JPEGsnoop - Identifying Edited Photos

by Calvin Hass © 2009

Details regarding the use of JPEGsnoop to detect edited photos

Return to JPEGsnoop Main Page

Ever wondered if that UFO photo or sasquatch sighting is a fake? ... or if that camera manufacturer's sample images have been touched up?

Simply open an image in JPEGsnoop and scroll down to the section titled, `*** Searching Compression Signatures ***`. This option can be enabled/disabled with the `Signature Search` item in the Options menu.

The utility will compare the compression characteristics of the photo against an internal database of thousands of camera "signatures" to locate a match. If a match is found, the matching digital camera or editor is shown. If the signature matches a photo editor (such as Photoshop), then there is a good chance that the photo has been edited (i.e. not original!).

The assessment line indicates one of four possible outcomes:

- **Class 1 - Image is processed/edited**
- **Class 2 - Image has high probability of being processed/edited**
- **Class 3 - Image has high probability of being original** -- NOTE: Please see description below!
- **Class 4 - Uncertain if processed or original**

```
*** Searching Compression Signatures ***

  Signature:           01E5F053039A59A823FEDC91959822BF
  Signature (Rotated): 011B33BAEED0A54091895B8D5389FA91
  File Offset:         0 bytes
  Chroma subsampling:  2x1
  EXIF Make/Model:     OK   [Canon] [Canon EOS 10D]
  EXIF Makernotes:     OK
  EXIF Software:       NONE

  Searching Compression Signatures: (3327 built-in, 0 user(*) )

        EXIF.Make / Software        EXIF.Model                          Quality          Subsamp Match?
        ------------------------    ----------------------------------  ---------------  --------------
     CAM:[Canon                   ] [Canon EOS 10D                    ] [fine          ] Yes
     CAM:[Canon                   ] [Canon EOS 20D                    ] [fine          ] Yes
     CAM:[Canon                   ] [Canon EOS 300D DIGITAL           ] [fine          ] Yes
     CAM:[Canon                   ] [Canon EOS 30D                    ] [fine          ] Yes

  Based on the analysis of compression characteristics and EXIF metadata:

  ASSESSMENT: Class 3 - Image has high probability of being original
```

Image is Authenticated as very likely original

What is "Original"? How confident can we be?

It is virtually impossible for any software to ever guarantee with absolute certainty that a file or image has not been modified in some way. Even files that have an integrated cryptographic hash (eg. SHA-1 or MD5) could theoretically be altered to give a false positive integrity check, albeit unlikely. Apart from the use of cameras providing tightly-integrated authentication features (such as the Canon 1Ds / 1D mk II with the Data Verification Kit DVK-E1 / DVK-E2), it becomes a formidable task to prove that an image is guaranteed to be in its original, unaltered state. It is a much easier task to prove with certainty that an image has been processed / edited (ie. not original).

JPEGsnoop can be used with reasonable confidence in identifying "processed" images, but what can we draw from the tool's assessment that an "`Image has a high probability of being original`"? ... only that the JPEG compression "signatures" and certain metadata elements match those expected from the indicated camera model(s). Note that assessment "Image is Original" is not used, for this reason.

Is this sufficient information to **prove** that an image is "original"? In a word, no.

Important Note: For this, and related reasons, the **tool should not be used as direct evidence for legal investigations**!

It would take a very specialized set of tools to create a false positive "original" from an altered image. It is possible, and I have proven this in my own development. However, in most circumstances, it is highly unlikely that a set of JPEG analysis tools have been used to produce such a fabrication. Even if the compression signatures and metadata were altered carefully to match, there is an array of advanced image content analysis techniques (eg. statistical noise analysis, etc.) that could then be applied to further identify possible alterations.

In-Camera Editing
More interesting perhaps, is that some new digicams allow for a limited set of in-camera editing facilities. These digital cameras may allow for an externally edited photo to be brought back into the camera for resaving (via the editing functions). This mechanism may indeed enable an image to present all of the hallmarks of an "original" image (matching metadata and quantization tables), but bare no relationship to the original captured image.

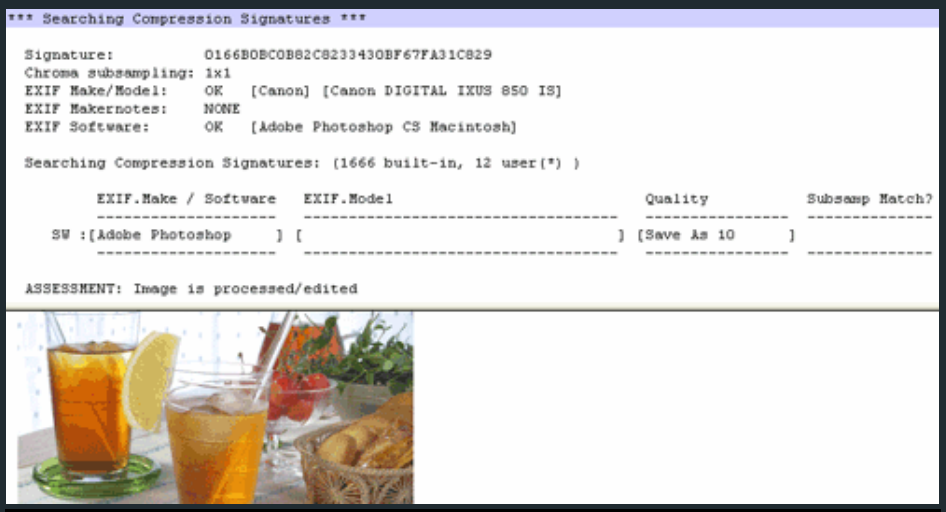
Video Frame Analysis
JPEGsnoop's image assessment functions are not designed to be performed on JPEG frames extracted from video files (eg. AVI MJPG). In most cases, these will report as "Processed/Edited".

Conclusions
Therefore, while JPEGsnoop cannot absolutely guarantee an image's authenticity, it can be used to indicate with reasonable probability that an image has not been modified. If authenticity must be "proven", further analysis methods would be required. On the other hand, disproving an image's authenticity is accomplished quite easily (provided that the original image camera's signatures have been captured in the database)

Images that are not "Original"
There are many reasons that images may be flagged as being likely "processed / edited", including: the image was altered in a photo-editing program (such as Photoshop), resized before emailing, re-compressed for submission to a website, or simply processed from another image source such as RAW. Note that RAW images are generally converted to JPEG (via ACR or other software) for general-purpose output. The fact that the camera itself didn't encode the JPEG image is what leads it to be marked as processed / edited. Of course converting from RAW does not necessarily mean that any modifications were made to the image content. Nonetheless, there is no way to prove that from the resulting JPEG, so it is marked as being "processed".

You would be surprised at how many images on the web are apparently original, but are quickly revealed as being edited / post-processed. For example, even some of the "Sample Images" on Canon's official website have been edited in Photoshop, using Save As quality 10. The following is one such example #3.

In this example, Canon may have simply enhanced the sharpness or increased the saturation, but one could easily see how it could be misused.



Canon's Sample Image example was edited!

Compression Signatures

Matching IJG Library Signatures
In some cases, JPEGsnoop may determine that the image's signature matches the digital fingerprint characteristic of IJG's compression quality scale. This scale is based on a formula that generates DQT tables based on a quality value from 1-100. The majority of image editors that provide a quality scale across this range use the same formula to generate their compression tables.

Once JPEGsnoop has determined a match, it will list out several known editors that use this particular scale, as they are all candidates and can produce the same signature.

Submit your own Compression Fingerprint / Signature!
While the built-in database includes thousands of signatures, not all digital cameras or software editors have been analyzed. If JPEGsnoop does not recognize the digicam or software editor, you have an opportunity to submit the compression signature to the JPEGsnoop database (stored on your computer and in the shared database).

If you know the origin of a file (i.e. you took a file direct from your digital camera, or the file is direct from saving within a photo editor / image processing program), then you are invited to submit the compression signature with the `Add Camera/SW to DB...` command. A dialog box will display the calculated compression signature unique to that file, along with a request for some additional details:

- What is the **source of the file**? Was it direct from your digital camera or has the file been processed / edited?
- The **name of the software** (e.g. Adobe Photoshop), if the file has been processed (i.e. no longer original).
- The **image quality setting**. In this field, you are requested to enter the quality setting (if you happen to know it). Digicams generally provide the user with a selection of up to three image quality modes (e.g. superfine, fine, normal). Similarly, if you have edited / processed a file with software, you are often given the choice of JPEG quality (e.g. high, medium, low, 70, etc.).

When submitting the compression signature to the database, no identifying information or image content is captured -- only the compression signature (a long series of digits) and setting info.

Local User Database

When you add a camera / editor to your database, it is included in all future searches for compression signatures when processing photos. If you want to modify or clear this list (for example, if you entered information that was invalid), then you can use the `Manage User DB` option.

JPEGsnoop stores the local user database (and configuration options) in the following location:
`<Profile Drive>/Documents and Settings/<User Name>/Application Data/JPEGsnoop/`

In Windows 95/98 (or in operating systems where the User Profiles haven't been configured), the data file is stored in the same directory as the executable.

Reader's Comments:

Please leave your comments or suggestions below!

Notify me of Page Updates
Notify me of New Comments

2019-09-30 natalie

Hello, I would like to know when the signature value will be different.

2019-03-11 Wolfgang Hugemann

Hi Calvin,

there are suggestions to detect double JPEG compression by looking at histograms of certain DCT coeficients. (You will easily find papers on this when searching for these key words.) Could you incorporate such histograms in JPEGsnoop? Do you know of any free software that can readily perform this job?

Kind regards
Wolfgang

Hi Wolfgang -- thank you for the suggestion. I have in the past considered additional DCT histogram reporting capabilities, but this could provide a useful application for it. I did locate one recent research paper discussing this in arxiv, but will need to spend some time to determine how much work might be involved. Of course I am always open to users creating a pull request on the JPEGsnoop github repo to introduce the basic prototype of such features, if this would interest you. As for other software with the feature, I'm not aware of them at this time. Thanks again Wolfgang for the interesting feature request.

2016-05-26 Andre

Hi!
How I can change compression signature of my Camera(Photo)?
Maybe exist the spacial programs that have Advanced settings of compression

Cameras will not let you change the compression "signature" directly -- instead, they will give you an option to select a different compression ratio for encoding / saving the images. A change in the compression ratio is one element that what will lead to a different signature. The signature is a value computed by JPEGsnoop and does not actually come from the camera itself. If one wanted to generate a very different compression signature (that didn't match any cameras), then one would need to force the JPEG encoder to use a different set of custom compression tables, but this is not something I have ever seen in a camera.

2016-01-13 steve

using an App called Uproov that takes a video or photo in App and locks it into the blockchain immediately meaning you can't manipulate the video and if you do it doesnt match its key indicating its a fake. a great tool for proving authenticity.

Steve, thanks for the pointer -- Uproov looks like it should be an interesting player in the image validation problem space. Canon (and presumably Nikon) addressed the problem by capturing an HMAC (hash) key in the image metadata ("Original Decision Data"). Unfortunately, once the keys were extracted from the camera hardware, the image authentication could be compromised (ie. it was possible to generate fake authentication data that would pass the OSK validation kit software).

From the little I have seen, it seems like applications such as Uproov might provide for a more robust strategy, given the foundation upon the bitcoin blockchain concept. While people can use ProofOfExistence.com to perform a similar record of their photos, having the digest generated at the time of image capture is a natural step and presumably more difficult to compromise.

2015-07-14 Key

All of my checks of my own pictures taken with my Nikon P510 get a Class 4 "Uncertain" rating. I also get "While the EXIF fields indicate original, no compression signatures in the current database were found matching this make/model". The "Searching Compression Signatures" section shows [NIKON] [COOLPIX P510] and [COOLPIX P510 V1.0] because I have added them in the past.
When I add my camera and software with [Tools->Add Camera to DB], shouldn't that add the P510's compression signature to the current database?

When you add cameras to the database, it adds it to the user database. What you are probably experiencing is

that the Nikon may use a number of different signatures (depending on camera settings and image content). Therefore, you may have added one of them in the past but the current image doesn't match a stored signature. For such cameras, it may take a few additions before they match all new images.

2015-07-14 Key

You told rc enriquez to check the "Signature" string in the "Searching Compression Signatures" section to tell if the same camera took various pictures. I took four pictures in about 2 minutes within 20 yards of each other with the same camera, and got four wildly different Signature values. What does this mean?

In all likelihood, the reason for the different signature values was that your camera uses variable quantization tables. Some cameras will use a multitude of different quantization tables to encode a photo, causing different signatures to be shown.

2015-01-14 Erkam

Hi Calvin,

First thanks for your previous responses. We have cited JpegSnoop in our orphaned jpeg fragment carving article. And, now, we are looking for new tracks about image fingerprinting.

So, I want to ask that what is the criterions while you are extracting image signatures?

Best regards

Hello Erkam -- first, congratulations on your research paper!

For image signature / fingerprinting, I am generating a cryptographic hash on a combination of the extracted DQT tables (could be several of them) and the chroma subsampling ratio.

The signature could be made more specific with other image metadata (eg. resolution) but I had decided against doing that at this stage.

All the best, Cal.

2014-02-27 Sergi Boix

Wow, I don't understand why your tool lies, for example, my flow, open RAW in viewNX, then open in PS for reveal to JPG, open ACR, reveal the RAW, the image is now in PS revealed, save to JPG and your tool says that image is processed /edited?

No, this is not true, my image is revealed from RAW, who are you to say is processed / edited? I shoot in RAW so I reveal my images. Do you want an example?

Thanks Sergi for your response... JPEG images converted from RAW are almost always marked as "processed" as the original image underwent processing to re-encode into JPEG. This does not necessarily mean that any editing has been done (hence the reason why "processed / edited" is used, as opposed to just "edited"). For example, images that are simply resized will also be marked as processed, even though the content may not have been altered in any way.

To help clarify this, I have updated the text on the page to draw attention to this point. I thought I had raised this important detail elsewhere, but it was worth making it more clear. Thanks for raising the question!

2014-02-23 Bob

Can you tell the location where a photo was taken? Example: June 23 2013 in Peoria Illinois USA

Nearly all cameras record the date & time that a photo was taken (based on the settings in the camera). Some cameras automatically record the GPS coordinates of where the photo was taken. To find the location, have a look for a section titled `EXIF GPSIFD`.

2013-04-12 LKJ

If a portion of a white background has been erased with an eraser tool using white and is undetectable to the naked eye, then some black text added over the erased area, then the image captured via print screen and saved, can this change be detected?

If print-screen were used to save a snapshot of the screen, then JPEGsnoop would only be able to determine that some software (eg. microsoft) was used to capture the final image. It would not be able to tell you any of the preceding changes that have occurred.

2013-03-11 rc enriquez

hi,

If i want to find out if the same camera was used to take 2 different photos, where should i compare? Sorry for my ignorance on this.

Generally, you would look at the section "*** Searching Compression Signatures ***". There, look for a numbered sequence after "Signature:". If both images have the same sequence, then there is a good chance that they were from the same camera.

2013-02-14 Sergio

Hello, Calvin! A very useful program!
Please tell us why the primary signature frames may differ from final frames video from a DVR? The video has not been edited.

Hi Sergio -- if I understand correctly, you are seeing a different quantization table associated with different frames exported from a MotionJPEG video. If so, this is not too uncommon as some video encoders attempt to optimize the compression rate between successive video frames. One reason to do this might be to attempt to restrict the overall video data rate. Some frames require higher compression rates to offset an increase in image complexity.

2012-10-05 Chris

Hi. I have just downloaded your program and have been checking out a few photos in it, but I do have a question for you.
If the assessment of the photo shows a Class 3, what does a line underneath the assessment mean that says "Note that EXIF Software Field is set (typically conatins Firmware version)"?
Thank you for your time and for this fantastic program!!!

What this means is that although everything in the image appears to be indicating that it is an original, the EXIF Software Field has some content. This field is usually by digital cameras to indicate the version of the encoder that is built into your camera. However, there are some photo editors out there that also modify this field to indicate what program was used. JPEGsnoop is not able to differentiate all of these differences, so it just reports it. Have a look at the EXIF Software field and if it looks like a photo editor, then there is reason to believe the image may have been altered in some way (might have been rotation, etc.).

2012-09-20 snooper

You can use the Matlab Jpeg Toolbox (a free GPL based software) to extract Huffman tables in Matlab...

Thanks for pointing out an alternative in Matlab!

2012-06-22 pad

Hey, this is a really clever tool, like some of the posters below i am trying to test for authentic images, it has been able to spot any photoshop edits as it returns a message like 'Photoshop IRB detected'...does it recognise any other image editing software yet?? ie imageready, gimp etc...thanks

Thanks! It does recognize other photo editing software through quantization tables and EXIF software tags. Photoshop adds its own markers that make it ever easier to detect.

2012-02-13 amer

how can i run jpegsnoop in matlab,
i only want huffmancode from images to test the neural network ,can anybody help me to give a solution for it .i only want to extract huffman code from images to test them.

2012-02-07 Faith

I also had the same issue as a previous poster--all of my images came up as class 1 edited, even those that haven't been edited at all. Some of these photos I tested came off of a website, and had identical analyses/compression signatures...could you shed some light on this?

Generally, most images that are posted on a website are automatically downsized from full-resolution to a more suitable resolution for web display. The act of resizing causes recompression and hence a new compression signature. Therefore, most images that you'll see posted on websites will likely appear to be "unoriginal". Are the images you're downloading full-resolution?

2011-06-21 Bern

I've just tried the software. It came back class 4. I have a cheapo camera (vivitar) - digicam click and go. I just want to be sure the picture I took really shows a ghost? How can I tell if its double exposure or something???? help

Although JPEGsnoop can help you tell if the image might have been direct from your Vivitar (and not edited), it won't tell you anything about what is in your image. In other words, it can't tell you if your image is a double-exposure or other things that may look suspicious :)

2011-05-08 Jamie

I have tested this on some of my photos, however everyone comes up as class 1 edited. All that I can think of is that when i changed the photo number or added a comment that says that the photo is edited. Is that the case? as none of the photos have actually been edited in any way??

Hi there Jamie -- It is possible that the "adding a comment" can cause an update to the files that leaves a trace of the software that let you add the comment (depends on the program). Some digital cameras generate files that may trigger a false-positive. This is especially the case with cameras on cellphones. If you send me an example file, I'll be able to take a look.

2011-04-27 User

I just want to tell you thanks, you have saved me of a couple of scams :)

Glad to hear it!

2011-02-05 Mark

Hi !
Well, I've tried JPEG snoop, and every image of mine that I've tested it on says Cat 1, even on those I have not in any way altered.

Any advice?

Hi Mark -- what camera make/model was used to take the photos? Note that the standard signature database does not include many camera phones so they will often be interpreted as modified (due to a hint from the "Software" tag string).

2010-11-17 Pablo

Calvin,

I'm working on my master's thesis regarding detecting alterations on digital images and I found JPEGsnoop very interesting in the field of digital ballistic based on quantization matrix of every camera and model.

I also found the work of H. Farid "Digital Image Ballistics from JPEG Quantization" about the same technique. In that paper he listed lots of cameras and models. Is that information already contained in JPEGsnoop?

My idea is that eventually we could have a default signature that can be validated and taken for granted for specific camera and model, alas NIST's signature DB for applications.

Hany Farid's articles are definitely worth a read, and very interesting. I don't think his quantization tables were published, so no, JPEGsnoop doesn't include those. However, I am sure that most of the cameras used in testing out his concepts have eventually been submitted to the JPEGsnoop main database.

I think it is a fantastic idea to have a fully-validated signature database. This has come up many times with my friends in the forensics field. The challenge is that it would probably require physical access to a large selection of digital cameras or some other means of truly validating the sample files.

I have considered adding a feature to JPEGsnoop that will allow users to load and save their own separate signature databases, which may help enable such a process. If you or anyone else is seriously interested in building a validated database, let me know and I can adjust JPEGsnoop to automate much of the process.

2010-11-03 b

Is your 'compression signature' the same as the 'Encoder Signature' that Jens Duttke has in his Photome app? If you are not familiar with Jens' work, you can see it here: http://www.photome.de/

No -- the signatures are not currently the same value, but they are probably generated in a similar way. Jens has done a fantastic job with PhotoME. I will followup to see if there is some way to bridge the gap between the different signature algorithms.

2010-11-03 Jeff

Great work. Since the project is open sourced, would you be able to provide some steps how to recompile the code into a .dll without any GUI? I have a need to use this to detect whether the photo is edited or not and need a simple method that returns yay or nay Can you point me in the right direction?

Hi Jeff -- Good idea. I have not experimented with building a DLL so it's best to file a feature request on the project page: hopefully someone who has had experience can see if it is a relatively easy change.

2010-10-29 urgentasap

Is there a way to identify photo which downloaded from facebook using jpegsnoop or other software? Which strings should we notice? I want to check whether the pic is original taken from camera or grab from other website? Please help me out. I really need your full support.

2010-10-16 Arindam

Dear Sir,

You have given a comment for Francisco's query made on 30-06-2009 which has been reproduced below:

"JPEGsnoop does not currently offer any methods to localize an image edit. However, there are several techniques available that can help determine where an image may have been modified: objective/statistical methods such as error level analysis, double-compression, replication detection, etc. and subjective methods such as lighting / highlight analysis, etc. I have plans to explore some of the objective methods in future releases of JPEGsnoop."

Can you please provide me the useful links of objective/statistical methods such as error level analysis, double-compression, replication detection, etc. and subjective methods such as lighting / highlight analysis, etc.at the above e-mail id.

I shall be obliged if you could provide links to other techniques also (if any).

Thanking You.

Arindam

Dr Neal Krawetz wrote up a great article on a number of these techniques. Please have a look at A Picture's Worth (PDF). There is a web-based ELA tool available at: ErrorLevelAnalysis.com.

2010-06-18 Angga

Oh yea! Thank's.
JPEGsnoop really helped me. it works well.

2010-06-06 annatjie

Hi

I have 3 photographs which was used to scam me. I do not know how to go about finding out who the person in the photographs is and whether there is a way to identify him, because it seems that it may be possible that they have been stolen and have been tampered with.

Is there any way you could help?

Thanks
Annatjie

2010-06-02 Thomas

Martine,

Il faut écrire les commentaires en anglais, c'est plus commode pour avoir une réponse de la communauté et en particulier de l'auteur.

A priori tu peux utiliser JPGsnoop pour reconnaitre si une image a été prise par un appareil photo ou logiciel (pour faire simple) car c'est écrit dans le fichier jpeg. Si l'image jpeg contient des traces de la sauvegarde d'un logiciel tu peux te douter que l'image a été modifié. Par contre tu ne peux pas savoir ce qui a été modifié.

Hi,
I answer to martine who ask if JPGsnoop can detect if a photo has been modified. So i explain to her that JPGsnoop can help her to know if the jpeg file was saved by a device or by a software so if a software was used we can bet the photo was edited.

Thomas

Merci beaucoup, Thomas!

2010-05-24 Martine

j'ai recu une photo, et j'aimerais savoir si elle a ete retouche et les corrections qu'elle a subi ... est-ce que le logiciel JPGsnoop peut m'aider.
je suis une neophite en la matiere, mais j'aimerais beaucoup apprendre.

2010-05-23 Gary

If during a court proceeding a person, who was ordered to produce a complete disk copy of the photos from his digital camera, deleted several of the shots and then reshuffles the JPEG and camera clock numbers in order to eliminate obvious numeric and time line evidence, would his action leave a forensic trace? If so, would your program detect this kind of tampering? In other words, if only the meta data was altered and not the visible content of the photograph, would this still be detectable?

Time and date alterations are generally outside the scope of what can be detected with these type of methods. Modifications to the image sequence number (in the filename) can be detected, provided that the camera recorded a copy of this sequence number in the EXIF metadata. Have a look in the metadata report for sequence numbering and the creation/digitization/capture timestamps -- in some cases you may be able to identify differences, but in general most people who go to lengths in hiding their edits will easily be able to align them all for consistency.

2010-05-17 Aline

Hello, according to information from the Internet, this program shows how the program edited the picture. I would like to know how to visualize that information and whether it is possible to visualize how it was before the image editing.

thankfully,
Aline

No -- this program doesn't show how an image was edited, only that it was edited. Other techniques (such as error level analysis) are pretty effective at helping identify which regions were edited.

2010-05-05 Dallasgoldbug

You mentioned "other software" would be needed to do more advanced analysis on images to locate the area of

tampering. Can you suggest one of them or point me in the right direction to learn more about the techniques used.

Thanks for your assistance.

One popular visual technique presented by Dr. Neal Krawetz is "Error Level Analysis". Someone has created an online Error Level Analyzer based on Neal's work.

2010-03-29 hal

Does this program tell us that which part of the photo has been edited as in co-ordinates? (x,y) If yes which part of the codes I can get it from?

Many Thanks

No. The program is not able to localize any edits -- that requires a completely different image analysis approach.

2010-03-23 PJ

Hi, Calvin.

I've got two questions:

1. I would like to reference a great response you gave me for a college paper I'm writing. May I do that, and how would you like it formatted; e.g., your name + website name + hyperlink...etc

2. I have been using Photoshop since version #5. I did an experiment to see what, if any, differences exist between CS2 and CS3 in the file sizes they save (I always retain my prior versions of software).

I have noticed, anecdotally, that CS3 tends to produce a smaller sized file than CS2. To make the tests equal, I scanned a color document into both versions and saved each one as a PSD file. The first thing I noticed was that CS3 produced a smaller-sized PSD file than CS2.

I then opened the CS3 file with CS2, and vice versa. I saved them again as PSD files and compared the results.

The CS2 file opened and saved in CS3 produced a smaller PSD file than the CS3 opened and saved in CS2.

I cannot account for the differences. What is CS3 doing that CS2 will not?

2010-03-21 Jules

I am a paranormal investigator and downloaded the software which is great, what worries me is if someone takes a photograph of a photograph of a printed out manipulated image of an alleged spook and claims it to be a ghost, how can I get around that? Get what I mean :S

Jules

Taking a digital photo of a printed photo will exhibit the signature of the camera taking the last digital photo. So, there is no way to get around this type of issue. However, it may be possible to detect the photo-of-a-photo through more advanced image content analysis, but it's quite dependent upon the quality of the print.

2010-02-27 vajira

Thank you so much for creating such an invaluable site and giving us the opportunity to get what we want. In fact I have been searching a methodology to idnetify fake images and I got to know about the JPEGSNOOP because of your page . Thank ever so much. I wish you good luck in everything you do and successfull future .

Thanks!

2010-02-26 Machiavelli

Your software is great. It has found 3 images to be of Class 1. These images are of a controversial world record. Would you mind taking a quick look at them for further insight (via email)? Thanks.

2010-01-25 dp

the question "is the photo digital?" means: if i have a printed photo and I scan it with a scanner (not with a camera) the Compression Signature can match the signature of a camera anyway?

No -- the compression signature will in fact match that of the scanner software instead.

2010-01-22 dp

what does it mean the column "Subsamp Match?"

if i have a list of cameras and software under Searching Compression Signature, does it mean that the photo has been taken/edited with any of these cameras/software? can i exclude others cameras/software?

is there a way to detect if a photo is a digital photo or it is a scanned photo (from a print or a film)? if i have some cameras under Searching Compression Signature, does it mean that the photo is certainly digital?

thanks

The "subsamp match" column indicates that the type of chroma subsampling used in the image matches the type associated with the signature entry in the database.

In general, the subsampling should match for the signature to be a reliable match.

The list of cameras and software under the signature search are all ones that have the same signature as the one identified in the image. It means that those other cameras and software tools could have also produced images with the same signature, not that someone used multiple cameras or software programs to produce the image.

However, with regards to your question: "is the photo digital"... By this I think you mean that someone took a photo with a digital camera of a scene versus taking a photo with a digital camera of a printed/film photo. One cannot tell this by the signatures alone.

2010-01-15 KEN

I received a picture as an e-mail attachment which has some parts of it deliberately blocked out, is there any way of unblocking or decoding this block so I can see the whole image?

I'm going to assume that the attachment was an image. Normally you won't be able to recover the blocked out regions. However, if the original image was a digital photo that was later edited, it is possible that the embedded thumbnail still reveals the original image (but at a smaller resolution). Therefore, within JPEGsnoop, you might try the "Search Forward" command to see if that is the case.

2010-01-01 Jane

If a photo is coming up Class 1 does that mean it was photoshopped or that is may just not be the original and its a copy.

This usually means that the image has been saved within an editor (such as Photoshop) and not simply a file copy. Whether anything was altered prior to the resaving is not determined.

2009-11-20 Dave

Hi i was wondering if i can pause a video then do a screen shot would that still be able to tell if a video of that time frame has been edited?

No, not with this type of technique. The act of taking a screen shot causes JPEG recompression to take place.

2009-10-19 john

If received a pic that has a class 1 that means it is a fake. a couple software programs came up when i used your program. paint photoshop etc. can u please tell me if i am right.

The list of programs that you see does not mean that someone used all of them to create the photo. It is simply telling you that the image has a signature that matches the signatures created by those programs. In other words, any one of those programs might have performed the last edit to the image (or another whose signature is not in the database yet). We can't tell if multiple programs have been used to produce an image, only what the last program to touch the image might have been.

2009-10-17 james

i ran a non edited photo through it and it said it was edited, which was not true

The process of identifying originality is not guaranteed as there is the potential for false positives -- after all, we're dealing with digital data that can be modified at will, without any form of cryptographic authentication. The scenarios that are most likely to trigger this are: a) RAW converted files (JPEGsnoop picks up on the conversion), b) files from very old digicams that don't use the makernote field.

If you can email me a copy of this image, I can provide more insight into the result or refine upcoming releases of the software. Thanks!

2009-10-14 shane

Is there a way to back out the editing.. or to tell what exactly was edited ?

Once a photo has been edited and resaved as a basic JPEG file (versus other file formats that provide layers and non-destructive editing), there is no way to undo the editing that has been performed. While JPEGsnoop can't localize the changed regions (it is more appropriate for an all-or-nothing indication), there are some other statistical analysis methods that can be used to highlight possible regions of edits (eg. error level analysis, etc.)

2009-09-22 marcos

excelente para los que deseamos aprender mas de la edician de imagenes Felicidades!

2009-07-21 John

I entered a signature from one of a series of photos I took. Only the photo that I entered the signature shows a status 3. Does each photo have to be entered into the local database?

Hi John -- No, you should only need to add the signature one time for each quality setting (normal, fine, superfine, etc.) that you intend to use on that camera model.

2009-07-08 ARTGAS

great software~~~ Any version for MAC??

Thanks! At the present time JPEGsnoop is only available for Windows. However, people have reported that it works fine using "wine" on LINUX / Mac.

2009-06-30 Francisco

Hi, if a photo is edited to make something in the image disappear, or in the case of ufo photo, insert the ufo into the photo, can I know exactly where in the photo were the alterations made?

JPEGsnoop does not currently offer any methods to localize an image edit. However, there are several techniques available that can help determine where an image may have been modified: objective/statistical methods such as error level analysis, double-compression, replication detection, etc. and subjective methods such as lighting / highlight analysis, etc. I have plans to explore some of the objective methods in future releases of JPEGsnoop.

Leave a comment or suggestion for this page:

Name:

Email: (**Never Shown** - Optional)

Comments:

Submit

NOTE: Image repair requests are not accepted. Thanks for your understanding.

Statcounter Visits!

Back to Top | Bookmark