windows-7-not-xp-was-the-reason-last-weeks-wcry-worm-spread-so-widely/.
14. ‘Ransomware: Latest NCSC Guidance’. National Cyber Security Centre, 13 May 2017. Accessed Sep 2017. https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance.
15. Newman, LH. ‘How an accidental ‘Kill Switch’ slowed Friday’s massive ransomware attack’. Wired.com, 13 May 2017. Accessed Sep 2017. www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.
16. ‘Schroedinger’s Pet(ya)’. Securelist, 27 Jun 2017. Accessed Sep 2017. https://securelist.com/schroedingers-petya/78870/.
17. ‘Ransomware’. Get Safe Online. Accessed Sep 2017. www.getsafeonline.org/protecting-yourself/ransomware/.
18. Lane, VP. ‘Security of computer based information systems’. Macmillan Education, 1985.

Exposing fraudulent digital images

David Spreadborough, Amped Software

David Spreadborough

As a predominantly visual species, we tend to believe what we see. Throughout human evolution, our primary sense of sight has allowed us to analyse primeval threats. We are genetically hardwired to process and trust what our eyes tell us. Edgar Dale’s cone of learning states that the brain retains information visually, over any other sensory stimulus.[1]

This innate hardwiring means that the arrival of digital images has posed a problem for the fraud investigation community. There are many different reasons why someone would want to maliciously alter a photo to ‘tell a different story’. Although photos can be manipulated with ease, many people still harbour a natural tendency to trust photos as a true and accurate representation of the scene in front of us.

This innate trust in photos is engrained across all industries. Imagine the difficulty you would face by sketching your version of a contract with a pencil in a legal dispute, or submitting a painting as proof of a previously lost item when making a claim with an insurance company.

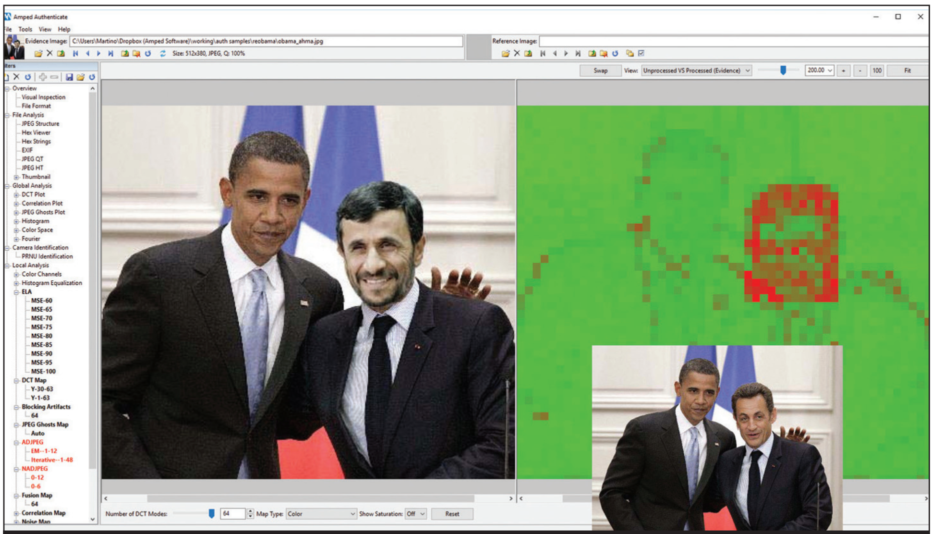
Digital manipulation

While this may sound a little extreme, photo manipulation techniques date back to the 19th century, almost as long as the history of photography itself. Modern digital manipulation tools have reached new levels of sophistication, with Photoshop now celebrating its 27th birthday. Such software can craft fantasies pixel by pixel, leaving the human eye none the wiser. Participants in a recent study could only spot irregularities in a doctored image 45% of the time.[2]

Even smartphone apps can alter images at the click of a button. Nowadays, children of primary school age can capture high-quality images, edit them and share with just a few finger swipes on their phones. It is easy to see how even minor changes can tell an entirely different story. For example, a quick rearrangement of words and letters on a document can change dates, statements and price quantities. Or the addition of just one face into a crowd scene creates an alibi out of thin air.

> ***“Until now, many people have trusted the photographic image as being a true and accurate representation. This is evident in the news and media, where scandals of tampered images being ‘fake news’ run rife”***

We cannot be so naive as to believe that fake images do not end up in fraud investigations. This is evident in the news and media, where scandals of



Evidence Image: C:\Users\Martino\Dropbox (Amped Software)\working\auth samples\reobama\obama_ahma.jpg

Size: 512x380, JPEG, Q: 100%

Reference Image:

View: Unprocessed VS Processed (Evidence)

200.00

100

Number of DCT Modes: 64

Map Type: Color

Show Saturation: Off

The detection of manipulated images is important in a number of areas, including the unmasking of 'fake news'. Here, the inset on the lower right shows the original, unaltered image.

tampered images being 'fake news' run rife. We must ask ourselves the question, can we rely on this image we see before us? Has it been authenticated?

Authentic images

Luckily, image authentication procedures exist and take many forms in the digital forensic process. Image authentication has its roots in metadata analysis to identify and compare the hidden information in an image. Various options exist:

- Compression analysis to identify capture type.
- Visual analysis to identify signs of manipulation.
- Camera matching to link a specific device to an image.

Digital images therefore reveal their meaning and integrity not only by what they show but also through the metadata associated with them. The location data, for example, is embedded within the files and can be used to see if the metadata location matches what is shown in the picture. A suspicious document allegedly signed in London can be analysed to see if the metadata location verifies this.

Originally, this method of analysis required an extensive knowledge of a proprietary computer script and even a PhD in advanced mathematics to apply the algorithms required. Such techniques are promising but fall victim to an expertise bottleneck. They are ill-equipped to counter the sheer volume of consumer-friendly desktop and mobile phone photo manipulation freeware available at the click of a button.

But image authentication software has been catching up in the arms race against altered imagery. Modern software goes one step further and can use metadata to reverse image search online for other photos taken by a potentially stolen device. Each camera has a unique noise pattern from its sensor arrays and even two identical iPhone models will have a unique separate noise signature, analogous to a fingerprint. This makes it possible to track down and cross-compare online photos taken from a missing device using GPS metadata.

Automating the process

Software capable of automating the process of cross-comparing seized digital photos can piece together photos taken with the same camera and can build cases and link fraudulent activity to previously unconnected individuals. Information embedded in digital images can therefore help to protect individuals against criminal activities.

The need for non-metadata specialists to be able to quickly validate digital images is now more important than ever. Specialist software is used by police officers to authenticate images submitted as evidence in criminal investigations. Police officers undergo a short training course lasting several days and are then able to verify an image's credentials without a PhD or extensive knowledge in coding languages.

> ***"To effectively carry out fraud investigations in a world where anyone can edit and manipulate a photo at the touch of an app, we must remain vigilant and treat photo images with a pinch of salt"***

It is not just scientists, academics or even police officers who should possess this ability as a base skill set. Journalists continue to battle with verification of fake news, a hot topic that understandably requires a more reliable means of detecting misleading images. Similarly, there is a need within the scientific community, where the need to verify questionable research paper findings is fast becoming a major issue. It is estimated that up to one in five published scientific papers contain imagery that has been tampered with.[3]

Remaining vigilant

Image manipulation and image-to-camera identification is a unique and fascinating part of digital forensics that has growing importance. Seeing is no longer believing in this day and age. To effectively carry out fraud investigations in a world where anyone can edit and manipulate a photo at the touch of an app, we must remain vigilant and treat photo images with a pinch of salt.

The tools and resources are there to do this. A shift in attitude towards how we see photos and their merit in fraud investigation processes is vital. In the face of advanced fraudulent technology, we must urgently treat photos with the same level of suspicion as we would a drawing or painting. With the right