# Schneier on Security

Home > Blog

## Digital Cameras Have Unique Fingerprints

Interesting research:

> Fridrich's technique is rooted in the discovery by her research group of this simple fact: Every original digital picture is overlaid by a weak noise-like pattern of pixel-to-pixel non-uniformity.
>
> Although these patterns are invisible to the human eye, the unique reference pattern or "fingerprint" of any camera can be electronically extracted by analyzing a number of images taken by a single camera.
>
> That means that as long as examiners have either the camera that took the image or multiple images they know were taken by the same camera, an algorithm developed by Fridrich and her co-inventors to extract and define the camera's unique pattern of pixel-to-pixel non-uniformity can be used to provide important information about the origins and authenticity of a single image.
>
> The limitation of the technique is that it requires either the camera or multiple images taken by the same camera, and isn't informative if only a single image is available for analysis.
>
> Like actual fingerprints, the digital "noise" in original images is stochastic in nature  that is, it contains random variables  which are inevitably created during the manufacturing process of the camera and its sensors. This virtually ensures that the noise imposed on the digital images from any particular camera will be consistent from one image to the next, even while it is distinctly different.
>
> In preliminary tests, Fridrich's lab analyzed 2,700 pictures taken by nine digital cameras and with 100 percent accuracy linked individual images with the camera that took them.

There's one important aspect of this fingerprint that the article did not talk about: how easy is it to forge? Can someone analyze 100 images from a given camera, and then doctor a pre-existing picture so that it appeared to come from that camera?

My guess is that it can be done relatively easily.

Tags: cameras, de-anonymization, forensics, forgery

Posted on April 25, 2006 at 2:09 PM • 68 Comments

## Comments

**AG • April 25, 2006 2:36 PM**

I have to wonder if the study was from different camera models or the same exact model. I bet they were using different camera models.

The imperfections though would seem to me to be worthless do to the malleability of digital data. I would think even if someone resized the image or changed the format it would lose it's "fingerprint".

---

**Erik V. Olson • April 25, 2006 2:38 PM**

I'm surprised this is coming out now — it's been known for years in the astronomical community that each pixel in a CCD array doesn't respond exactly the same. Thus, the importance of thing like dark frames (images shot with the shutter closed) that allow you to correct for pixel response irregularites.

---

**Jef Poskanzer • April 25, 2006 2:41 PM**

Yeah, it's probably forgable. Well, the first step would be to remove the noise signature from your own camera – software for that will probably show up pretty fast. Applying that software in reverse would let you forge someone else's noise signature. I guess the question would be, can you get the noise signature from someone else's camera by just analysing pictures they have taken, or do you need to borrow the camera and take a picture of a known subject such as a black/white/gray frame (chosen plaintext).

---

**Victor Bogado • April 25, 2006 2:42 PM**

I would be interested if this analisis would be able to remove the noise and make my digital images less noisy. 😛

---

**Per Hedetun • April 25, 2006 2:56 PM**

It would be interesting to know what needs to be done in order to mask the fingerprint of a picture. Is it enough to just decrease the resolution of the picture slightly?

Or perhaps some slight gaussian blur is the answer?

Which actually brings me to Victor Bogado's question above – this GIMP-tutorial describes how to best remove CCD noise:

http://gimp.org/tutorials/Selective_Gaussian_Blur/

I'm guessing that this method is also sufficient in masking/removing the fingerprint…?

---

**dewey • April 25, 2006 2:59 PM**

There's already software to improve digital images by reducing noise. Some time ago I compared two competitors. (http://www.thesassers.com/dewey/NoiseReduction.html)

I have no idea if use of this software leaves sufficient variation for digital fingerprinting. Both packages, however, say that for the ultimate in noise reduction you need to use an image taken by the actual camera as a basis. I also seem to recall that there are many other factors to sensor noise including ambient temperature and activity of the sensor (e.g. exposure time). I'm not sure what effect this has on fingerprints.

I, too, am surprised that this is news — and from the reputed credentials of the researcher I would suspect that it was news only to the reporter and the researcher has a more interesting realization which the article didn't cover. Perhaps the fingerprint survivies all of the criteria and processing I've described.

---

**Chris • April 25, 2006 3:13 PM**

I'm skeptical as to how well this will actually work in practice. I can believe analysis such as this will work if the examiner has access to raw and complete sensor data (e.g. a Nikon "NEF" file). But I only have those types of files available for images I shoot myself; generally I don't distribute them because of their large size.

If all that is available for analysis is a file (or files) that uses a lossy compression algorithm like JPEG, the minute variances the technique would seem to require would not be present. Further, even if lossless copies of multiple images are available, they have likely been manipulated by the photographic workflow (color and brightness adjustments, sharpening, cropping, etc.). These adjustments also seem likely to skew any calculations to fingerprint the sensor of the camera that took the original photo. Would simple image cropping eliminate enough sensor data that only a partial fingerprint is possible?

Further, it seems that anyone serious enough about distributing illegal-to-produce/possess photographs (the article mentions child pornography) would take steps to obfuscate the origin of the image beyond any potential effects of normal image adjustments.

The article is too short on details to know if any of my speculations are true, or how robust their fingerprinting technique is. It seems more likely that this is an attempt to gather funding for further research.

Remember, the root passwords to the U.S. Constitution are "terrorism" and "child pornography".

---

**BWJones • April 25, 2006 3:13 PM**

Well sure. This has been known for some time (and used by certain "groups") as each digital camera has unique properties inherent to its lens, CCD, CCD filter and other optical path properties. (Also, think dead pixels that are sometimes hard to detect given the processing algorithms in many digital cameras, but they *are* there). SLR camera systems can complicate matters some given the diversity of lens and filter combinations used, but often the CCD will be able to be identified as uniquely belonging to a particular camera regardless of what other optical path devices are used.

---

**D • April 25, 2006 3:22 PM**

"Disappearing Cryptography", P. Wayner, gets into this subject pretty well. The images they speak of are necessarily in RAW format. This noise appears in the least significant bits of the image. JPGs would have the noise compressed right out (JPG is lossy starting with least-significant, and working its way up…)

Removing the signature from RAW photos should be as simple as setting all least significant bits to know values (all 0, all 1, 0101, etc). If they can use several images from a single camera to determine the fingerprint, they can certainly emulate the fingerprint.

What does this really prove? It can't really relied upon to prove copyright of the image as it can be forged. It's probably noteworthy as an investigative technique, but not as court-admissible evidence.

IANAL.

---

**D • April 25, 2006 3:30 PM**

Also, professional digital photographers maintain their original, unprocessed photos in archives. (This might come in handy if a photography house needed to research which photos were taken by which camera…but why?) You *never* destroy the original photo of a paying client by altering the file in any way — that's asking for trouble (the Murphy kind usually, but sometimes the legal kind).

Further, they don't distribute those originals – at the least, the files are compressed to a lossy format before publishing or sharing with a client.

Lastly, I'm sure these variances show up between cameras of the same model. The CCD manufacturing process causes this phenomenon to occur.

---

**dr.bad • April 25, 2006 3:33 PM**

in ideal conditions (getting raw uncropped images from the camera) this would be quite easy : there is no alignment to do. for every image and every pixel (x,y), estimate the true value at (x,y) by avering neighbours, then check the difference with the actual value. the difference gives the error, which should have a gaussian noise component and a fix component due to the sensor. then correlate matrices of personal components. this is all fine and dandy until the loss induced by JPEG compressions completely blows up your individual variances. anyway assume enough information filters by. you still need to compensate for the Big Three of computer vision : rotation, translation and scaling. this therefore reduces to choosing characteristic sensors (those that are obviously bad) and then doing constellation matching. filtering those should be pretty easy and as said above, recreating the characteristic pattern for your camera (to "prove" that you took a picture) should also be a piece of cake.

---

**Woody • April 25, 2006 3:36 PM**

As others have pointed out, this is well known in some digital photo circles. Mainly the low-light/long exposure ones (like astronomy), where the noise builds up over time and gets rather visible.

IIRC, cameras were now allowing black frames to be shot to internally compensate, or apps like Photoshop and Aperature were able to apply the inverse of a black frame to the images in bulk as a specialized de-noise filter.

I think it's a per-pixel subtration operation, with the black frame matched in exposure time to the photo's exposure (which should be encoded into the image).

At least, I thought you could do all this (and that professional photographers were doing it).

---

**Dragonhunter • April 25, 2006 3:50 PM**

9 camera's seems like a *very* small sample size to me….plus, as others have mentioned, we are talking digital information here. Only if you have the actual, original, uncompressed image will this work. I don't think terrorist child pornographers shoot in RAW mode (no pun intended) I'm guessing a lossy jpeg would work just as well for whatever they want it for. Therefore, all of this is just well…..snake oil.

---

**Carlo Graziani • April 25, 2006 3:57 PM**

Doesn't the pattern drift over time? I would have thought that thermal and environmental effects would cause shifts in this sort of noise, and that it would be difficult to match up the noise in pictures not taken in the same session.

---

**Alexandre Carmel-Veilleux • April 25, 2006 3:58 PM**

In MRI image processing, non-uniformity correction is par for the course. The uniformity corrected against is the magnetic field so it is easier to estimate and correct (it doesn't require multiple images to do a reasonnable job) but the concept is the same.

It would be trivial to correct – or randomize – this uniformity issue if required. Heavy JPEG compression is probably sufficient to muddle it beyond recognition. Resizing to a smaller size would also do the job. Or applying a gaussian blur of some sort.

---

**Mulder • April 25, 2006 4:10 PM**

I'm surprised no-one has brought out the possibility of similar scheme that was recently revealed wrt. printers: the ability of authorities to track back the images to certain printer/camera based on a secret list of fingerprints maintained by the manufacturers. While this might not be probable, I would think cameras are actually more tempting target for such scheme than printers.

---

**Alan Porter • April 25, 2006 4:22 PM**

@ Victor Bogado and Woody

This technique is currently in use by some relatively cheap digital cameras. My Canon (Ixus/Powershot 330) measures the noise right after taking long-exposure shots, and then it subtracts that noise from the image.

---

**Fred Page • April 25, 2006 4:25 PM**

@Mulder
"I would think cameras are actually more tempting target for such scheme than printers."

One of the major concerns about printers is their capability to make reasonable counterfeit currency. Reducing fake currency is essential for any government that both makes and uses their own currency.

**Anonymous • April 25, 2006 4:38 PM**

The restrictions on needing either multiple images or the camera are the exact same restrictions currently needed for matching guns to bullets. You either need the gun or multiple bullets to match to each other. This technology works exactly the same as bullet matching.

**jmr • April 25, 2006 4:48 PM**

@Anon

… except that bullets are hard to counterfeit markings on, while digital pictures can be trivially manipulated.

**Longwalker • April 25, 2006 4:51 PM**

Even if a camera’s noise fingerprint survives JPEG compression, it’s not going to survive going through Noise Ninja, Neat Image, or any of the other CCD noise reduction tools.

**Wim L • April 25, 2006 5:13 PM**

As I understand it there are a handful of pixel-to-pixel manufacturing variations like this. “Dark noise” is very consistent and is commonly subtracted out by the camera (as best it can), and there is also a temperature-dependent variation, and probably others. Given a raw file and exposure info, it’d probably be possible to estimate the temperature of the imaging chip, for example.

I don’t think that a Gaussian blur or JPEG compression would reliably eliminate this “fingerprint”. Consider that the speckle pattern has a Fourier transform which is probably white-noise-like. A blur or a JPEG compression will only mess with some parts of that spectrum. Looking at the quantization table used for the JPEG image will let you figure out which parts of the image still contain information on the sensor noise pattern. Multiple unaligned JPEG compressions might make it impossible to do this, but I think it’d take a real statistician to answer that question.

**citadel • April 25, 2006 6:00 PM**

Here is a link to the original paper if you’re interested:

http://www.ws.binghamton.edu/fridrich/Research/LukFriSPIE06_v9.pdf

**Jeremy H • April 25, 2006 6:05 PM**

“In preliminary tests, Fridrich’s lab analyzed 2,700 pictures taken by nine digital cameras and with 100 percent accuracy linked individual images with the camera that took them.”

9 cameras is too small of a sample size. The same kind of studies “prove” that digital face recognition work. The algortihm works wonders (with 100% accuracy, no less) on a very small closed set of targets, but completely fails when tested in the wild.

---

**kashmarek • April 25, 2006 6:13 PM**

When someone tells you they can find this “signature” in the printed copy of a digital image, then you should start worrying. For some copiers/printers, that signature is found in the printed output.

---

**Brandon • April 25, 2006 6:15 PM**

Any thoughts on when 1984 will arrive?
Has it already?

---

**citadel • April 25, 2006 6:45 PM**

It would be interesting to know the results if Fridrich studied say x pictures using y different cameras that were all of the exact same make and model. Then repeat that test for z different makes and models of digital cameras available on the market today. It’s quite a large problem to tackle.

---

**citadel • April 25, 2006 7:06 PM**

“Any thoughts on when 1984 will arrive?
Has it already?”

1984 is alive and well in Dillingham Alaska…

80 Cameras for 2,400 People

http://www.schneier.com/blog/archives/2006/03/

---

**anonymous Mooard • April 25, 2006 7:18 PM**

I am highly skeptical that this can be used outside of a laboratory setting i.e. would the CCD behave the same at 0 degrees and 100 degrees? How about different light intensities. I don’t know much about CCD but quartz crystals used in timers change frequencies quite a bit with respect to heat as well as with age and use.

---

**Longwalker • April 25, 2006 8:28 PM**

“Any thoughts on when 1984 will arrive?”

It arrived on 20 January 2001.

---

**Anonymous • April 25, 2006 9:45 PM**

To quote the paper:

The most important component of PRNU is the pixel non-uniformity (PNU), which is defined as different sensitivity of pixels to light. The PNU is caused by stochastic inhomogenities present in silicon wafers and other imperfections imposed during the sensor manufacturing process. As such, it is not dependent on ambient temperature and appears to be stable over time.

---

**Stefan Wagner • April 25, 2006 11:25 PM**

From the pdf, linked by citadel: "Our research indicates that it is possible to perform relatively reliable identification of forged regions even from images that were JPEG compressed with quality factors as low as 70."

And Longwalker is right, it was Jan. 20th or 2001 when it arrived.

---

**RonK • April 25, 2006 11:36 PM**

@Victor

It would make your photos less noisy, but unfortunately, probably not significantly so if you are talking about the noise you see when taking photos in low-light conditions. If I'm not mistaken that noise is "shot noise", and happens because of photonic quantization.

@dr.bad

"need to compensate for the Big Three of computer vision : rotation, translation and scaling" — I don't see why unless the images have been subsequently transformed after being registered by the sensor.

@Jef Poskanzer

"can you get the noise signature from someone else's camera by just analysing pictures they have taken" — If the result required an image of a specific scene it wouldn't be useful in general for tying a camera to the images it generates. I can think of several ways to calculate the signature as long as the input images you give me do not all have strong gradients in fixed locations.

BTW, kind of interesting to see your name pop up here! Thanks for inventing PNM way-back-when.

@D

After a cursory glance at the article, it seems to deal with the question if some parts of an image taken by a camera have been retouched after the fact; i.e., a technique to show in court or other investigations that a non-professional has been fiddling with evidence. As the discussion shows, if you know what you are doing, you should be able to get around it.

---

**AndrewM • April 25, 2006 11:49 PM**

As other posters have pointed out, this information has been in use in astronomy for a long, long time. I worked on dark and flat fielding CCDs for a few years way back when. The signature will mostly survive JPEG compression on a high-resolution camera (but probably won't survive scaling), is temperature stable (but not entirely exposure time stable), and doesn't change much over time.

However, it’s also pretty trivial to dark-field and flat-field most cameras, some even do it themselves (take dark field and flat field images at the same shutter speed and ISO setting, subtract the dark field then divide by the flat field, renormalise, you’re done). Noise reduction software may not necessarily do a good enough job if it only works on single images, since the statistical properties of the CCD can survive that… and the analysis software may well be able to tell what software you used to reduce the noise.

---

**Ingo • April 26, 2006 1:53 AM**

This sounds like a typical application of Independent Component Analysis (ICA). The CCD-pattern is statistical independent from the scenes of the photos and should result in a stable component. If you know it’s distribution and have some photos to analyse, it should be easy to find.

---

**blinky bill • April 26, 2006 1:53 AM**

“The limitation of the technique is that it requires either the camera or multiple images taken by the same camera”

umm .. which is a problem for whom? not for “anyone” with a hook into the megacorps who manufacture (or distribute) the cameras.

Maybe not in country A, but perhaps in country B.

@Mulder
“I’m surprised no-one has brought out the possibility of similar scheme that was recently revealed wrt. printers”

Very much so.

@Fred Page
“One of the major concerns about printers is their capability to make reasonable counterfeit currency. Reducing fake currency is essential for any government that both makes and uses their own currency.”

So is reducing effective counter-propoganda, whether it’s conducted by disenfranchised “kids at the mall”, “enemy foreign agents”, “traitorous capitalist/communist interests”, “terrorists”, “religious fundamentalists”, “the criminals”, or merely the “democratic opposition”.

The motivations of the actors need not be entirely malicious, imagine how easily a true believer can be convinced of the benefits of ‘early intervention’ in the case of the disenfranchised …

… and with all the terrorist child pornographers on the loose that the government/media do such a good job of warning us about, it seems a bit of a dead cert that if printers have been flagged for the last X years (yes the rumours started back in the days of black and white) and internet traffic has been being swallowed whole (google AT&T NSA) then cameras are also flagged at the factory.

And if not by the “official” government, then why not by the same “criminals” and “terrorists” who infiltrate so effectively our “white collar” society?

The idea of ‘levering’ this idea for noise cancellation is .. well .. redundant. The manufacturers probably already build in a degree of cancellation, the costs of correlating and effectively cancelling is part of what makes a good camera expensive, I think. (Yes, software post-processing might make a nice addition to GiMP .. I think it was already mentioned wrt commercial sw).

If one accepts the idea of conspiracies at play, one might also expect that an artificially high level of noise may be allowed in cheaper models … “for whatever reason”.

Statistically, matching images between only nine cameras is not impressive. What is impressive is that it was successful 100% of the time. That is statistically significant, whatever way you look at it. It “merits further investigation” to say the least.

@RonK
“As the discussion shows, if you know what you are doing, you should be able to get around it.”

I wouldn’t bet on it. Statistical analysis improves with quantity of data. So whatever measure you take to anonymise your data can be abrogated by analysing larger data sets.

And assisted by eliminating the potential sources who are known not to have been at whatever event it is that was photographed.

Given present-day leeching of phat data pipes by the “authorities”, I think any useful photojournalist’s activites are already categorised and metered.

Interesting but infrequent posters would go into ‘watch this space’ categories until enough data arrives.

Those which never amount to enough data probably get grouped into ‘are they dodging the system and how’ category, for later re-analysis.

Not many people can afford to dispose of a decent camera on a regular basis. It really is an effective means of social control, even if this is all ‘just theory’, since it scares the willies out of wanna-be photojournos like me.

I have the requisite technical background to understand these issues, and I gave up any belief in anonymity through technology long, long ago. The “number of the beast” luddites are closer to the mark than the delusional ‘Oh I’ve got nothing to hide’ types.

---

**IVLIANVS • April 26, 2006 1:57 AM**

“Can someone analyze 100 images from a given camera, and then doctor a pre-existing picture so that it appeared to come from that camera?”

This is already done since a long time in astronomy if my memory serves me correctly. Exposition time is in minutes/hours for these CCD, so it’s important to remove any non-linearity. And yes, to remove most of the thermal noise, these cameras are cooled.

---

**blinky bill • April 26, 2006 2:02 AM**

apologies, I misunderstood RonK’s comment. Missed the context and thought “getting around it” was re cleaning up the signatures, not forging them.

Re forging them, yes, I think it would be possible to forge convincingly for small areas of small numbers of photos if you know how they are analysed … but new or different analysis schemes might work in ways you have not anticipated when falsifying the signature .. so my answer does somewhat match RonK’s point anyway. 🙂

---

**Gabriel • April 26, 2006 3:23 AM**

Couldn’t you destroy the fingerprint by randomly altering the least-significant bits of the RGB values of each pixel in the image?

---

**MoonShadow • April 26, 2006 5:02 AM**

@Carlo Graziani – “Doesn’t the pattern drift over time?”

Yes. It also depends on temperature and moisture levels. Some cameras take shots internally with the shutter closed to provide a reference for automatic noise removal; such reference images must indeed be taken as soon as possible after the target image to minimise discrepancies.

---

**Aether • April 26, 2006 6:22 AM**

“This virtually ensures that the noise imposed on the digital images from any particular camera will be consistent from one image to the next, even while it is distinctly different.”

With all this CSI in the airwaves, people tend to think that identification technologies (fingerprint s, DNA, bullet striae, etc) can be trusted in absolute terms, which is not the case at all – there is ALWAYS a very important subjective element in deciding whether a match is there or not.

IMHO, the most interesting part is actually the algorithm to extract the noise signature:

http://research.microsoft.com/~kivancm/publications/icassp99.pdf

---

**bob • April 26, 2006 6:54 AM**

Analog cameras have ‘unique’ lens signatures at the near microscopic level as well.

---

**Clive Robinson • April 26, 2006 8:17 AM**

The cammera relies on an electronic chip full of sensors. People forget that making the chip uses masks and electromagnetic radiation. Therefore just like with any printed image you would expect registration variation (think Ink Jets and cartridge changes) as well as the variability in sensitivity that Astronomers use “Dark Frames” to help correct. Forensic Bods have been doing similar with typewriters, photocopiers and all sorts of optical equipment for years.

I guess you can view the finger print in exactly the same way as a Digital Water Mark (DWK). Therefore it is prone to all the attacks DWK’s are prone to.

The Cambridge Labs under Ross J Andersson showed that digital watermarks could be compleatly destroyed just by a non perceptable 2D stretching and shrinking process.

The golden rule with all of these things is “If Science can Measure the Difference Science can Fake the result”. We have seen this with real fingerprints DNA and there is some evidence to suggest that Iris scanning is also fakeable.

---

**Mr W • April 26, 2006 9:07 AM**

The pattern of pale yellow dots deliberately added to every page by colour laser printers has been well studied and documented:

http://www.eff.org/Privacy/printers/

The dots encode date, time and printer serial number.

In this case, I imagine the scheme is easily defeated by printing on pale yellow paper.

Mr W

---

**Jeremiah Blatz • April 26, 2006 9:40 AM**

I couldn’t tell from reading the paper, but does this apply to JPEG compressed images? One might imagine that a camera that mapped out hot pixels, then JPEG compressed the file (which is most good digicams these days) would make this significantly more difficult. Furthermore, many people go through lots of effort to remove the noise form their images in post, making this approach even more difficult for images found in the wild.

---

**arl • April 26, 2006 9:42 AM**

I wonder if this is as accurate as they claim. I am thinking of the claim that was made as to being able to tell which box a bullet came out of, based on testing the trace elements in the metal. Independent testing showed that it was not possible, but people had gone to jail as a result of the claim.

“ladies and gentlemen of the jury, the lab results prove that the picture was taken by this camera….”

---

**Tank • April 26, 2006 9:51 AM**

“There’s one important aspect of this fingerprint that the article did not talk about: how easy is it to forge?”

I think you’ll find they didn’t talk about it because that actually isn’t an important consideration.

“Can someone analyze 100 images from a given camera, and then doctor a pre-existing picture so that it appeared to come from that camera?”

No. Humans have a limited life span. Without any sane reason to be wasting time analysing hundreds of images so one can be passed off as coming from a particular camera then nobody will do it.

This is ridiculous on like 5 different levels.

---

**Anonymous • April 26, 2006 9:55 AM**

“No. Humans have a limited life span. Without any sane reason to be wasting time analysing hundreds of images so one can be passed off as coming from a particular camera then nobody will do it.”

Framing somebody else, obviously.

---

**Anonymous • April 26, 2006 10:03 AM**

*Without any sane reason to be wasting time analysing hundreds of images so one can be passed off as coming from a particular camera then nobody will do it.*

*The amount of effort required would be far less than any number of weird little hobby activities. And I can come up with a number of reasons to do it, most of which involve implicating someone in a crime.*

---

**jayh • April 26, 2006 10:18 AM**

100% of 9 cameras is not that significant. 9 different is a pretty easy target if you know the pic was from one of them. If you don’t know the pic was from one of them, or if you’re trying to assign a pic to one of 1000 or 10000 cameras it is a very different exercise.

---

**Zaphod • April 26, 2006 12:21 PM**

@jayh

Exactly right. The noise signature from nine cameras can be expected to be disparate -fairly unique and thus associating the images to one of the nine appears plausible.

If the set of cameras is large (think millions of cameras), it is probable that the noise signatures form a continuous spectrum (at least per CCD model) and the association between the noise signature from the sample images and any particular camera will be degraded as the number of matches within a certain tolerance will be large. Too large to be conclusive in a court of law

Zaphod

---

**RonK • April 26, 2006 2:20 PM**

@Tank

It’s trivial to forge this; you just have to extract the signature of the camera you want to appear to have taken the picture (which just involves running a computer program on a large number of images from that camera), and also calculating the signature of the camera which actually took the image, and subtract and add (or some other relatively easy pixel-by-pixel operations).

@jayh

Can I borrow your insignificant ability to guess a random integer between 1 and 9 correctly 2,700 times without error?

@Zaphod
The signature is a vector in N-dimensional space where N is the number of pixels in the camera sensor. If each dimension only had two possibilities, that would still leave a *lot* of room even if you wanted to classify every subatomic particle in the known universe.

Of course, there is probably a lot more overlap between two sample distributions at one pixel than between 0 and 1. But I wouldn't be at all surprised if every digital (CCD/CMOS) camera which will ever be manufactured until the heat death of the universe could have distinct signatures. There are a lot of pixels in those sensors.

---

**Benny • April 26, 2006 3:40 PM**

@RonK:

I don't think Zaphod was saying that cameras may have the exact same signature. Rather, I believe he was saying that given enough cameras, there may well be two (or more) whose signatures only differ by a small amount, small enough to be considered inconclusive in a court of law.

---

**Tank • April 26, 2006 7:47 PM**

@ Anonymous at April 26, 2006 09:55 AM
"Framing somebody else, obviously."

For what ? Photography without a permit ? Try to think just one step ahead here.

@ Anonymous at April 26, 2006 10:03 AM
"And I can come up with a number of reasons to do it, most of which involve implicating someone in a crime."

Don't be scared to name em.
Hey, why not draw on well over 100 years worth of history relating to non-digital photography and crime as a rich base for where people have been implicated in crimes by suggesting a particular camera was used rather than another particular camera…. in something… for some reason.

Nobody least of all me would be silly enough to suggest commenters on this blog couldn't come up with a convoluted and ridiculously implausible hypothetical security scenario just so they could agree with the blog's author. That's 95% of the posts here.

What I'm saying is there is NO practical implication here let alone an important one. It is pointless.

---

**Anonymous • April 27, 2006 6:01 AM**

WRT uses,

It could be intellectual property disputes, where somebody claims to have taken a picture with his/her camera when that is not the case. Somebody else cries in outrage. The signature in the disputed image and the alleged cameras is compared. The signature matches one of the cameras and not the other.

Some person has child porn pics in a HD. The signature on the pics matches a camera/phone that belongs that person.

Some person distributes illegal videos through a website or P2P system – beheadings, movie screenings , whatever. Once he is caught, the videos in question have signatures corresponding to camers in his property.

Or, any of the above where someone inserts the signature of your camera/phone in the pics/videos and then blows the whistle on you.

I agree, these might seem pretty lame, as the camera is not somehow biometrically paired with the person. But the same happens with weapons, and means to ID weapons are not considered useless.

The fact that you cannot think of an scenario does not mean that there is not one (Think early responses to the telephone and computers, which were miles off target).

---

**Tank • April 27, 2006 8:23 AM**

"Some person has child porn pics in a HD. The signature on the pics matches a camera/phone that belongs that person."

Did you consider what happens if nobody bothers to check the digital signature ?

You're talking about proving someone had 501kg of cocaine instead of 500kg. It's pointless.

You think there's someone caught with kiddie porn staring down a sentence who's banking on the guys in the yard with shivs caring whether your phone or someone elses was involved ?
Seriously WTF is the point ?

"It could be intellectual property disputes, where somebody claims to have taken a picture with his/her camera when that is not the case. Somebody else cries in outrage. The signature in the disputed image and the alleged cameras is compared. The signature matches one of the cameras and not the other."

Sorry, and I say this for the first time ever, but it's a post-9/11 world. Like that was the one day where uncredited photographs of unconfirmed sources could have won awards. And it's over.

Either way, there's physical entities involved that don't need filters and checksums run on them. The guy. The guy with the camera. The guy with the camera with the photo on it.

Stick the word "transcript" into google. Is all that material up for contention as to who was involved ?
You think a deep analysis of my lexicon will be the deciding factor in determining which of those speeches I delivered or does simple shit like "hey he looks nothing like FDR" and "don't you live on the other side of the world" going to be determining factors ?
The internet and digital image manipulation make many things possible. Physically being in front of stuff at a particular location and holding a camera are still the determining factors in who took particular pictures though. Pixel-to-pixel non-uniformity or not.

“Or, any of the above where someone inserts the signature of your camera/phone in the pics/videos and then blows the whistle on you.”

To who ? The cop who knows about this crap that isn’t even detectable in any commonly transmitted picture format ?
You’re in fantasy land.

“I agree, these might seem pretty lame, as the camera is not somehow biometrically paired with the person. But the same happens with weapons, and means to ID weapons are not considered useless.”

That’s because they are weapons.
Like I said, unless you’re in China and facing down a firing squad for being accused of photographing something in a slightly un-nationalistic way, cameras generally don’t lead to death. This kind of fetishism really isn’t necessary.

“The fact that you cannot think of an scenario does not mean that there is not one (Think early responses to the telephone and computers, which were miles off target).”

Actually I said YOU couldn’t think of one and rather than computers I referred you to the fact photographs aren’t new and you would have well over 100 years worth of incidents, anecdotes, news and recorded history to draw from.

The fact that you came up short does mean something. This. Is. Pointless.

Now get a name or take a hike.

---

**Jeremiah Blatz • April 27, 2006 10:38 AM**

@Tank

You’re being a fool. The fingerprinting thing, if it works correctly, can place a camera at the scene of a crime. Let’s take the kiddie porn example that you so glibly scoffed at. Say investigator Alice finds kiddie porn on the net and computes the noise signature. Say she suspects Bob as the source, but doesn’t have enough evidence. Now, Bob is smart, and doesn’t have any kiddie porn images lying around. It doesn’t matter. Alice gets ahold of the camera or images that are known to have come from that camera, and matches the noise signature. Boom, evidence! It’s not fingerprints on a smoking gun, but it is significant.

You can say that this is good or bad, but that’s largely a component of who Alice and Bob are, and what Bob allegedly did. (Shot kiddie porn, or attended a Falun Gong meeting in China.) But the fact of the matter is that this technique, if workable in the real world, is powerful and significant.

---

**Dugie • April 27, 2006 11:11 AM**

If someone take a pictures with any didital camera, when the picture is downloaded to a computer, you will get noise! When someone edits the picture in anyway, the software will add noise! And if the person is a pro, he or she will most likly be using editing software (photoshop) to enhance the picture, crop, scale, add noise recolor paintbrush, filters, and then reformat to be saved for the web (compression). So I don't know how this study would hold water in any case. This finding makes since if the RAW FILE is left on the orignal camera memory stick. Once it is moved to a computer it's gonna get noise ,and that would be all it would take to introduce doubt in any case.

And what happens if a picture is taken with a disposable camera and printed from a kiosk printer at a wolf camera store??? How do you prove that?

---

**Mark Lomas • April 27, 2006 11:24 AM**

History has a tendency to repeat itself.

CCDs are similar to solid-state memory. I understand that the Bell Labs researchers who invented them were originally researching memory devices.

Memory used to need refreshing or it would lose its state. Some processors (e.g. the Zilog Z80) had refresh registers that would scan through a range of addresses automatically refreshing the corresponding memory rows (in reality only 7 bits from the address). It turned out that if you repeatedly wrote certain values into the register, interfering with the refresh process, the memory cells discharged according to a pattern that varied between different memories.

This allowed me to write a program (circa 1979) that could distinguish between a number of supposedly identical Tandy TRS-80 computers. However, by its nature, it had the side effect of wiping most of the machines' memory.

I would imagine that many semiconductor devices can be distinguished if you know what to look for.

---

**Clive Robinson • April 27, 2006 11:45 AM**

@Dugie

"Once it is moved to a computer it's gonna get noise ,and that would be all it would take to introduce doubt in any case.
"

Unfortunatly for a criminal the fingerprint may have a statistical property that caries through all the normal events that a photographer might do.

For instance during processing the image intensity is taken down a few points by the software, however even though all pixel values have changed the relative difference between individual pixels may well have not.

Likewise a colour re-balence effects all the pixels in a similar way so again pixel to pixel relative difference might well be preserved.

In essence this was the holy grail of digital watermarking, and quite a bit of investigation was caried out as to how much distortion etc would go undetected by the human eye, but still alow the watermark to be detected.

In all cases digital watermarks failed when all the pixels where changed individually. This was however not true for filtering and other effects that effected all pixels in a known way.

The question then becomes how big a group of pixels is required to keep some level of statistic detectable.

---

**Madhu • April 27, 2006 8:21 PM**

I don't know all the details of the techniques used, but I do know something about signal processing, CCDs, and semiconductors in general. Semiconductor fabrication, like any other manufacturing process, is not perfect. There are variations in several variables, many of which can be measured reliably to distinguish different devices. A few that come to mind are leakage current and transfer functions such as gain, transconductance etc. In the early days of semiconductor fabrication, reliable devices were difficult to produce. Modern techniques have improved the art considerably, but it's far from perfect. Datasheets for discrete transistors list the variations of many parameters. Some parameters are more consistent than others. Design engineers are well aware of this, as are good carpenters, and choose design techniques that minimize the effects of variations on the finished product.

Given those facts, the identification problem can potentially be reduced to signal processing by applying a correlator. The important point is that as long as there is random noise and correlated information buried in that noise, it is possible to dig the information out, no matter how small it is. Random noise does not correlate, whereas systematic biases, such as leakage currents, do. Leakage current and gain varies from pixel to pixel and is *relatively* stable over some time scale significantly greater than the sample time. There are other potential fingerprints such as the linearity in the analog to digital converter (ADC) used to digitize the CCD output.

Can the "fingerprints" be wiped clean? Sure, but simple filtering isn't enough. Filtering just adds time to the correlation process. JPEG compression does muddy the waters, but it wasn't designed to eliminate the fingerprint. All it does is remove some signal and add some noise. More importantly, it's an equal opportunity function. It doesn't know anything about the image and doesn't really care.

Correlated variations are everywhere. Theoretically, one could use similar techniques to uniquely identify a radio or a computer sound card. An enterprising gambler made a lot of money by identifying biases in roulette wheels. His tool: Microsoft Excel. He was caught through correlation techniques as well. Casino owners are not fools. The nice thing about CCDs, and memories in general, there are millions of leakage currents that can be measured very quickly. This makes the job of correlation much easier.

I can imagine that some wheels are turning out there 🙂

---

**Myself • April 27, 2006 11:24 PM**

Dark-field subtraction is trivial, and is used all the time to eliminate "hot pixels" and "stuck pixels" from pictures before publication. Any photographer worth her salt would be doing this on every image, just to improve quality of output.

There's lots of software already out there for this. Take a look at Pixelzap for Windows. It would also be trivial to add a bogus noise signature back into an image, to make it appear to have come from a different camera. (Be sure to doctor the EXIF headers appropriately! The tool "jhead" can help with that.)

What baffles me is that anyone thinks this is news. Photographers have been dealing with it since the invention of the CCD. Whoever funded this “research” should be smacked.

---

**Tank • April 28, 2006 2:04 AM**

@ Jeremiah Blatz at April 27, 2006 10:38 AM
“You’re being a fool. The fingerprinting thing, if it works correctly, can place a camera at the scene of a crime. Let’s take the kiddie porn example that you so glibly scoffed at. Say investigator Alice finds kiddie porn on the net and computes the noise signature.”

No lets not. The internet is the reason image compression exists and is used as standard. That same compression is the reason she’s not computing any signatures for anything she finds on the net because it removes those signatures. Read the rest of the posts here.

“You can say that this is good or bad…”

I say it’s a non-event.

“But the fact of the matter is that this technique, if workable in the real world, is powerful and significant.”

No the fact is there are about 7 images on the net that don’t use compression and are able to have these highly sensitive pattern calculations done. Hence this isn’t workable in the real world since it doesn’t work on any other images using compression.

---

**nunyac • April 28, 2006 4:18 AM**

It seems to me that 9 cameras is not a very large sample for such a study. Unless the study proposes to show that 9 digital cameras having identical designs and sensor chips from the same semiconductor wafer will produce substantially different intrinsic images, then its conclusion may be questionable.
I have noticed that some digital cameras by default deliver an image file that has been translated into a “.jpg??? format. This is a lossy process that can replace a very significant portion of the original (from analog) data with parameters that will be used by an interpolation process to reconstruct the replaced part of the image at viewing time. The original “intrinsic image??? will not be recoverable form this part of a jpg encoded image.
nunyac

---

**Matthias Urlichs • April 29, 2006 7:34 AM**

“The limitation of the technique is that it requires either the camera or multiple images taken by the same camera, and isn’t informative if only a single image is available for analysis.”

That’s not a limitation, that’s just basic common sense. Like a real fingerprint, you need either the person, or more fingerprints by the same guy/gal, to get any meaningful data. The fact that the algorithm itself doesn’t work with more data, unlike a fingerprint duster, is irrelevant — you just store the raw image until then.

NB, I do wonder what JPEG compression will do to this idea — kill it, is my guess. Most images floating around the net aren't exactly compressed at a high-enough, details-preserving level.

---

**RADIOFLYER • June 19, 2006 4:28 PM**

TO BRANDON- 1984 HAS BEEN HERE LONG BEFORE 2001 IT STARTED IN WORLD WAR ONE, TWO, AND ALL OTHER WARS, AND MOST OF ALL, THIS ONE. WHERE THE GOVERNMENT HAS TAKEN AWAY OUR FREDOMS IN THE NAME OF "SECURITY" IF YOU GO BACK TO THE 1940'S AND LOOK AT OUR FREEDOMS THEN, AND COMPARE THEM WITH TODAY, IT WILL SCARE YOU.
THIS CAMERA TRACING, IS JUST ONE MORE STEP IN THAT DIRECTION, AND WHAT SCARES ME MOST IS THE GOVERNMENT USING IT TO CONVICT SOMEONE BY MAKING FALSE IMAGES.(HAVE YOU EVER HAD A POLICE REPORT, THEN READ IT. AND SEEN ALL THE "FALSE" STATMENTS THE POLICE ADD?)
OUR GOVERNMENT MONITORING ALL OF EVERYONES PHONE CALLS IS ANOTHER
AND NOW GETTING PROVIDERS TO GIVE THEM THE WEB SITES YOU GO TO, IS AGAIN ANOTHER.(I USE ANONYMOUSE.ORG ONLY NOW) IF BY PURE CHANCE, YOU END UP AT A CHILD PORNO SITE, YOU CAN NOW GO TO JAIL. INSTALLING TV CAMERAS IN NEW TV'S YOU BUY, SO AN IMAGE AND SOUND OF YOUR HOME CAN BE VIEWED, IS STILL AN OTHER.(I HAVE ONE WAY SAT. AND WILL NEVER HAVE CABLE WHICH IS TWO WAY) 1984? IT IS HERE MY FRIENDS, AND I BELIEVE WE HAVE NOW GONE PAST THE POINT OF NO RETURN.
NOTHING WE CAN DO NOW WILL BRING THEM BACK.
BUSH HAS "GOD" BEHIND HIM.

---

**joe90 • August 16, 2010 9:28 AM**

I do not know if this blog is still going, but anyway. Last night I saw a TV cop show where the criminal was caught by a digital photo fingerprint from his camera. He was a pro. photographer. Re fingerprint, if you took a photo, printed it then scanned it into your computer changed the format and size and then reprinted it I would have thought there would be no signature left.

---

**albert • August 24, 2016 3:41 PM**

@Mulder, @Mr. W,

I have a laser color printer. They can be used for counterfeiting since the toner sets on the surface of the paper, similar to the intaglio process used for printing currency. These printers use a lot of yellow toner, even when printing b/w. 🙂 The ID patterns are generated inside the printer. While it's possible, in theory, to 'copy' the pattern from a printed sheet, one would have to duplicate it on another similar printer in order to impersonate the original. You see the problem.

Using pale yellow paper won't work, because the pattern sits on the surface. I got dollars*-to-donuts that there are easy ways to discern the dot pattern from the paper: UV light, spectral analysis, whatever..

The real fun would be to hack the printer firmware, to eliminate the fingerprint, or, alter it (talk about a perfect frame). Just speculating, not advocating.

## It’s an interesting subject.

- real dollars:)

  . .. . .. — ....

Subscribe to comments on this entry

## Leave a comment

Login

**Name**

**Email**

**URL:**

□ **Remember personal info?**

**Fill in the blank: the name of this blog is Schneier on ___________ (required):**

**Comments:**

**Allowed HTML** <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> • <ul> <ol> <li> • <blockquote> <pre> **Markdown Extra** syntax via https://michelf.ca/projects/php-markdown/extra/

Preview Submit

← RFID Cards and Man-in-the-Middle Attacks

The Security Risk of Special Cases →