

## Digg.com Home page June 19 2007

**digg**™ News Videos Podcasts<sup>beta</sup>

All Topics Technology Science World&Business Sports Entertainment Gaming


All Apple Design Gadgets Hardware Tech Industry News Linux/Unix Microsoft Mods Programming Security Software Tech Deals

967 diggs **Bounty Fishing: 5 Ways to Easily Spot a Photoshopped Image**

The biggest hurdle we faced was how we were going to validate and authenticate the fish photos our users submitted - digitally altered photos can be incredibly convincing. Below are a few tips for spotting an image that has been photoshopped.

digg it

Submitted: 1 day 22 hours ago, made popular 1 day 20 hours 49 minutes ago

Submitter:  Oatmeal (news: [submissions](#), [diggs](#), [comments](#))

Topic: [News](#) » [Technology](#) » [Design](#)

Source: [www.bountyfishing.com](http://www.bountyfishing.com)

### [Photoshop and fishing don't go hand in hand](#)

Posted by [Richard M. Shafter](#) on June 19, 2007 in [Forensics software](#)

How to Spot a Photoshopped Image

BountyFishing works like so:

- Participants go fishing and photograph what they catch
- Participants then submit these photos to the BountyFishing website
- BountyFishing awards cash and prizes for the longest validated catch

The biggest hurdle we faced was how we were going to validate and authenticate the fish photos our users submitted. Photos altered with Photoshop can be incredibly convincing. With a few simple clicks of the "Quick Selection Tool" the fish shown below (top left) was selected, dropped into a separate layer, and stretched to add more than an inch to its length. With a little more work to move the shadow and soften any rough edges, the resulting image (top right) shows no signs of tampering. **Unaltered image**



## Photoshopped image



The solution we found was to use a piece of software developed by [Hany Farid](#), a professor at Dartmouth College who is renowned in digital forensics. When the fish was stretched, Photoshop filled in the missing pixels by interpolating their values from the original recorded pixels. These regularly spaced new pixels are a specific combination of their surrounding pixels. Such regularities rarely occur in natural images, so their presence can be used as evidence of tampering.

Shown below is the output of the BountyFishing software that detects these correlations – the red-coded regions corresponds to the doctored portion of the image.



This software is used by federal law enforcement agencies and can detect various forms of tampering.

We have exclusive rights to the software for measuring fish, but if you really feel like getting your hands dirty with digital forensics [Hany Farid's website](#) has an interface to [MatLab](#) for manipulating and analyzing digital images. In addition to the software above, a few other dead giveaways that a photo has been altered are:

- Excessive cloning - repetition of a particular piece of the photo, often used to stretch or morph images.
- Inconsistencies in lighting and noise. The easiest way to spot altered lighting is to increase the contrast of a photo so all the differences in lighting are exaggerated.
- Look for shadows that don't match up what's casting them.
- Optical aberrations, including patterns that aren't seamless or appear to be inconsistent (or artificially consistent) with the surrounding area.
- Using human anatomy and other reference points BountyFishing verifies the authenticity of the ruler's length.

We've got a [flash demo](#) of how we authenticate photos that gives a little bit more information about how this all works.