Forging a photo is easy, but how do you spot a fake?

November 21 2014, by Stuart Gibson

I can tell this has been 'shopped, on account of the pixels. Credit: Mmxx, CC BY-SA

Faking photographs is not a new phenomenon. The Cottingley Fairies seemed convincing to some in 1917, just as the images recently broadcast on Russian television, purporting to be satellite images showing the MH17 airliner being fired upon by a jet fighter, may have convinced others.

In fact, recently there's been a proliferation of images appearing in the media that are not all they seem. Did Malaysian politician Jeffrey Wong Su En really receive a knighthood from the Queen? Has Iran exaggerated

its missiles, or North Korea its assault hovercraft? Was this cover of *Nature* manipulated for artistic symmetry? The widespread use and high quality of digital cameras and photo editing software has made the art of faking a whole lot easier and more commonplace – whether convincing or not.

Worth a thousand words

Images can mislead the viewer by modifying, inserting or removing objects from the scene. Many photo editing applications include tools that can remove objects cleanly from their surroundings with a few clicks. This is known as inpainting.

An early method was to fill the void left in the image by smoothly interpolating inwards, based on sampling the pixels at the edge of the missing area. Other techniques include seam carving, content-aware image resizing in which an algorithm establishes the image's important areas in order to remove or expand sections around them without affecting the subject of the image.

One of the Cottingley Fairy images - high tech in 1917. Credit: Elsie Wright

An alternative is to clone an area of the image (or another) and copy it into the gap. This technique can also be used to replicate objects – such as Iranian missiles, or North Korean hovercraft – and is easily implemented in editing software, although the edges of the copied region may need to be skilfully blended into the background to be convincing.

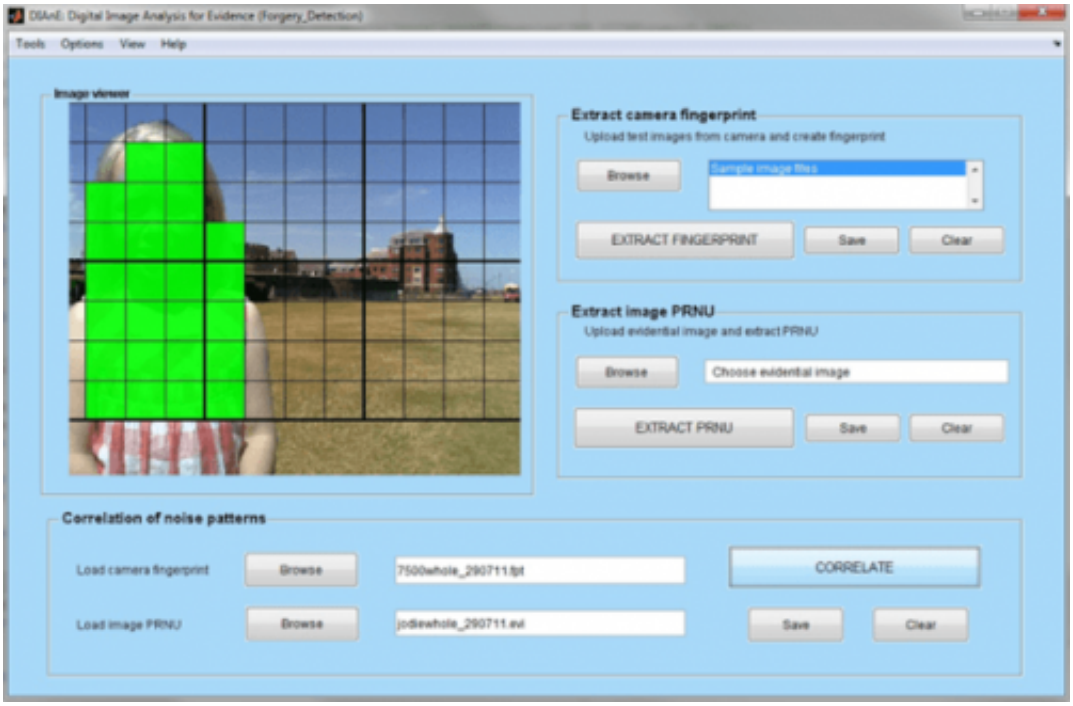
So the content – and therefore the interpretation – of an image can be dramatically altered. But creating really convincing images is more challenging than you might think; the direction and strength of lighting must be consistent between the altered region and the rest of the image, and this is hard to fake.

Unmasking a forgery

Digital image forensics is the science of detecting tampered regions in images and connecting images to the cameras or devices that created them.

Broadly there are two lines of investigation: those forgeries revealed by inconsistencies in the image's composition and those with detectable disturbances introduced during editing.

A poorly constructed composite photo will exhibit gross inconsistencies in lighting and perspective that will be noticed even by the untrained eye. For more accomplished forgeries, a rigorous analysis of shadow and reflection geometry may be required to detect tampered regions. This is a method developed recently by researchers at Dartmouth College in the US, whose approach is to superimpose lines on an image connecting objects to their shadows in order to indicate the position of a light source within the scene. Objects inserted into the image are likely to exhibit shading that is inconsistent with what would be expected given the position of the light source in the image.



Our research group designed software that detects differences in image noise to identify the edited region. Credit: Stuart Gibson, Author provided

When white light passes through a lens it can separate into red, green and blue wavelengths of light, producing an effect called lateral chromatic aberration which can be seen in photographs. The strength of the chromatic aberration depends on the properties of the lens and the distance of objects in the image from the lens' focal centre. So any elements of the composition added from another photograph, captured using a different lens, will show detectable differences in chromatic aberration.

All photographs contain artefacts – regular patterns, distortions, or errors – caused by the imaging process which are mostly imperceptible to the human eye but play an important role in digital image forensics.

For example, colour digital images are created by applying a filter of alternating red, green and blue over the pixels of a camera's sensor, so that each absorbs only one colour. A process called demosaicing then renders this information as a full colour image, but leaves a regular pattern. Any interruption to this pattern indicates tampering.

An interesting, growing trend is counter forensics, where the forger attempts to cover their tracks in order to evade these and other detection methods. For example, the image noise present in the original can be sampled and fake noise applied to any inserted image objects so that they appear to match the original. Clearly, faking it and finding fakes are two disciplines that are going to keep evolving as technology advances.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation