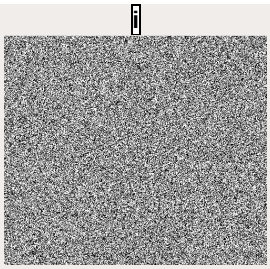
Avoiding Camera Noise Signatures



If you take enough images with your digital camera, they can all be compared together and a unique signature can be determined. This means that even when you think that you are posting a photo anonymously to the internet, you are actually providing clues for the government to better tell who you are. The larger the sample size of images they have, the easier it is them to track down images coming from the same camera. Once they know all the images are coming from the same camera, all they then have to do is find that camera and take a picture to confirm it beyond a reasonable doubt.

It is important to remove this noise signature so that you cannot be tracked down. I cannot guarantee any of these methods will work beyond the shadow of a doubt because the woman doing research for the government on how to find the signature is very good. Check out her papers if you're *really* good at dense math, and pass along what you learn. I can only promise that this will make their work more difficult.

Step 1Remove the camera info

When you take an image with a digital camera, the camera itself leaves a data file which automatically identifies itself. This file is called an EXIF and usually has information like the make of the camera, the ISO setting, the date and time, the pixel setting, etc. This needs to be removed. The easiest way to remove this is to open photoshop and save it for web.

When you save, I recommend using a JPG compression with a quality setting of no better than 60%. This will add a lot of ugly noise make it slightly harder to create a noise signature.

Step 2Clean the lens

Clean your camera's lens constantly with a non-scratch cloth that you can get for cleaning camera lenses or eye glasses. This will remove specks of dirt that will show up from image to image and never change. If there are pixels never changing on your camera then it makes it really easy to identify you. This is why it is important to crop the image.

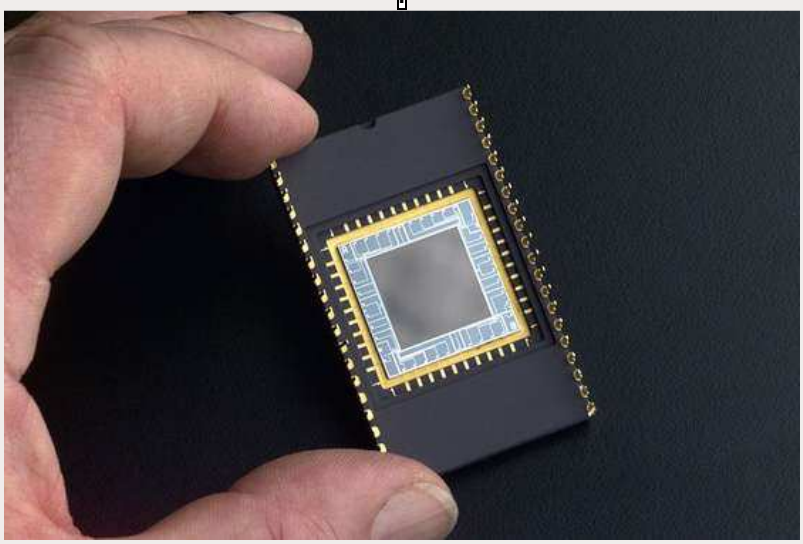
Step 3Crop and resize the image

If you have dirt on your lens, dead pixels or "hot" pixels, then it is really easy to find images from the same camera since they will all have static pixels. This means, from image to image there will always be a handful of pixels that don't change.

The way to get around this is by cropping and resizing the image. This will shift the position static pixels and when images are compared together make them just seem like noise.

This alone will not always remove the noise signature itself, but it is one way to make it harder to identify it.

Step 4About the noise signature



So far I've only told you how to make it hard to tell a picture has come from your camera, but not how to remove the noise signature. The marks made by dirt on the lens and dead pixels is actually different than the noise signature that they use to keep track of what pictures you are taking.

The noise signature itself is actually due to thermal noise (environmental heat) and imperfections on the CCD itself. Professional photographers and astrophysicists have tried to compensate for this by creating cameras that evenly lights a CCD a moment before the image is taken to create a noise reference against the image being taken or by super-cooling the camera itself so that heat can't distort the CCD.

In your store-bought camera, it won't have either of these functions and so you will end up getting a lot of pseudo-random noise mainly on the last 3 bits of every pixel. This noise isn't really noticeable to the naked eye, but with a large enough image sample, they can create a noise profile and match almost with certain accuracy pictures from the same camera. Since the noise is dispersed throughout the image itself and tends to remain constant through certain standard image manipulations, it is hard to remove without destroying the image.

Step 5Removing the noise signature

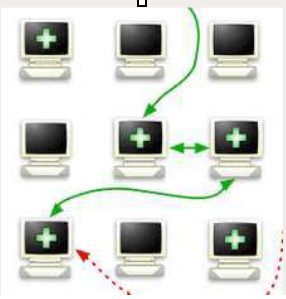
Ideally, you would remove the noise signature by making the image cleaner. It is noise after all. Although, determining which noise to remove isn't always clear.

It is probably more effective to remove the noise signature by creating more noise. One thing to try is to open Photoshop and save an image as a jpg using bicubic compression, resize it, crop it and then save it for web, again as a jpg (removing the exif) and finally save it for web again as a jpg using a quality of about 50. This should destroy the noise signature beyond recognition, but the image might not look too good.

It wouldn't be good to do this ever time either since you will end up creating a new "signature." The best thing to do is to save each image using a different elaborate method every time. For instance, you might convert something to a flash video, take a screenshot and then save for web as a jpg compressed with a quality of about 50.

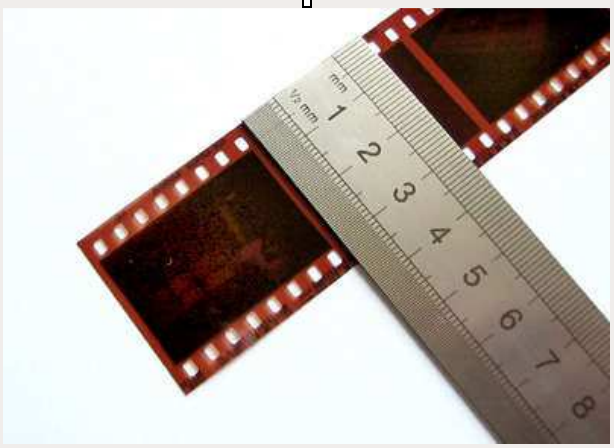
It may not work, but you could also try adding a small amount of random noise to the red and green channels. This might actually clean up the image and remove the signature, but I'm not sure.

Step 6Common sense

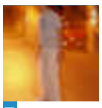


If you're bothering to make your image anonymous, post it anonymously. Use a TOR server and if you have to register for an account to post it, create a new one for every couple of images. Make the images seem like they are coming from as many places as possible.

Step 7Use a film camera



If you are really that concerned, use a film camera and scan your images using multiple scanners at multiple different corporate copy shops. The only downfall to this is that you actually have to go somewhere to scan the images and store employees or video cameras could maybe identify you. If you wait a few days before posting things online, it will make it harder for them to connect it with you.



5

May 1, 2008. 12:47 PM**mightysinetheta** says:

Tor isn't inherently a better or safer idea, unless you use full end to end encryption independent of Tor. It encrypts within the network, but the exit nodes are not encrypted. Thus the exits are good choke points to sniff at.

http://czarism.com/tor-vs-security-sniffing-exit-nodes

Reply

1

May 3, 2008. 10:04 AM**NuclearDog** says:

Tor is an inherently better idea in a case like this (posting images). The link you posted discusses the ability for an exit node to sniff the traffic coming out, but I'm pretty certain the author of this instructable is more concerned about anonymity (which would still be preserved) than someone

getting a hold of some of his traffic (only some, as tor will change exit nodes each request). He's talking about posting the images online anyways, so someone sniffing them and getting a copy is really not a concern at all.
Reply

May 3, 2008. 7:00 AM**WikiLeak** says:
@ mightysinetheta -
End to End encryption (e.g. PGP encrypted files or emails, or SSL secure web sessions) on its own might protect the Confidentiality of your uploaded images in transit or storage, but does nothing to preserve your Anonymity from powerful snoopers who have access to either your computer's Communications Traffic Data, or that of the target upload computer i.e. host IP address, time, date, amount of data uploaded, and possibly other web browser environment variables etc.

If, for example, you are uploading pictures of riots being brutally suppressed by the authorities, and yours is one of the few, or perhaps the only, upload session to a particular website, from say, Burma, Tibet or Zimbabwe, then the fact that you have used End to End Encryption will make little difference, as you, your family, friends and associates, are hunted down by the local secret police.

One approach may be to use an encrypted Secure Sockets Layer web server upload session (https:// as used for online credit card and internet banking transactions) in combination with a Tor Hidden Service running on the same machine.
e.g. one of the methods of secure anonymous uploading offered by the wikileaks.org whistleblower website:

http://wikileaks.org/wiki/Tor

This is not that easy or swift to use, and is not infallible either - you have to trust that wikileaks.org or their former Pirate Bay web hosting company in Stockholm, Sweden, has not been infiltrated.
Anybody posting banned or controversial images, has to make their own risk calculation, balancing risk of discovery with speed and convenience.

Wikileaks archives of censored images of riots in Tibet
Reply

5

May 3, 2008. 1:58 PM**mightysinetheta** says:
@ WikiLeak and NuclearDog You guys are correct, I didn't mean to say that you shouldn't use Tor or that SSL was better alone for this application. (Should have worded my post better) What I wanted to

point out was that Tor has its own issues as well, some of which are remedied by using SSL in conjunction with Tor. I think WikiLeak covered it very well in his post.
Reply

May 2, 2008. 11:51 AM**ax0n** says:

I found this article highly interesting. Let me share with you a tip I use that might help:

When I'm scanning in images from a print source, I invariably see all the dots used to make up the image. The trick with those is to scan them at the highest optical resolution you can (1200 dpi or so). Zoom in to 100%, then apply gaussian blur. Push the radius just far enough that the dots start to run together. Then under resize image, chop the DPI in half, choose "bicubic sharper" and let it go.

The result is a smooth image, and usually I apply a gentle unsharp mask afterwards to restore some edge contrast.

In this case, you'd probably do well to just leave it a tad blurry. Any radius over 1.5 pixels should be enough to knock out the noise signature after it's resized.

Additionally, there's a very nice Perl script called exiftool that's part of the perl-Image-ExifTool module. It allows all kinds of scriptable exif manipulation, but the most important, is the ability to destroy the exif data completely.

Example: *exiftool -all= <filename>* (note the space after equals)

The article also mentions digital noise reduction. My Canon DSLR has such an option. (All Canon DSLR's offer this, from the original digital rebel up to the EOS Mark 1 DS) What it does is takes the shot, then takes the same shot with the mirror down and aperture closed to get a "noise print". It then subtracts the second data from the first. That should help slightly, although it may be possible that this creates a "hole" that can be identified also.

As the article says, any set of manipulations repeated will eventually hand someone a pattern should they choose to undertake such an option. (No doubt they will.)

To wit, you should take as much precaution in **how** you post your image as you do in scrubbing them to prevent them from being used against you.

Tor is a good start, but not a complete solution in and of itself. Consider stealing wireless from somewhere and then using Tor. Additionally, using services hosted outside your country (preferably ones that aren't cooperative with your government) can be a good road block also.

Lastly, remember that the truth will set you free!
Reply

May 1, 2008. 2:28 PM**No One of Consequence** says:
I've worked as a professional astronomer, and I know a lot about methods of noise reduction in images. The "evenly illuminated screen" method (called a flat-field) described is useful for taking out some portion of unchanging image noise, but there are other methods that we use as well. The one that's practical for use with regular digital cameras is the "image flat" -- we would take all of the images taken over the course of the night and average them together. The signal averages out given enough image, leaving only the unchanged noise -- you can then subtract it out from your actual images. The software we used doesn't work with JPGs, and it's a lot easier for monochrome images (you'd probably want to work separately with the blue, red, and green channels) but the principle should work just as well. Take a bunch of pictures of something fairly boring -- the sky on a cloudless day, a white piece of paper, whatever -- and average them together to get your flatfield.
Reply

May 2, 2008. 10:49 AM**cypherpunk1** says:
I seem to recall a program called Vega that could do dark frames, and that sort of thing.

That could be quite useful, as presumably, subtracting the dark frame should do that. I think it works with jpgs.
I'm not sure where to find a copy, but whilst looking, I found a program called Astromix that looks promising.
Its at http://www.astromix.com/download.htm
Reply

May 1, 2008. 2:18 PM**Memetic Engineer** says:
Digitally scanning a film image is really just another form of digital photography, so you should really also apply Steps 1 to 5 to your scanned images as well.

Scanners also have their characteristic individual electronic, optical and mechanical imperfections and abberations within their manufacturing tolerances, and they also pick up extra potentially identifying charateristic wear and tear with use.

If as Step 7 suggests, you make use of someone else's scanner, then you might not be able to erase the original copies of the temporary files which are written to the hard disk of the personal computer running the scanning software, or which are sometimes built into the the larger types of office or

commercial scanning / photocopying systems (or even Johnny Mnemonic style high resolution fax machine memory buffers).

You will also have probably have left your fingerprints and DNA samples on the equipment.

Photoshop and other image manipulation software tends to preserve most of the identifying EXIF metadata, which can include potentially traceable digital camera serial numbers, Adobe software GUIDs etc.even if you apply filter effects (some of which are reversible) or resize the image, unless you Save As to a different file name from the original.

Most digital cameras (and mobile phone cameras) also embed a small thumbnail image which they use when they display a "photo album" view of the various images you have taken, on the camera / phone display , usually to aid image selection for deletion or transfer etc.

This is not amended when the main image is manipulated in Photoshop etc, and may betray or give clues about identifying numbers or human faces etc. which you are trying to censor or redact.

Phil Harvey's multi-platform ExifTool perl libary and stand alone Windows executable software, allows you to view, amend , add or remove such metadata (and extract embedded thumbnail images), from a wide variety of image and document file types.

http://www.sno.phy.queensu.ca/~phil/exiftool/

Reply

4

May 1, 2008. 4:29 PM**damasta** says:

digitally scanned images don't need to be edited if you don't use your own scanner you may leave traces to the copy store, but never to your own home

Reply

May 1, 2008. 1:04 PM**tuesdayschild** says:

Scanning the image is really the only way to be sure; even noise added by cropping and recompressing won't disguise everything, according to Fridrich's work.