

SENSOR FORENSICS: PRINTERS, CAMERAS AND SCANNERS, THEY NEVER LIE

Nitin Khanna[†], Aravind K. Mikkilineni[‡], Pei-Ju Chiang[‡], Maria V. Ortiz[†], Sungjoo Suh[†]
George T.-C. Chiu[‡], Jan P. Allebach[†], Edward J. Delp[†]

[†]School of Electrical and Computer Engineering

[‡]School of Mechanical Engineering

Purdue University

West Lafayette, Indiana 47907

ABSTRACT

Forensic characterization of devices is important in many situations such as establishing the trust and verifying authenticity of data and the device that created it. Current forensic identification techniques for digital cameras, scanners and printers are highly reliable due to the fact that each of these devices cannot escape inherent electro-mechanical properties which add “signatures” to the data they produce. In this paper we will describe the sensor forensics work going on at Purdue University. ²

1. INTRODUCTION

The falling cost and wide availability of electronic devices has led to their widespread use by individuals, corporations, and governments. These devices, such as computers, cell phones, digital cameras, and printers, all contain various sensors which generate data that is stored or transmitted to other devices. One example of this is a security system containing a network of video cameras, temperature sensors, alarms, computers, and other devices. In such a network, it is important to be able to trust the data from each of these sensors. Another use is to verify the source camera and authenticity of digital photographs in a court case or to identify a printer that was used to perform some illicit activity. Forensic techniques can be used to uniquely identify each device using the data it produces. This is different from simply securing the data being sent across the network because one is also authenticating the sensor that is creating the data. One technique that is used to authenticate a device involves embedding information, or a watermark, into the signal generated by the device. This strategy has potential problems in that the watermark could be attacked, allowing untrusted data to appear authentic.

¹This material is based upon work supported by the National Science Foundation under Grant No. CNS-0524540. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. Address all correspondence to E. J. Delp at ace@ecn.purdue.edu.

²<http://www.sensor-forensics.org/>

Identification through *forensic characterization* means identifying the type of device, make, model, configuration, and other characteristics of the device based on observation of the data that the device produces[1]. The characteristics that uniquely identify the device are known as *device signatures*, which can be classified as *intrinsic* and *extrinsic*. The *Intrinsic signature* represents artifacts that are due to optical, electrical, or mechanical limitations of the device. For instance, the noise characteristics in a digital image can be used as a signature of the camera which produced it. Similarly, the “noise” characteristics of a print engine can be used as a signature of the printer that generated a document. Because they are tied to specific features of the hardware, intrinsic signatures are distinctly different from watermarks that are embedded in the image file, or tags that are attached to it as metadata. The extrinsic signature is generated by modulating the process parameters according to a specified pattern that may encode the serial number of the sensor or other information. In the following sections we show how these signatures can be used to identify the device by using signal analysis tools on output produced by the device.

2. IMAGE CAPTURE DEVICES

Three main sources of digital images are digital cameras, scanners, and computer software such as Adobe Photoshop. A digital image can originate from a single source or it can be a mosaic made by combining images from multiple sources. An image generated by merging a digital photo of a person with a background generated in Photoshop is an example of an image belonging to a mixed class; cameras + computers. Similarly, other classes of forged images exist.

There are various levels at which the image source identification problem can be solved. One may want to find the particular device (digital camera or scanner) which generated the image or one might be interested in knowing only the make and model of the device.

The basic structure of a digital camera pipeline can be seen in Figure 1. First, light from a scene enters the camera

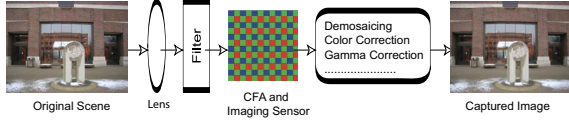


Fig. 1. Imaging Pipeline for a Digital Camera

through a lens and passes through a set of filters including an anti-aliasing filter. Next the light is “captured” by a sensor. These sensors, typically CCD or CMOS imaging sensors, are color blind in the sense that each pixel captures only intensity information. To capture color information, the light first passes through a color filter array (CFA) which assigns to each pixel of the sensor one of three (or four) colors to be sampled. The individual color planes are filled in by interpolation using the sampled pixel values. Next, a number of operations are performed by the camera which include white point correction and gamma correction. The image is then written into the camera memory in a user-specified image format (e.g. RAW, TIFF or JPEG). The details of the algorithms used at each stage vary between digital cameras of different makes and models, but the basic structure remains same. This variation from one camera model to another can be used to identify the camera used to acquire an image.

The basic imaging pipeline for scanners is similar to that for digital cameras. The difference is that the imaging sensor in a scanner is a one dimensional array whereas in a digital camera it is a two dimensional grid. The document is placed in the scanner and the acquisition process starts. A cold cathode fluorescent lamp (CCFL) or xenon lamp is used to illuminate the document. Using a stabilizer bar, a belt, and a stepper motor, the scan head slowly translates linearly to capture the image. The scan head includes a set of lenses, mirrors, a set of filters, and the imaging sensor. Most desktop scanners use charge-coupled device (CCD) imaging sensors. Other scanners use CMOS (complementary metal oxide semiconductor) imaging sensors, Contact Image Sensors (CIS), or PMTs (photomultiplier tube). The number of elements in the linear sensor determines the horizontal optical resolution. The step size of the motor controlling the scan head dictates the vertical resolution.

The manufacturing process of imaging sensors introduces various defects which create noise in the sampled pixel values. Because this noise is directly related to manufacturing defects, which can vary from one sensor to another, it can be used to forensically characterize a digital camera or scanner. There are two types of noise. The first type of noise is caused by array defects. These include point defects, hot point defects, dead pixels, pixel traps, column defects and cluster defects. These defects cause pixel values in the image to deviate greatly. For example, dead pixels show up as black in the image and hot point defects show up as very bright pixels in the image, regardless of image content. The second type of noise

is pattern noise which refers to any spatial pattern that does not change significantly from image to image. Pattern noise is caused by dark currents and photoresponse nonuniformity noise that vary from pixel to pixel due to differences between pixels such as detector size, doping density, spectral response, thickness in coatings and other imperfections created during the manufacturing process.

2.1. Intrinsic signatures for image capture devices

In [2], it is shown that defective pixels can be used for reliable camera identification even from lossy compressed images. This type of noise, generated by hot or dead pixels, is typically more prevalent in cheap cameras. The noise can be visualized by averaging multiple images from the same camera. These errors can remain visible after the image is compressed. However, many cameras post-process the captured image to remove these types of noise, so this technique cannot always be used.

In [3], a different approach, based on sensor pattern noise, is used to address the problem of camera identification from images. The identification is based on pixel non-uniformity noise, which is a unique characteristic for both CCD and CMOS based cameras. The high frequency part of the pattern noise is estimated by subtracting a denoised version of an image from the original image. The camera’s reference pattern is determined by averaging the noise patterns from multiple images taken with the camera. This reference pattern serves as an intrinsic signature of the camera. To identify the source camera of a given image, the noise pattern from the image is correlated with known reference patterns from a set of cameras. This approach is shown to provide correct source camera identification between a set of 9 cameras without a single misclassification over several thousand images [3]. It is also possible to perform reliable identification from images that have been JPEG compressed and/or resized, as well as to distinguish between images taken by two cameras of the same model.

The methods of device identification discussed above for digital cameras are also applicable to digital scanners. In [4], the use of imaging sensor pattern noise for source scanner identification is presented. Since the scanned image is generated by a linear sensor array translated across the object, sensor noise is expected to have a periodic structure along the scan direction. A linear row reference pattern is used for scanner identification instead of a two dimensional array reference pattern used for source camera identification. The average of all the rows of the sensor noise is found. Statistical features are obtained from this average row including the first and higher order statistics (such as mean, variance, kurtosis and skewness). Similar statistics are extracted from the correlations of this average row with all the other rows. Similar features are also extracted from columns of the sensor noise. A 16 dimensional feature vector is created using these ex-

tracted features from each image. The statistical feature vector based method is shown to give an average classification accuracy of 96% between four scanners (two of which are the exact same model). Experiments were also performed to verify the effectiveness of proposed scheme for JPEG compressed images. The statistical feature vector based method is more promising than correlation based methods used for source camera identification because of almost unavoidable desynchronization in scanned images. In contrast to correlation based method in which reference pattern was obtained by averaging sensor noise over multiple training images, in feature vector based method there is no averaging over multiple images and thus the desynchronization problem is avoided. Further work is under progress to develop methods which will be completely robust to the section of the scanner from which images are scanned. We are also developing methods to work for heavily sub-sampled images like those scanned at 200dpi.

In order to effectively work, the type of device that created an image must be known in order to choose the proper forensic analysis method to use. In [5], the imaging sensor pattern noise was used to group digital images into one of two classes based on their originating device: a scanner or digital camera. This scheme utilized the difference in the geometry of the imaging sensors and demonstrated promising results with an average classification accuracy of approximately 90% for images scanned at the native resolution of the scanners.

3. IMAGE OUTPUT DEVICES

Among the various types of image output devices, printers produce a permanent record that can form the basis for subsequent extraction of an intrinsic signature. Today there are two primary technologies for desktop printers – electrophotographic (usually laser) and inkjet. The very same features that give rise to an intrinsic signature for these devices may also cause visible and unacceptable image artifacts if they are not properly controlled.

Figure 2 shows a side view of the cartridge for a typical EP printer. The print process has six steps. The first step is to uniformly charge the optical photoconductor (OPC) drum. Next a laser scans the drum and discharges specific locations on the drum (exposure). The discharged locations on the drum attract toner particles (development) which are then attracted to the paper which has an opposite charge (transfer). Next the paper with the toner particles on it passes through a fuser and pressure roller which melts and permanently affixes the toner to the paper. Finally a blade or brush cleans any excess toner from the OPC drum.

In EP printing, artifacts are created in the printed output due to electromechanical imperfections in the printer such as fluctuations in the angular velocity of the OPC drum, gear eccentricity, gear backlash, and polygon mirror wobble. In previous work we have shown that these imperfections are di-

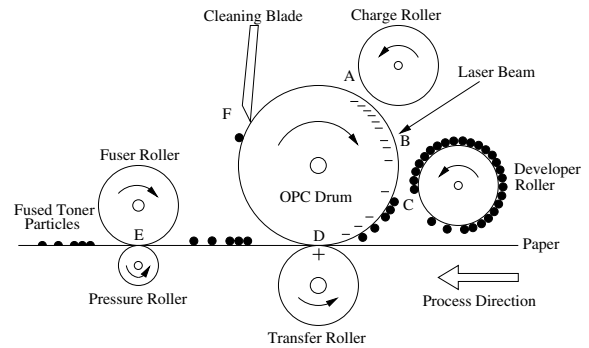


Fig. 2. Diagram of the EP Process: (A) charging, (B) exposure, (C) development, (D) transfer, (E) fusing, (F) cleaning

rectly related to the electromechanical properties of the printer. This property allows the corresponding fluctuations in the developed toner on the printed page to be treated as an intrinsic signature of the printer. The most visible print quality defect in the EP process is banding, which appears as cyclic light and dark bands.

Techniques that use banding in electrophotographic (EP) printers as an intrinsic signature to identify the model and manufacturer of the printer have been reported in [6]. It is shown that different printers have different sets of banding frequencies which are dependent upon brand and model. This feature is relatively easy to estimate from documents with large midtone regions. However, it is difficult to estimate the banding frequencies from text. The reason for this is that the banding is present in only the process direction and in printed areas. The text acts as a high energy noise source upon which the low energy banding signal is added.

One solution which was previously reported in [7] is to find a feature or set of features which can be measured over smaller regions of the document such as individual text characters. If the print quality defects are modeled as a texture in the printed areas of the document, then texture features can be used to classify the document. These types of features can be more easily measured over small areas such as inside a text character. The approach in [7] was based on texture measures estimated from the graylevel co-occurrence matrix (GLCM) generated from the printed region of the text characters. A support vector machine (SVM) is then used to select the printer most likely to have printed the page. Each text character that is processed in the document casts a vote for the most likely printer and the majority vote is taken as the final decision. This framework provides very robust performance.

3.1. Extrinsic signatures for imaging devices

The very same features that provide an intrinsic signature for an imaging device can be modulated from within the device

to embed auxiliary information in the image data. Extrinsic signatures are distinctly different from watermarks that are embedded in the image file, or tags that are attached to it as metadata, since they are embedded at the hardware level. This makes the control of these signatures much less accessible to the user, and thereby more difficult to tamper with or “hack”.

In [8, 9, 10], the capability to embed extrinsic signatures on text, forms, and halftoned images in EP printers is demonstrated. We have investigated two different embedding approaches. One utilizes the effect of laser intensity on dot size to modulate the dot size in a predefined pattern or code. The other exploits the halftoning algorithm by shifting a set of dots in a halftone cell by a predetermined pattern. Depending on the content of the image, such as text or halftone, a different encoding schemes is chosen. The problem is modeled as a communication channel, where channel noise characteristics and capacity are coupled and in which channel and data coding approaches can be employed. It is shown that with proper system control, coding and image analysis, it is possible to embed 250 bits of data in a full page letter sized document with 12 point font. For halftoned images, a data capacity of 5 bits for every quarter of an inch is achievable. Preliminary studies have shown similar results for forms.

4. CONCLUSION

Forensic characterization of devices is important in many situations today and will continue to be important for many more devices in the future. We have presented an overview of current characterization techniques for digital cameras, scanners and printers. All these techniques identify the device with high reliability due to the fact that the features used for identification are tightly coupled with the electro-mechanical aspects of the device.

5. REFERENCES

- [1] Nitin Khanna, Aravind K. Mikkilineni, Anthony F. Martone, Gazi N. Ali, George T.-C. Chiu, Jan P. Allebach, and Edward J. Delp, “A survey of forensic characterization methods for physical devices,” *Digital Investigation*, vol. 3, pp. 17–28, 2006.
- [2] Zeno J. Geradts, Jurrien Bijhold, Martijn Kieft, Kenji Kurosawa, Kenro Kuroki, and Naoki Saitoh, “Methods for identification of images acquired with digital cameras,” in *Enabling Technologies for Law Enforcement and Security*, Simon K. Bramble, Edward M. Carapezza, and Lenny I. Rudin, Eds. 2001, vol. 4232, pp. 505–512, SPIE Press.
- [3] Jan Lukas, Jessica Fridrich, and Miroslav Goljan, “Detecting digital image forgeries using sensor pattern noise,” in *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VIII*, San Jose, CA, January 2006, vol. 6072.
- [4] Nitin Khanna, Aravind K. Mikkilineni, George T.-C. Chiu, Jan P. Allebach, and Edward J. Delp, “Scanner identification using sensor pattern noise,” in *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX*. 2007, SPIE, to appear in.
- [5] Nitin Khanna, Aravind K. Mikkilineni, George T.-C. Chiu, Jan P. Allebach, and Edward J. Delp, “Forensic classification of imaging sensor types,” in *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX*. 2007, SPIE, to appear in.
- [6] Gazi N. Ali, Pei-Ju Chiang, Aravind K. Mikkilineni, George T.-C. Chiu, Edward J. Delp, and Jan P. Allebach, “Application of principal components analysis and gaussian mixture models to printer identification,” in *Proceedings of the IS&T’s NIP20: International Conference on Digital Printing Technologies*, Salt Lake City, UT, October/November 2004, vol. 20, pp. 301–305.
- [7] Aravind K. Mikkilineni, Osman Arslan, Pei-Ju Chiang, Roy M. Kumontoy, Jan P. Allebach, George T.-C. Chiu, and Edward J. Delp, “Printer forensics using svm techniques,” in *Proceedings of the IS&T’s NIP21: International Conference on Digital Printing Technologies*, Baltimore, MD, October 2005, vol. 21, pp. 223–226.
- [8] Pei-Ju Chiang, Aravind K. Mikkilineni, Osman Arslan, Roy M. Kumontoy, George T.-C. Chiu, Edward J. Delp, and Jan P. Allebach, “Extrinsic signature embedding in text document using exposure modulation for information hiding and secure printing in electrophotography,” in *Proceedings of the IS&T’s NIP21: International Conference on Digital Printing Technologies*, Baltimore, MD, October 2005, vol. 21, pp. 231–234.
- [9] A. K. Mikkilineni, P.-J. Chiang, S. Suh, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, “Information embedding and extraction for electrophotographic printing processes,” in *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VIII*, San Jose, CA, January 2006, vol. 6072.
- [10] Sungjoo Suh, Jan P. Allebach, George T.-C. Chiu, and Edward J. Delp, “Printer mechanism level data hiding for halftone documents,” in *Proceedings of the IS&T’s NIP22: International Conference on Digital Printing Technologies*, Denver, CO, September 2006, pp. 436–440.