A Survey of Forensic Characterization Methods for Physical Devices

By

Nitin Khanna, Aravind Mikkilineni, Anthony Martone, Gazi Ali, George Chiu, Jan Allebach and Ed Delp

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2006 USA

Lafayette, IN (Aug 14th - 16th)

available at www.sciencedirect.com

journal homepage: www.elsevier.com/locate/diin

A survey of forensic characterization methods for physical devices☆

Nitin Khanna[a,*], Aravind K. Mikkilineni[a], Anthony F. Martone[a], Gazi N. Ali[a], George T.-C. Chiu[b], Jan P. Allebach[a], Edward J. Delp[a]

[a]School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907, USA
[b]School of Mechanical Engineering, Purdue University, West Lafayette, IN 47907, USA

Keywords:
Device forensics
Camera identification
Printer identification
RF device identification

A B S T R A C T

This paper describes methods for forensic characterization of physical devices. This is important in verifying the trust and authenticity of data and the device that created it. Current forensic identification techniques for digital cameras, printers, and RF devices are presented. It is also shown how these techniques can fit into a general forensic characterization framework, which can be generalized for use with other devices.

1. Introduction

The falling cost and wide availability of electronic devices have 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 are stored or transmitted to another device. 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. 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 we are 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.

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 (Martone et al., 2006). The characteristics that uniquely identify the device are called *device signatures*.

There are many scenarios in which it is useful to characterize a device. One use is to verify the source camera and authenticity of digital photographs in a court case. Another would be to identify a printer that was used to perform some illicit activity. For instance, the noise characteristics in a digital image can be used as a signature of the camera that produced it. Similarly, the ''noise'' characteristics of a print engine can be used as a signature of the printer that generated a document. For an RF device, such as a cell phone, the radiation re-emitted after excitation from an external RF pulse

☆ Parts of this research were supported by a grant from the National Science Foundation under Award Number 0219893, and by the U.S. Army Research Office as a Multi-disciplinary University Research Initiative on Standoff Inverse Analysis and Manipulation of Electronic Systems under grant number W911NF-05-1-0337.

* *Corresponding author.*
E-mail addresses: khannan@ecn.purdue.edu (N. Khanna), amikkili@ecn.purdue.edu (A.K. Mikkilineni), amartone@ecn.purdue.edu (A.F. Martone), alig@ecn.purdue.edu (G.N. Ali), gchiu@ecn.purdue.edu (G.T.-C. Chiu), allebach@ecn.purdue.edu (J.P. Allebach), ace@ecn.purdue.edu (E.J. Delp).

1742-2876/$ – see front matter © 2006 DFRWS. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2006.06.014

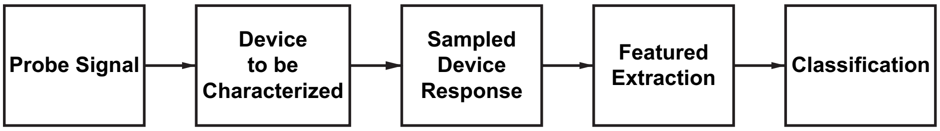


Fig. 1 – Device characterization framework.

contains characteristics that are unique to each device's make and model.

This paper presents a framework for forensic characterization. Current characterization techniques for digital cameras, printers, and RF devices are presented in relation to the proposed framework.

A block diagram of a general forensic characterization system is shown in Fig. 1. A device to be characterized is first excited by a specially designed "probe signal". For a printer or camera, this signal might be a specially designed test page to be printed or photographed. The device response would then be a print or digital image. For an RF device or other sensor, the probe signal might be a specially designed RF pulse sent toward or through the device. The pulse will interact with the device and be re-emitted. In this case, the re-emitted signal would be the device response.

The device response is sampled and a set of features are extracted from the sampled signal. These features are then used to determine various information about the device using standard classification techniques.

2. Characterization of digital cameras

In contrast to the analog world, where the depicted event in a photograph has generally been accepted as reality, the authenticity of digital images cannot be taken for granted. This is especially true when it comes to legal photographic evidence. Digitization of data, along with the availability of digital processing tools, has made creation and manipulation of digital images an easy task. As digital images and video continue to replace their analog counterparts, the importance of reliable, inexpensive, and fast identification of authenticity and origin of digital images increases. Reliable digital camera identification would especially prove useful in the court. For example, the identification could be used for establishing the origin of images presented as evidence, or one could prove that a certain image has been obtained using a specific camera and is not a computer-generated image. Therefore, a reliable and objective way to examine image authenticity is needed.

Not only is the general public rapidly replacing classical analog cameras (film) with digital cameras, law enforcement agencies are doing so as well. Agencies are increasingly relying on digital photography to create a visual record of crime scenes, physical evidence, and victim's injuries. One reason for this is that a digital camera gives the photographer immediate visual feedback of each picture taken. Digital images can be readily shared using computer networks and conveniently processed for queries in databases. Also, properly stored digital images do not age or degrade with usage. On the other hand, thanks to powerful editing programs, it is very easy even for an amateur to maliciously modify digital media and create realistic looking forgeries. Forensic tools that help establish the origin, authenticity, and the chain of custody of digital images are essential to the forensic examiner. These tools can prove to be vital whenever questions of digital image integrity are raised.

Image forensics is concerned with the following questions:

- Is this an "original" image produced by a digital camera, or is it a computer-generated image? Was it created by cut and paste operations from multiple images?
- Was this image captured by a camera manufactured by vendor X or vendor Y? Did this image originate from camera X? at time Y? at location Z? Is reliable identification possible from processed images?
- Has this image been modified?
- Was this image manipulated to embed a secret message? Is this image a stego-image or a coverimage?

There has been some effort in the digital watermarking community to embed watermark in the captured image that would carry information about the digital camera such as a time stamp, or even biometric of the person taking the image (Blythe and Fridrich, 2004). This technique only works if all digital cameras implement it, which is not the case currently, and will probably not change in the near future. The application of this watermarking solution is mostly limited to a closed environment such as "secure cameras" used by forensic experts taking images at crime scenes (Blythe and Fridrich, 2004). Under these controlled conditions, the secure cameras can provide a solution to the problem of evidence integrity and origin. Another issue is that there is no completely secure authentication watermarking algorithm that can survive all attacks. Also the hardware system has to be secured from unauthorized watermark embedding. In the absence of widespread adoption of digital watermarks, it is important to develop techniques that can help make statements about the origin, authenticity and nature of digital images.

There are various techniques by which the source camera of an image can be determined. Some techniques are simple and straightforward. For example, the EXIF headers of most digital still camera images contain information about the camera type and the conditions under which the image was taken (e.g., exposure, time). Additional information can be obtained from the quantization table in the JPEG header (some cameras use customized quantization matrices). This header data, however, may not be available if the image is converted to a different format, and can easily be removed or modified.

To overcome these problems, techniques that use only features that are intrinsic to the camera itself need to be used. The following three sections describe the workings of a digital camera, as they relate to second and third blocks of the device characterization framework in Fig. 1. Then, techniques for

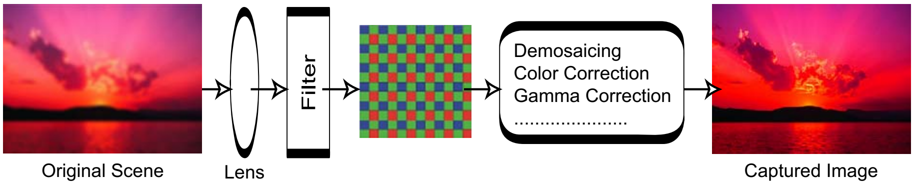


Fig. 2 – Image acquisition.

identifying the source camera of a digital image, using only intrinsic features, are presented.

2.1. *Imaging pipeline*

The imaging pipelines of digital cameras are similar, irrespective of manufacturer or model. The basic structure of a digital camera pipeline can be seen in Fig. 2.

First, light from a scene enters the 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 from the light hitting it. To capture color information, the light first passes through a color filter array (CFA), which assigns each pixel on the sensor to one of the three (or four) colors to be sampled. Shown in Fig. 3 are CFA patterns using RGB and YMCG color spaces, for a 4 × 4 block of pixels. The individual color planes are filled in by interpolation using the sampled pixel values. There are a number of different interpolation algorithms, which could be used, and different manufacturers use different interpolation techniques.

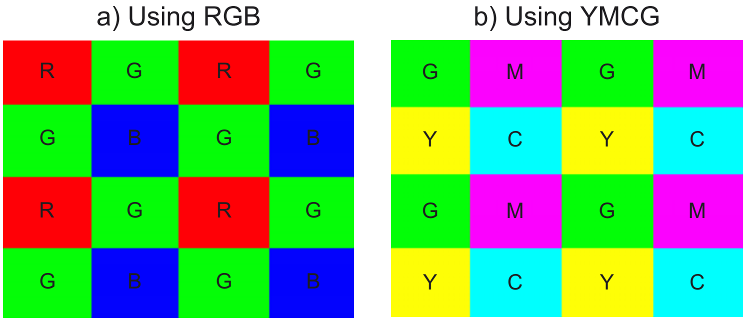
Finally, a number of operations are performed by the camera, which include, but are not limited to, color interpolation, white point correction and gamma correction. The image is then written into the camera memory in a user-specified image format (e.g., RAW, TIFF or JPEG). Although the operations and stages explained in this section are standard in a digital camera pipeline, the exact processing details in each stage vary from one manufacturer to another, and even between different camera models from the same manufacturer. This variation from one camera model to another can be used to determine the type of camera that a specific image was taken with.

2.2. *Sensor noise*

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. There are two types of noise that are important to understand the following sections.

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.

Pattern noise refers to any spatial pattern that does not change significantly from frame to frame and is caused by dark currents and photoresponse nonuniformity noise (PRNU). Dark currents are stray currents from the sensor substrate into the individual pixels. This varies from pixel to pixel and the variation is called fixed pattern noise (FPN). FPN is due to differences in detector size, doping density, and foreign matter trapped during fabrication. PRNU is the variation in pixel responsivity and is seen when the device is illuminated. This noise is due to variations between pixels such as detector size, spectral response, thickness in coatings and other imperfections created during the manufacturing process. The power spectrum of the PRNU is continuous (Holst, 1998) with slightly attenuated high spatial frequencies. Frame averaging will reduce all the noise sources except FPN and PRNU. Although FPN and PRNU are different, they are sometimes collectively called scene noise, pixel noise, pixel nonuniformity, or simply pattern noise.



a) Using RGB

R	G	R	G
G	B	G	B
R	G	R	G
G	B	G	B

b) Using YMCG

G	M	G	M
Y	C	Y	C
G	M	G	M
Y	C	Y	C

Fig. 3 – CFA patterns.

2.3. Image acquisition model

The raw signal that is captured by the sensor due to incoming light (if no sources of noise are present) is represented by matrix $\mathbf{x} = (x_{ij})$, $i \in \{1,2,\ldots,m\}$, $j \in \{1,2,\ldots,n\}$, where $m \times n$ is the sensor resolution. A general model

$$y_{ij} = \eta_{ij}(x_{ij} + \epsilon_{ij}) + \xi_{ij} \tag{1}$$

can be written, where $\mathbf{y} = (y_{ij})$ represents the digitized output of the sensor before any other camera processing occurs. The factors η_{ij} are close to 1 and capture the PRNU noise, which is a multiplicative noise. After removing the low frequency component, the pattern noise component can be used as an intrinsic characteristic (fingerprint) of the sensor. The PRNU noise is not present in completely saturated areas of an image where all sensor pixels produce a constant maximum signal. It is also clear from Eq. (1) that in very dark areas (when $x_{ij} \approx 0$) the PRNU noise is largely suppressed.

The signal $\mathbf{y}$ goes through a chain of complex processing before the final image file is stored on the camera's memory card. This processing includes neighborhood operations such as demosaicing, color correction, and kernel based filtering. Some operations may be nonlinear in nature, such as gamma correction, white point correction, or adaptive color interpolation (Lukas et al., 2006). The final pixel values

$$p_{ij} = \Psi(y_{ij}, N(y_{ij}), i, j) \tag{2}$$

are assumed to be in the range [0, 255] for each color channel. Ψ is a nonlinear function of y_{ij}, the pixel location (i, j), and values $\mathbf{y}$ from a local neighborhood $N(y_{ij})$. This function is heavily dependent on the camera model or manufacturer-specific image processing algorithms used in different stages described earlier.

2.4. Sensor-based characterization

One approach to camera identification is through analysis of pixel defects. Geradts et al. (2001) point out that defective pixels, such as hot pixels or dead pixels, can be used for reliable camera identification even from lossy compressed images.

This type of noise is typically more prevalent in cheaper cameras than in more expensive ones. The noise can be visualized by averaging multiple images from the same camera. These errors remain visible even after the image is compressed by the camera.

This approach fails for cameras that do not contain any defective pixels or cameras that eliminate defective pixels by post-processing their images on-board. Also, the defective pixels may not be obvious in every scene. In order to identify the defective pixels, one either needs to have access to the camera or have sufficiently many images from which the defective pixels can be determined.

In Lukas et al. (2005) and Digital bullet scratches for images (2005), a different approach, based on sensor pattern noise, is presented to the problem of camera identification from images. The identification is based on pixel nonuniformity noise, which is a unique stochastic characteristic for both CCD and CMOS-based cameras. The presence of this noise is established using correlation as in the detection of spread spectrum watermarks. Reliable identification is possible even from images that are resampled and JPEG compressed.

The pattern noise is caused by several different factors, such as pixel nonuniformity, dust specks on optics, interference in optical elements, dark currents, etc. The high frequency part of the pattern noise is estimated by subtracting a denoised version of an image from the original image. This is performed using a wavelet-based denoising filter described in the work by Mihcak et al. (1999). A camera's reference pattern is determined by averaging the noise patterns from multiple images taken with that 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. If the correlation is above a certain threshold for one of the reference patterns, then the camera corresponding to

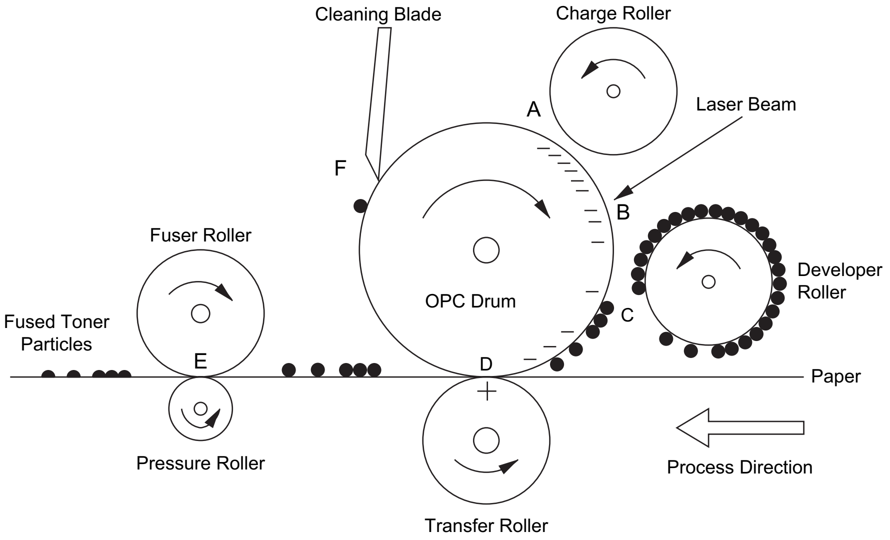


Fig. 4 – Diagram of the EP process.

that reference pattern is the source camera. This approach is shown to provide correct source camera identification between a set of nine cameras without a single misclassification over several thousand images (Lukas et al., 2005). 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 (Lukas et al., 2005). Our experiments agree with these published results.

Some assumptions made in this technique are open for questioning. The wavelet denoising filter (Mihcak et al., 1999), for example, assumes that the image in the wavelet domain is a non-stationary Gaussian signal and that the pattern noise is a stationary Gaussian signal. Since these assumptions are satisfied only approximately, the pattern noise extracted using the denoising filter is not Gaussian either. Another problem is that the filter is applied to the image on slightly overlapping blocks and it also pads image borders with zeros. This leads to a small residual dependence between all extracted noises. Furthermore, reference patterns of different cameras are often slightly correlated due to the use of similar or even the same image processing algorithms.

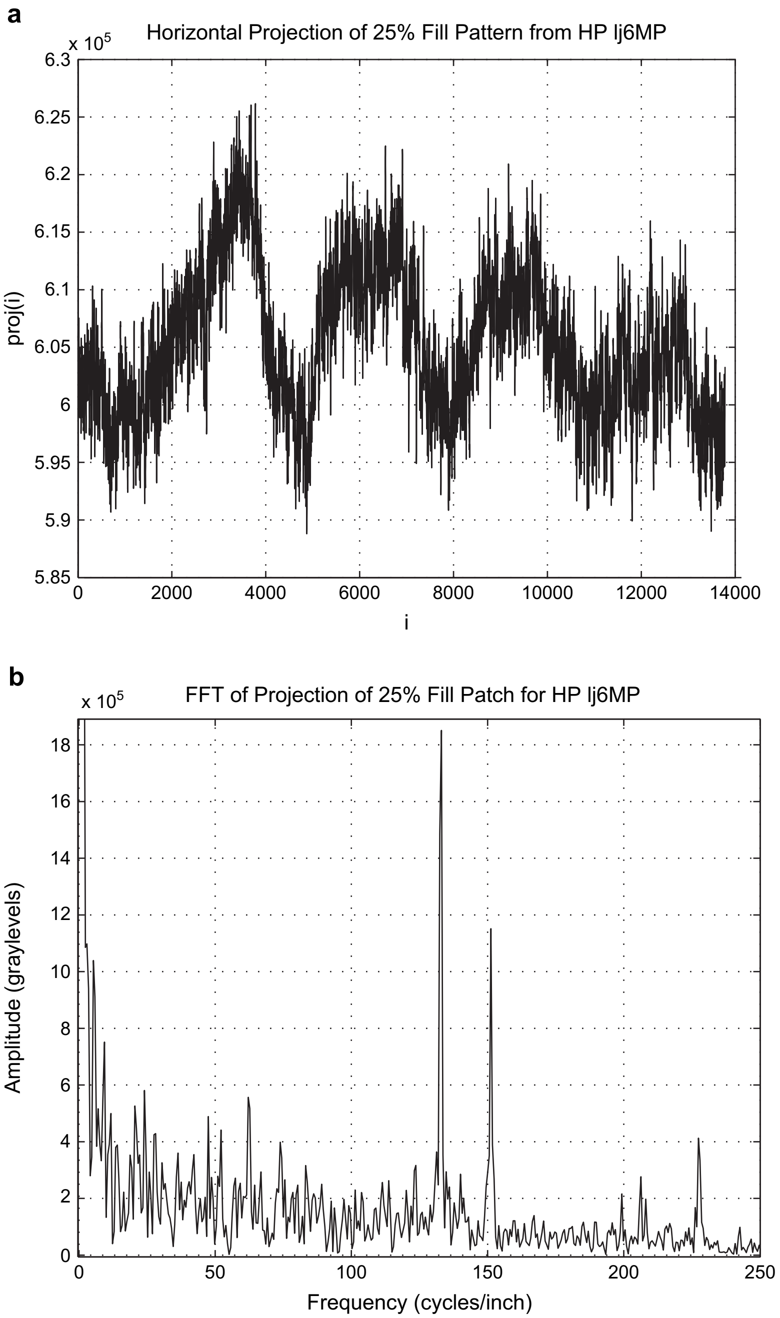


Fig. 5 – Projection and FFT.

2.5. *Feature vector*

In the works by Kharrazi et al. (2004) and Avcibas et al. (2004), a technique is proposed in which a classifier is used to determine the source camera using a set of content independent features extracted from the image. The feature vector is constructed from average pixel values, RGB pair correlations, center of mass distributions, RGB pair energy ratios, wavelet-based features, and a blind image quality metric. This technique is shown to provide close to 90% classification accuracy across five different cameras (Kharrazi et al., 2004). Further experiments need to be performed to determine whether this method is capable of distinguishing between similar camera models or between cameras of the exact same model. Also, the large number of images needed to train a classifier for each camera may not always be available.

2.6. *Color filter analysis*

Most digital cameras capture color images using a single sensor in conjunction with a color filter array. As a result, roughly only one third of the samples are captured by the camera and the other two thirds are interpolated. This interpolation introduces correlations between the samples of a color image. The noninterpolated samples are unlikely to be correlated in the same way as the interpolated samples.

Bayram et al. (2005), proposed a method based on the observation that both the size of the interpolation kernel and the demosaicing algorithm vary from camera to camera. The source camera of a digital image is identified based on estimation of the color interpolation parameters used by the camera. This method is limited to images that are not highly compressed since the compression artifacts suppress and remove the spatial correlation between the pixels created by the CFA interpolation.

Furthermore, the interpolation operation is highly nonlinear, making it strongly dependent on the nature of the depicted scenery. These algorithms are fine-tuned to prevent visual artifacts such as over-smoothed edges or poor color transitions in busy parts of the image. On the other hand, in smooth parts of the image these algorithms exhibit a more linear characteristic. Therefore, smooth and nonsmooth parts of images are treated separately (Bayram et al., 2005). Since no a priori information is assumed on the size of interpolation kernel, probability maps are obtained for varying the sizes of kernels. When viewed in the frequency domain, these probability maps show peaks at different frequencies with varying magnitudes indicating the structure of correlation between the spatial samples. The classifier relies on two sets of features: the set of weighting coefficients used for interpolation, and the peak locations and magnitudes in the frequency spectrum. A Support Vector Machine (SVM) classifier is used to test the effectiveness of the proposed features.

A similar technique, presented by Popescu and Farid (2005), assumes a linear model for the periodic correlations introduced by CFA interpolation. The assumption is that each interpolated pixel is correlated to a weighted sum of pixels in a small neighborhood centered about itself. While perhaps overly simplistic when compared to the highly nonlinear nature of most CFA interpolation algorithms, this simple model is both easy to parameterize and can reasonably approximate the CFA interpolation algorithms. Note that most CFA algorithms estimate a missing color sample from neighboring samples in all three-color channels. For simplicity, however, this technique ignores these interchannel correlations and treats each color channel independently. In practice, neither the specific form of the correlations (i.e., the parameters of the linear model) nor which samples are correlated to their neighbors

Table 1 – Banding frequencies

Printer model	Principal banding frequencies (cycles/inch)
HP LaserJet 5MP	37, 74
HP LaserJet 6MP	132, 150
HP LaserJet 1000	27, 69
HP LaserJet 1200	69
HP LaserJet 4050	51, 100
Samsung ML-1450	16, 32, 100, 106

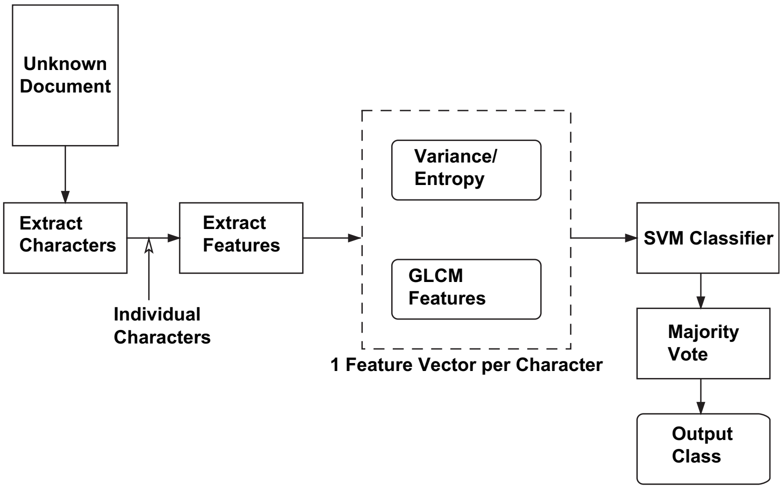


Fig. 6 – Diagram of printer identification.

are known. To simultaneously estimate both, the expectation maximization (EM) algorithm is used (Dempster et al., 1977).

3. Characterization of printers

Printed material is a direct accessory to many criminal and terrorist acts. Examples include forgery or alteration of documents used for purposes of identity, security, or recording transactions. In addition, printed material may be used in the course of conducting illicit or terrorist activities. Examples include instruction manuals, team rosters, meeting notes, and correspondence. In both cases, the ability to identify the device or type of device used to print the material in question would provide a valuable aid for law enforcement and intelligence agencies. We also believe that average users need to be able to print secure documents, for example, boarding passes and bank transactions (Delp, 2002; Chiang et al., 2004, 2005; Mikkilineni et al., 2006).

Additionally, there are a number of applications in which it is desirable to be able to identify the technology, manufacturer, model, or even specific unit that was used to print a given document.

Forensic characterization of a printer involves finding intrinsic features in the printed document that are characteristic of that particular printer, model, or manufacturer's products. This is referred to as the *intrinsic signature*. The intrinsic signature requires an understanding and modeling of the printer mechanism, and the development of analysis tools for the detection of the signature in a printed page with arbitrary content (Ali et al., 2003, 2004; Mikkilineni et al., 2004a,b, 2005a,b; Arslan et al., 2005).

Techniques that use the print quality defect known as *banding* in electrophotographic (EP) printers as an intrinsic signature to identify the model and manufacturer of the printer have been previously reported by Mikkilineni et al. (2004a) and Ali et al. (2003, 2004). We showed that different printers have different sets of *banding frequencies* that 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 the text. The reason for this is that the banding feature 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 for identifying intrinsic signatures in text, previously reported by Mikkilineni et al. (2004b, 2005a,b), 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 estimated over small areas such as inside a text character.

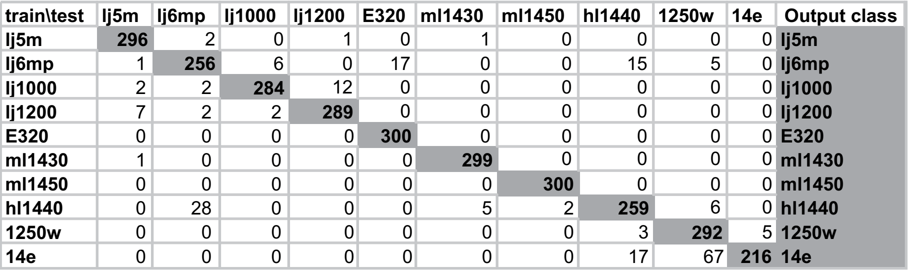
Table 2 – Printers used for classification

Manufacturer	Model	DPI
Brother	hl1440	1200
HP	lj4050	600
Lexmark	e320	1200
HP	lj1000	600
HP	lj1200	600
HP	lj5M	600
HP	lj6MP	600
Minolta	1250W	1200
Okidata	14e	600
Samsung	ml1430	600

An understanding of the EP (laser) printing process is necessary in order to gain insight into the types of features that can be used to describe these printers. The first thing to note is that in the printed output from any printer there exist defects caused by electromechanical fluctuations or imperfections in the print mechanism (Ali et al., 2003). Because these "print quality defects" are directly related to the printer mechanism, they can also be viewed as an intrinsic signature of the printer. The major components of these intrinsic signatures are stable over time and independent of the consumables in the printer.

Fig. 4 shows a side view of a typical EP printer. The print process has six steps. The first step is to uniformly charge an optical photoconductor (OPC) drum. Next, a laser scans the drum and discharges specific locations on the drum. The discharged locations on the drum attract toner particles, which are then attracted to the paper that has an opposite charge. Next, the paper with the toner particles on it passes through a fuser and pressure roller, which melt and permanently affix the toner to the paper. Finally, a blade or brush cleans any excess toner from the OPC drum.

In EP printing, some causes of the artifacts in the printed output are fluctuations in the angular velocity of the OPC drum, gear eccentricity, gear backlash, and polygon mirror wobble. These imperfections in the printer are directly tied to the electromechanical properties of the printer and create corresponding fluctuations in the developed toner on the



train\test	lj5m	lj6mp	lj1000	lj1200	E320	ml1430	ml1450	hl1440	1250w	14e	Output class
lj5m	296	2	0	1	0	1	0	0	0	0	lj5m
lj6mp	1	256	6	0	17	0	0	15	5	0	lj6mp
lj1000	2	2	284	12	0	0	0	0	0	0	lj1000
lj1200	7	2	2	289	0	0	0	0	0	0	lj1200
E320	0	0	0	0	300	0	0	0	0	0	E320
ml1430	1	0	0	0	0	299	0	0	0	0	ml1430
ml1450	0	0	0	0	0	0	300	0	0	0	ml1450
hl1440	0	28	0	0	0	5	2	259	6	0	hl1440
1250w	0	0	0	0	0	0	0	3	292	5	1250w
14e	0	0	0	0	0	0	0	17	67	216	14e

Fig. 7 – Classification results using 300 "e"s from 12 point Times text documents.

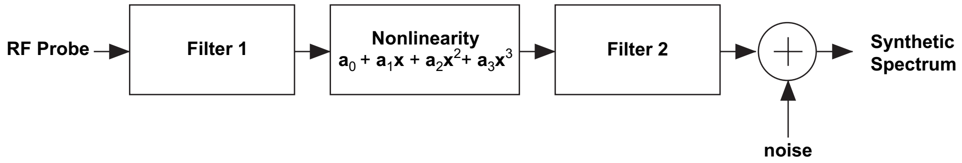


Fig. 8 – RF circuit model.

printed page (Lin et al., 2002; Chen and Chiu, 2001). The fluctuations in the developed toner can be modeled as a texture. Since the mechanical properties that contribute the most to these fluctuations, such as gear ratios, do not change over time, they can be used reliably to intrinsically identify a printer. In the following sections, two techniques for identifying the printer, which created a document, are described.

3.1. *Halftone images*

In EP printing, the major artifact in the printed output is *banding*, which is defined as artifacts due to quasiperiodic fluctuations in process direction parameters in the printer. These are primarily due to fluctuations in the angular velocity of the OPC drum and result in non-uniform scan line spacing. This causes a corresponding fluctuation in the developed toner on the printed page (Lin et al., 2002). The banding artifact appears as alternating light and dark bands perpendicular to the process direction (the direction the paper passes through the printer). The main cause of banding is electromechanical fluctuations in the printer mechanism, mostly from gear backlash. Because these fluctuations are related to the gearing, the *banding frequencies* present in the printed page directly reflect mechanical properties of the printer.

To estimate the banding frequencies of an EP printer, test pages with midtone graylevel patches created using a line fill pattern were printed and analyzed (Ali et al., 2003). These patterns were printed on a set of EP printers and then each pattern was scanned at 2400 dpi. Each scanned image, img(i, j), was then projected horizontally to produce proj$(i) = \sum_j$ img(i, j) shown in Fig. 5a. Fourier analysis of the projections was then obtained such as in Fig. 5, which shows spikes at 132 cycles/inch and 150 cycles/inch. Table 1 shows a list of printers and their principle banding frequencies as found by this method.

Detection and measurement of the banding signal in documents with large midtone regions, such as those with graphic art, can easily be done using methods similar to that used to produce Table 1.

3.2. *Forensic characterization of printed text*

Detection of the banding signal in text is difficult because the power of the banding signal is small with respect to the text, and because only a limited number of cycles of the banding signal can be captured within the height of one text character. Instead, all the print quality defects, including the banding, are lumped together and considered a texture in the printed regions of the document. Features are then extracted from this texture to be used as an intrinsic signature of the printer.

Features are extracted from individual printed characters, in particular, the letter "e"s in a document. The reason for this is that "e" is the most frequently occurring character in the English language. Each character is very small, about 180 × 160 pixels and is non-convex, so it is difficult to perform any meaningful filtering operations in either the pixel or

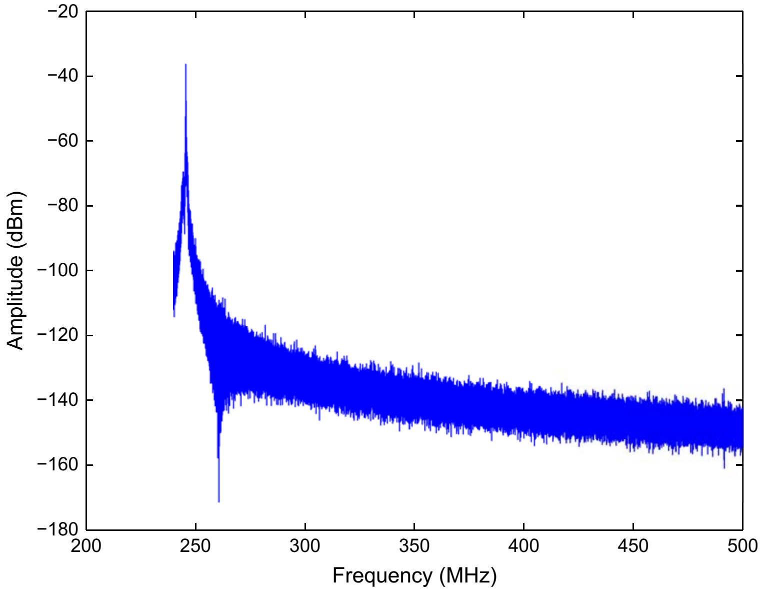


Fig. 9 – Power spectrum produced by the circuit model. The carrier frequency of the probe signal is 246 MHz.

transform domain if the area of interest is only the printed region of each character. To model the texture in the printed regions, gray level co-occurrence texture features, as described by Haralick et al. (1973) and Conners et al. (1984), as well as two pixel based features are used (Mikkilineni et al., 2005a).

Gray level co-occurrence texture features assume that the texture information in an image is contained in the overall spatial relationships among the pixels in the image (Haralick et al., 1973). This is done by first generating the Graylevel Co-occurrence Matrix (GLCM). This is an estimate of the second order probability density function of the pixels in the image. The features are statistics obtained from the GLCM as described by Mikkilineni et al. (2005a).

Fig. 6 shows the block diagram of the printer identification scheme for text documents proposed by Mikkilineni et al. (2005a). Given a document with an unknown source, referred to as the *unknown document*, this process can be used to identify the printer that created it. For testing purposes, the Forensic Monkey Text Generator (FMTG) described by Mikkilineni et al. (2004a) is used to create random documents with known statistics to be classified.

The first step is to scan the document at 2400 dpi with 8 bits/pixel (grayscale). Next, all the letter "e"s in the document are extracted. A set of features are extracted from each character forming a feature vector for each letter "e" in the document. Each feature vector is then classified individually using a support vector machine (SVM) classifier.

The SVM classifier is trained with 5000 known feature vectors. The training set is made up of 500 feature vectors from each of 10 printers listed in Table 2. Each of these feature vectors generated are independent of one another.

Let Ψ be the set of all printers $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ (in our work these are the 10 printers shown in Table 2. For any $\phi \in \Psi$, let $c(\phi)$ be the number of "e"s classified as being printed by printer ϕ. The final classification is decided by choosing ϕ such that $c(\phi)$ is maximum. In other words, a majority vote is performed on the resulting classifications from the SVM classifier.

Using this process with the GLCM feature set, a high classification rate can be achieved between the 10 printers listed in Table 2. A classification matrix showing these results using 300 letter "e"s from 12 point Times documents is shown in Fig. 7. Each entry of the matrix is the number of "e"s out of the 300 in the test document that were classified as the printer listed at the heading of its column.

In Mikkilineni et al. (2005b), the performance of this printer identification technique was tested for other font sizes, font types, paper types, and age difference between training and testing data sets. The classification results in these cases remain near 90% except for the case where the training data are older than the testing data, in which case the classification rate is near 70%.

4. Characterization of RF devices

In certain situations, it is of interest to remotely identify the types of devices that are located in an environment. In order to detect wireless devices, the environment must be probed. This reduces to a problem of determining the properties of an RF circuit by sending it a specially designed probe signal and examining the re-emitted RF signal from the device. The re-emitted signal contains unique distortion that is generated by nonlinearities in the RF circuitry of the device. This distortion is used to characterize the device.

Table 3 – Coefficient values used in circuit model, where $\mu = 10^{-6}$

	Circuit 1	Circuit 2	Circuit 3	Circuit 4	Circuit 5
a_0	1900μ	190 000μ	19μ	3800μ	2850μ
a_1	3μ	300μ	0.03μ	6μ	4.5μ
a_2	1.5μ	150μ	0.015μ	3μ	2.25μ
a_3	1.5μ	150μ	0.015μ	3μ	2.25μ

The probe signal is specially designed to produce intermodulation distortion (IMD) products (Pedro and Carvalho, 2003) in the circuitry of the RF device. IMD products are produced when a two-toned probe signal encounters nonlinear components in a device. A two-toned signal refers to a signal composed of two sinusoids at different frequencies f_1 and $f_2 = f_1 + \Delta$, where Δ is the two-tone offset value. A simplified model of a nonlinear device is represented by a power series (Steer and Khan, 1983) as defined in Eq. (3). In the frequency domain, the power series is used to identify the frequency locations of the IMD products (Generalized power series analysis of intermodulation distortion in a mesfet amplifier: simulation and experiment, 1987). The IMD product locations are defined by Eq. (4) and the order of the IMD product is defined as $o = |n_1| + |n_2|$ (Golikov et al., 2001), where n_1 and n_2 are integers

$$y(t) = \sum_{i=0}^{N} a_i x(t)^i \tag{3}$$

$$f_{\text{imd}} = \pm n_1 f_1 \pm n_2 f_2 \tag{4}$$

A circuit model is used to simulate the front-end of an RF circuit, as shown in Fig. 8. The power series of order three is used to model the nonlinearities in the circuit. The coefficients a_0, a_1, a_2, and a_3 characterize the circuit. Both filters have the same frequency response characteristics. The noise is modelled by a Gaussian Random Variable, $N(\mu, \sigma^2)$. This model generates a power spectrum using the fast Fourier transform. The power spectrum contains IMD products that are created by the power series equation. An example of this power spectrum is shown in Fig. 9.

Five circuit models are created. The coefficients used in each circuit model are shown in Table 3. Each coefficient is responsible for producing amplitude peaks of the IMD products. The coefficients for Circuit 1 are chosen to model experimental data (Martone and Delp, 2006). The coefficients for the

Table 4 – Feature extraction details

Feature	Location	IMD order	Feature value
1	f_1	1	$y_1 = V(f_1)$
2	f_2	1	$y_2 = V(f_2)$
3	$2f_1 - f_2$	3	$y_3 = V(2f_1 - f_2)$
4	$2f_2 - f_1$	3	$y_4 = V(2f_2 - f_1)$

Table 5 – Average feature values in data set 1 (all entries are in units of dBm)

Circuit	y_1	y_2	y_3	y_4
1	−36.09	−36.03	−50.27	−50.07
2	3.91	3.97	−10.27	−10.07
3	−76.11	−75.94	−90.31	−90.06
4	−30.12	−30.09	−44.22	−44.10
5	−32.58	−32.67	−46.69	−46.63

Table 6 – Classification results

Circuit	1	2	3	4	5
SVM	99.4%	100%	100%	90.9%	95.7%
BTC	98.1%	100%	100%	67.7%	89.0%
Distance	99.8%	100%	100%	80.7%	92.6%
GMLC	99.8%	100%	100%	81.8%	92.5%
Parzen	99.8%	100%	100%	82.0%	93.6%
K-NN	99.8%	100%	100%	82.4%	93.4%

remaining circuits are chosen based on the coefficients of Circuit 1. The coefficients for Circuit 2 are chosen to create amplitude peaks far greater than those produced by Circuit 1. The coefficients for Circuit 3 are chosen to create amplitude peaks far less than those produced by Circuit 1. Circuit 4 and Circuit 5 create amplitude peaks similar to the amplitude peaks of Circuit 1.

Multiple power spectra are generated by varying the carrier frequency f_1 in the probe signal. The energy values in the power spectra are dependent on f_1. A power spectrum is therefore denoted as S_{f_1}. f_1 ranges from 241 MHz to 499 MHz in increments of 0.5 MHz (this creates 517 power spectra). The amplitude values in each power spectrum are denoted by y, where $y(f) = V_{f_1}(f)$. The function $V_{f_1}(\cdot)$ returns the amplitude at frequency f, where f ranges from 240 MHz to 500 MHz.

Two data sets are created for each RF circuit model. Data set 1, denoted as $DS1_j$, contains 517 spectra for each circuit j. The noise created for the power spectra of data set 1 is $N(2, 2.5)$.[1] Data set 2, denoted as $DS2_j$, contains 517 spectra for each circuit j. The noise created for the power spectra of data set 2 is $N(0, 2)$.

4.1. *Feature extraction and results*

For a given power spectrum, four amplitudes are extracted and used as features. The amplitudes are extracted based on the locations of the first and third order IMD products. Feature extraction details are shown in Table 4. The four features are then used to form a feature vector as follows: $Y = [y_1\ y_2\ y_3\ y_4]$. A feature vector is formed for each power spectrum in $DS1_j$ and $DS2_j$. The average feature values for $DS1_j$ are shown in Table 5. This table shows that the features from Circuits 4 and 5 are close in value. The average feature values for $DS2_j$ are similar (within 2 dBm) to the values in Table 5.

Six classification systems are used to classify the feature vectors: SVM, binary tree classifier (BTC), distance classifier (Fukunaga, 1990), Gaussian maximum likelihood classifier (GMLC) (Hoffbeck and Landgrebe, 1995), Parzen-window classifier, and a K nearest neighbor (K-NN) classifier. The feature vectors from $DS1_j$ are used to train the classifiers. The feature vectors from $DS2_j$ are used to test the classifiers.

The classification results are shown in Table 6. These results are explained by examining the mean of each feature for each circuit as shown in Table 5. The average feature values for circuits 2 and 3 are well separated thereby leading to a perfect classification. The average feature values between Circuits 1, 4, and 5 are close and result in classification errors. The majority of the errors are for Circuits 4 and 5 since their amplitudes are similar.

5. 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, printers, and RF devices. All of these techniques follow the general forensic characterization framework shown in Fig. 1. This framework, we believe, can be applied to many other types of devices and systems.

REFERENCES

Ali GN, Chiang P-J, Mikkilineni AK, Allebach JP, Chiu GT-C, Delp EJ. Intrinsic and extrinsic signatures for information hiding and secure printing with electrophotographic devices. In: Proceedings of the IS&T's NIP19: International Conference on Digital Printing Technologies, vol. 19. New Orleans, LA; September 2003. p. 511–5.

Ali GN, Chiang P-J, Mikkilineni AK, Chiu GT-C, Delp EJ, Allebach JP. 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, vol. 20. Salt Lake City, UT; October/November 2004. p. 301–5.

Arslan O, Kumontoy RM, Chiang P-J, Mikkillineni AK, Allebach JP, Chiu GT-C, et al. Identification of inkjet printers for forensic applications. In: Proceedings of the IS&T's NIP21: International Conference on Digital Printing Technologies, vol. 21. Baltimore, MD; October 2005. p. 235–8.

Avcibas I, Memon ND, Ramkumar M, Sankur B. A classifier design for detecting image manipulations. In: Proceedings of the IEEE International Conference on Image Processing; 2004. p. 2645–8.

Bayram S, Sencar H, Memon N, Avcibas I. Source camera identification based on cfa interpolation. In: Proceedings of the IEEE International Conference on Image Processing; 2005. p. 69–72.

Blythe P, Fridrich J. Secure digital camera. Digital Forensic Research Workshop, Baltimore, MD; August 2004.

Chen C-L, Chiu GT-C. Banding reduction in electrophotographic process. In: Proceedings of the IEEE/ASME International Conference on Advanced Intelligent Mechatronics, vol. 1; July 2001. p. 81–6.

Chiang P-J, Ali GN, Mikkilineni AK, Chiu GT-C, Allebach JP, Delp EJ. Extrinsic signatures embedding using exposure modulation for information hiding and secure printing in electrophotographic devices. Proceedings of the IS&T's NIP20: International

[1] Mean and variance of the noise are in units of dBm.

Conference on Digital Printing Technologies, vol. 20. Salt Lake City, UT; October/November 2004. p. 295–300.

Chiang P-J, Mikkilineni AK, Arslan O, Kumontoy RM, Chiu GT-C, Delp EJ, et al. 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, vol. 21. Baltimore, MD; October 2005. p. 231–4.

Conners RW, Trivedi MM, Harlow CA. Segmentation of a high-resolution urban scene using texture operators. Computer Vision, Graphics, and Image Processing 1984;25:273–310.

Delp EJ. Is your document safe: an overview of document and print security. In: Proceedings of the IS&T International Conference on Non-Impact Printing, San Diego, CA; September 2002.

Dempster AP, Laird NM, Rubin DB. Maximum likelihood from incomplete data via the EM algorithm. Journal of the Royal Statistical Society 1977;39, no. 1:1–38.

Digital bullet scratches for images. In: Proceedings of the IEEE International Conference on Image Processing; 2005. p. 65–8.

Fukunaga K. Introduction to statistical pattern recognition. San Diego, CA: Academic Press; 1990.

Generalized power series analysis of intermodulation distortion in a mesfet amplifier: simulation and experiment. IEEE Transactions on Microwave Theory and Techniques December 1987; 35:1248–55.

Geradts ZJ, Bijhold J, Kieft M, Kurosawa K, Kuroki K, Saitoh N. Methods for identification of images acquired with digital cameras. In: Bramble SK, Carapezza EM, Rudin LI, editors. Enabling technologies for law enforcement and security, vol. 4232, no. 1.. SPIE Press; 2001. p. 505–12.

Golikov V, Hienonen S, Vainikainen P. Passive intermodulation distortion measurements in mobile communication antennas. In: Vehicular Technology Conference, 2001, vol. 4; October 2001. p. 2623–5.

Haralick RM, Shanmugam K, Dinstein I. Textural features for image classification. IEEE Transactions on Systems, Man, and Cybernetics November 1973;SMC-3, no. 6:610–21.

Hoffbeck J, Landgrebe D. Covariance estimation for classifying high dimensional data. In: International Geoscience and Remote Sensing Symposium (IGARSS95), vol. 2; July 1995. p. 1023–5.

Holst GC. CCD arrays, cameras, and displays. 2nd ed. USA: JCD Publishing & SPIE Press; 1998.

Kharrazi M, Sencar HT, Memon ND. Blind source camera identification. In: Proceedings of the IEEE International Conference on Image Processing; 2004. p. 709–12.

Lin G-Y, Grice JM, Allebach JP, Chiu GT-C, Bradburn W, Weaver J. Banding artifact reduction in electrophotographic printers by using pulse width modulation. Journal of Imaging Science and Technology July/August 2002;46, no. 4:326–37.

Lukas J, Fridrich J, Goljan M. Determining digital image origin using sensor imperfections. In: Said A, Apostolopoulos JG, editors. Proceedings of the SPIE International Conference on Image and Video Communications and Processing, vol. 5685, no. 1. SPIE; 2005. p. 249–60.

Lukas J, Fridrich J, Goljan M. Detecting digital image forgeries using sensor pattern noise. In: Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072. San Jose, CA; January 2006.

Martone AF, Delp EJ. Forensic characterization of rf circuits. In: Proceedings of Government Microcircuit Applications and Critical Technology Conference 06 (GOMACTech-06), San Diego, California; March 2006. p. 224–7.

Martone AF, Mikkilineni AK, Delp EJ. Forensics of things. In: Proceedings of the 2006 IEEE Southwest Symposium on Image Analysis and Interpretation, Denver, CO; March 2006. p. 149–52.

Mihcak MK, Kozintsev I, Ramchandran K, Moulin P. Low-complexity image denoising based on statistical modeling of wavelet coefficients. IEEE Signal Processing Letters 1999;6, no. 12:300–3.

Mikkilineni AK, Ali GN, Chiang P-J, Chiu GT-C, Allebach JP, Delp EJ. Signature-embedding in printed documents for security and forensic applications. In: Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VI, vol. 5306. San Jose, CA; January 2004. p. 455–66.

Mikkilineni AK, Chiang P-J, Ali GN, Chiu GT-C, Allebach JP, Delp EJ. Printer identification based on textural features. In: Proceedings of the IS&T's NIP20: International Conference on Digital Printing Technologies, vol. 20. Salt Lake City, UT; October/November 2004. p. 306–11.

Mikkilineni AK, Chiang P-J, Ali GN, Chiu GT-C, Allebach JP, Delp EJ. Printer identification based on graylevel co-occurrence features for security and forensic applications. In: Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VII, vol. 5681. San Jose, CA; March 2005. p. 430–40.

Mikkilineni AK, Arslan O, Chiang P-J, Kumontoy RM, Allebach JP, Chiu GT-C, et al. Printer forensics using svm techniques. In: Proceedings of the IS&T's NIP21: International Conference on Digital Printing Technologies, vol. 21. Baltimore, MD; October 2005. p. 223–6.

Mikkilineni AK, Chiang P-J, Suh S, Chiu GT-C, Allebach JP, Delp EJ. Information embedding and extraction for electrophotographic printing processes. In: Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072. San Jose, CA; January 2006. p. 385–96.

Pedro J, Carvalho N. Intermodulation distortion in microwave and wireless circuits. Norwood, MA: Artech House, INC.; 2003.

Popescu A, Farid H. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing 2005;53, no. 10:3948–59.

Steer M, Khan P. An algebraic formula for the output of a system with large-signal, multifrequency excitation. Proceedings of the IEEE January 1983;71:177–9.

Nitin Khanna received the Bachelor of Technology degree in Electrical Engineering from the Indian Institute of Technology, Delhi, India, in 2005. He is currently working towards the Ph.D. degree in Electrical and Computer Engineering at Purdue University, West Lafayette, Indiana. His research interests include image processing and multimedia security.

Aravind K. Mikkilineni received the B.S. from Ohio State University, Columbus, in 2002 and the M.S. degree from Purdue University, West Lafayette, in 2004, both in Electrical and Computer Engineering. He is currently working toward the Ph.D. degree at Purdue University. His research interests include printed document security and sensor forensics.

Anthony F. Martone was born in Newton, New Jersey. In 1999, he received an A.S. degree and A.A.S. degree at the County College of Morris in Randolph, New Jersey. In 2001, Anthony received his B.S.E.E. (summa cum laude) degree at Rensselaer Polytechnic Institute in Troy, New York. Since 2002, he has been with the School of Electrical and Computer Engineering at Purdue University, West Lafayette, Indiana, where he is a graduate student in the direct Ph.D. program. His research interests include video databases, closed captions, text alignment, pattern recognition, speech recognition, RF forensics, and radar systems.

Gazi Naser Ali received the B.Sc. degree in electrical engineering from Bangladesh University of Engineering and Technology. He is currently pursuing his Ph.D. degree in the School of Electrical and Computer Engineering, Purdue University, West Lafayette. His research interests are print quality analysis, document image processing, and pattern recognition. He is a student member of IEEE and IS&T.

George T.-C. Chiu is an Associate Professor in the School of Mechanical Engineering at Purdue University. He received his B.S. in Mechanical Engineering from the National Taiwan University in 1985 and his M.S. and Ph.D. degrees in Mechanical Engineering from the University of California at Berkeley in 1990 and 1994, respectively. Before joining Purdue University in 1996, he worked for the Hewlett-Packard company in developing low-cost, high performance color inkjet printers and multifunction devices. Dr. Chiu's research interests are mechatronics, dynamic systems and control, modeling and control of digital printing and imaging system, and noise and vibration control. He is a member of IEEE, ASME, and IS&T.

Jan P. Allebach received his B.S.E.E. from the University of Delaware in 1972 and his Ph.D. from Princeton University in 1976. He was on the faculty at the University of Delaware from 1976 to 1983. Since 1983, he has been at Purdue University where he is Michael J. and Katherine R. Birck Professor of Electrical and Computer Engineering. His current research interests include image rendering, image quality, color imaging and color measurement, printer and sensor forensics, and digital publishing.

Prof. Allebach is a member of the IEEE Signal Processing (SP) Society, the Society for Imaging Science and Technology (IS&T), and SPIE. He has been especially active with the IEEE SP Society and IS&T. He is a Fellow of both these societies, has served as Distinguished/Visiting Lecturer for both societies, and has served as an officer and on the Board of Directors of both societies. Prof. Allebach is a past Associate Editor for the IEEE Transactions on Signal Processing and the IEEE Transactions on Image Processing. He is presently Editor for the IS&T/SPIE Journal of Electronic Imaging. He received the Senior (best paper) Award from the IEEE Signal Processing Society and the Bowman Award from IS&T. In 2004, he was named Electronic Imaging Scientist of the Year by IS&T and SPIE.

Edward J. Delp received the B.S.E.E. (cum laude) and M.S. degrees from the University of Cincinnati, and the Ph.D. degree from Purdue University. In May 2002, he received an Honorary Doctor of Technology from the Tampere University of Technology in Tampere, Finland. Since August 1984, he has been with the School of Electrical and Computer Engineering and the School of Biomedical Engineering at Purdue University, West Lafayette, Indiana. In 2002, he received a chaired professorship and currently is The Silicon Valley Professor of Electrical and Computer Engineering and Professor of Biomedical Engineering.

His research interests include image and video compression, multimedia security, medical imaging, multimedia systems, communication and information theory. Dr. Delp is a Fellow of the IEEE, a Fellow of the SPIE, a Fellow of the Society for Imaging Science and Technology (IS&T), and a Fellow of the American Institute of Medical and Biological Engineering. In 2004, he received the Technical Achievement Award from the IEEE Signal Processing Society for his work in image and video compression and multimedia security.