Printer and Scanner Forensics

Pei-Ju Chiang[‡], Nitin Khanna[†], Aravind K. Mikkilineni[‡]
Maria V. Ortiz Segovia[†], Sungjoo Suh[†]
Jan P. Allebach[†], George T. C. Chiu[‡], Edward J. Delp[†]
[†]School of Electrical and Computer Engineering
[‡]School of Mechanical Engineering
Purdue University, West Lafayette, Indiana USA

INTRODUCTION: Contrary to popular opinion, the use of paper in our society will not disappear any time during the foreseeable future. In fact, the use of paper continues to grow rather than decline. It is certainly true that as individuals, we may be printing less than we used to. And the role of paper has been transformed from the archival record of a document to a convenient and aesthetically appealing graphical user interface. The use of paper is now intimately linked to the electronic systems that capture, process, transmit, generate, and reproduce textual and graphical content. Paper can be thought of as an interface between humans and the digital world. If this interface is not secure, the entire system becomes vulnerable to attack and abuse. Although paper is read by humans in the same way that it has been for millennia, and has had the same fundamental form and composition for almost that long as well, the technologies for printing and scanning documents and capturing their content have evolved tremendously, especially during the last twenty years. This has moved the capability to generate printed documents from the hands of a select few to anyone with access to low-cost scanners, printers, and personal computers. It has greatly broadened the opportunities for abuse of trust through the generation of fallacious documents and tampering of existing documents, including the embedding of messages in these documents.

In today's digital world, securing different forms of content is very important in terms of protecting copyright and verifying authenticity. Foreign trade losses due to piracy of books between 1995 and 2001 are estimated to be between $633 million and $695 million per year. In addition, printed material is a direct accessory to many criminal activities such as forgery or alteration of documents used for purposes of identity or recording of transactions. Printed material may also be used in the course of conducting illicit 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 or scan the material in

question would provide a valuable aid for law enforcement and intelligence agencies.

Digital images and scanned documents generated by various sources are widely used in a number of applications from medical imaging and law enforcement to banking and daily consumer use. The increasing functionality of image editing software allows even an amateur to easily manipulate images. In some cases a digitally scanned image can meet the threshold definition requirements of a "legal duplicate" if the document can be properly authenticated. Forensic tools that help establish the origin, authenticity, and the chain of custody of such digital images are essential to a forensic examiner. These tools can prove to be vital whenever questions of digital image integrity are raised. Therefore, a reliable and objective way to examine digital image authenticity is needed.

Signal processing plays a key role in the characterization of scanners and printers. Development of appropriate signal processing tools allows the ability to prevent or discourage unauthorized use of scanned or printed materials. Two strategies can be used to achieve these goals. The first strategy is passive and applies to both printers and scanners. It involves characterizing a device through the use of intrinsic features present in the scanned image or printed document that are distinctive for the particular device, model, or manufacturer's products. This is referred to as the *intrinsic signature*. The intrinsic signature requires an understanding and modeling of the device mechanism, and the development of analysis tools for the detection of the signature in a scanned or printed document with arbitrary content. The second strategy is active and currently applies only to printers. It involves embedding an *extrinsic signature* in a printed page either by modifying the document to be printed before it is sent to the printer, or by modifying process parameters in the printer mechanism to encode identifying information such as the printer serial number and date of printing. The extrinsic signature also requires an understanding and modeling of the device mechanism, and the development of modulation techniques for the embedding of the signature in a printed document with arbitrary content. It also requires the development of image analysis tools for detecting the presence of the extrinsic signature and demodulating and decoding its content. Several scanning and printing technologies currently dominate the non-commercial market. Scanners differ based on the type of sensor and mechanism that they use to image a document. Printers differ based on the mechanism and marking technology used to form the image on the printed page. The details of these technologies are discussed in later sections.

SCANNING AND PRINTING PROCESSES: A basic imaging pipeline commonly encountered in an office or household environment is composed of a printer, flatbed scanner, and a computer. A typical usage of this pipeline, in the case of duplicating a document, involves first scanning the document, processing and modifying it using editing tools, and finally printing the modified version. Notice that whereas the

scanner converts a hard copy document into a digital one, the printer accomplishes the opposite. Within this imaging pipeline, there exist several stages during which the document can be altered or corrupted either intentionally or accidentally. In later sections, the idea of forensically exploiting the way by which the printer and scanner produce outputs is discussed.

Scanning: In a conventional desktop scanner, a hard copy document is placed face-down on a glass window, a bright light illuminates the page, and the printed patterns are reflected back to a photosensitive element. The scanning head carries the light source and the photosensitive element back and forth underneath the glass until the selected area of the page is covered. A series of mirrors and lenses direct the reflected light onto the photosensitive element or sensor that converts it into electrical signals. To complete the process, electrical signals produced by the sensor are digitized by an analog-to-digital converter (ADC) and are sent to the host computer. The operational diagram for a typical scanner is shown in Figure 1.

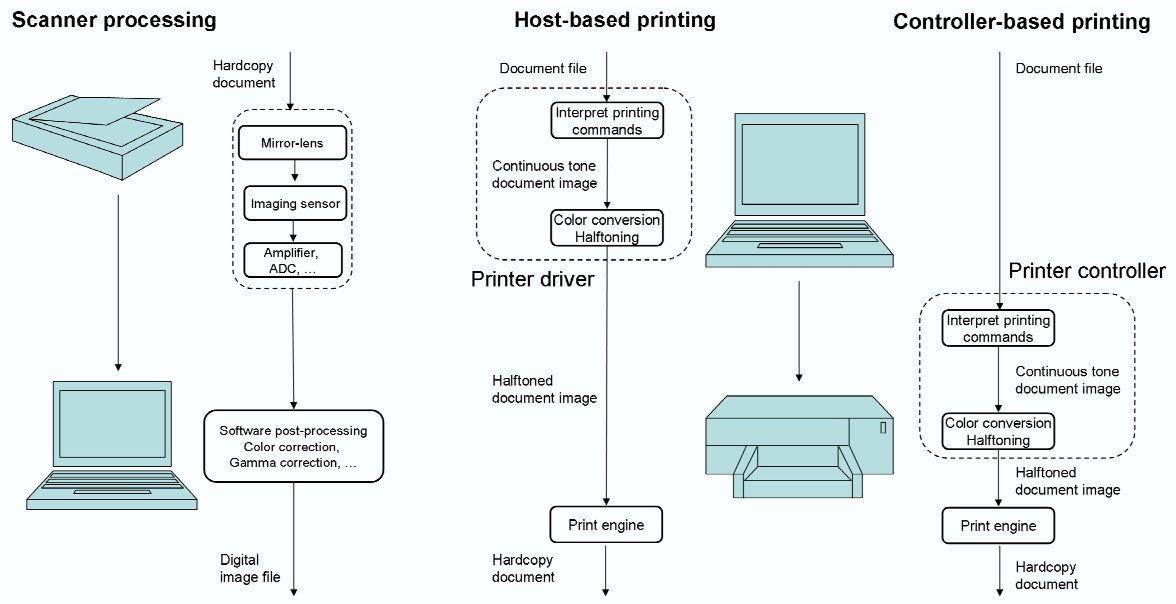

Fig. 1. Block diagrams of operations for typical scanner (left) and printer (right).

Printing: The goal of the printing operation is to transform the document into dots on a piece of paper. Figure 1 shows two different approaches to printing, namely *host-based printing* and *controller-based printing*. Host-based printing refers to the case in which the printer driver uses the host computer to do everything required to produce the printer-ready halftone page image. The printer driver interprets the

Page Description Language (PDL) file to create a display list. Then the objects on the display list are rendered into bit-map form. At the output of this interpretation stage, an 8-bit CMYK or RGB continuous-tone document page is generated. This continuous-tone document page is subsequently modified by color space conversion, gamut mapping, and finally halftoning. When these steps are complete, the printer driver sends the halftone data to the printer to produce a hardcopy document. In a controller-based printer, the document is sent to the printer in the form of a high-level description language or other graphic commands; and the printer controller performs all of the computations associated with the printing job that were just described for the printer driver used with the host-based printer.

SCANNER ARCHITECTURE: Figure 2 shows the architecture of a typical flatbed scanner. The document is placed on the scanner bed and the acquisition process starts. The lamp used to illuminate the document is either a cold cathode fluorescent lamp (CCFL), xenon lamp, or LEDs, while older scanners may use a standard fluorescent lamp. Using a belt and a stepper motor, the scan head slowly translates linearly to capture the image. Velocity fluctuations in the constant speed portion of the motor's motion may lead to color registration errors in the scanned document [1]. The scan head includes a set of lenses, mirrors, filters, and the imaging sensor. Most desktop scanners use charge-coupled device (CCD) imaging sensors. Other scanners use complementary metal-oxide semiconductor (CMOS) imaging sensors, contact image sensors (CIS), or photomultiplier tube (PMTs). The native resolution of the scanner is determined by the horizontal and vertical resolution. The number of elements in the linear CCD sensor determines the horizontal optical resolution. The step size of the motor controlling the scan head and the sensor data retrieval time determines the vertical resolution.

The process of manufacturing imaging sensors introduces various defects that create noise in the pixel values [2]. Sensor noise, which is of interest for use in forensic characterization, can be described in three forms. 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 current and photoresponse nonuniformity (PRNU). Dark currents are stray currents from the sensor substrate into the individual pixels. This varies from pixel to pixel and the variation is known as fixed pattern noise (FPN). FPN is caused by differences in detector size, doping density, and foreign matter trapped during fabrication. PRNU is the variation in pixel responsivity and is present when the device is illuminated. This noise is caused by variations between pixels such as detector size, spectral

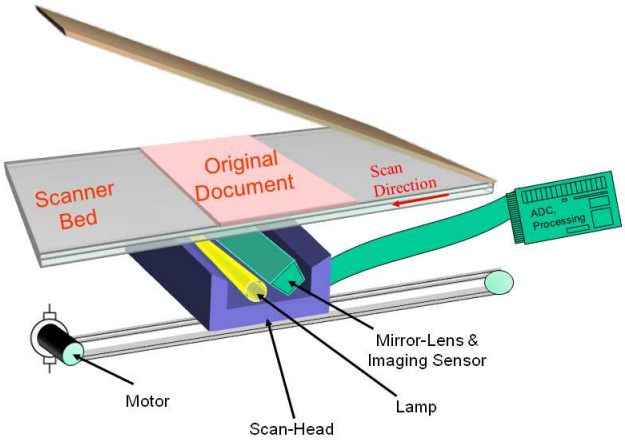

Fig. 2. Flatbed scanner architecture.

response, thickness in coatings and other imperfections created during the manufacturing process. The third type of noise is random noise components which vary from frame to frame. The random noise is inevitable and cannot be removed by calibration. However, its statistical characteristics may give some clues about the source scanning device. The first type of noise leads to large deviations in pixel values and is easily corrected in most of the devices available in market. The second type of noise does not lead to large variations in pixel values and algorithms such as flat-fielding used to correct it are difficult to implement. Due to the difficulties in achieving a uniform sensor illumination inside the camera, most consumer cameras do not flat-field their images [3].

SCANNER SIGNATURES: Recent advances in source scanner identification have been based upon techniques for source camera identification using sensor noise [3], [4]. Reference patterns for individual cameras are estimated and stored in a database. The source of an image is then determined by correlating its noise with a set of known reference patterns. A direct extension of the sensor noise based source camera identification algorithm can be used for the source scanner identification problem [5]. In this case, the 2-dimensional noise pattern in the image is used. However, experiments have shown a lower classification accuracy than those achieved in similar experiments for source camera identification. Improved results can be obtained by using statistical features of sensor noise estimates obtained through the use of denoising filters, high-frequency wavelet coefficients, and neighborhood prediction errors [6]. Experiments using

such statistical features from images scanned at low resolution from seven different scanners show an average classification accuracy of over 90%.

Similar classification accuracies can be achieved using only statistics of the sensor noise by exploiting the way in which the sensor is moved within the scanner mechanism [7]. This scheme uses an estimate of the fixed "row-pattern" of the noise in the scanned image. A robust intrinsic signature can be obtained in this manner since the same sensor elements are used to scan each row of the image. Using a set of statistical features derived from the row-pattern allows source scanner identification even from images scanned at low resolutions, or that have undergone post-processing such as JPEG compression and contrast stretching.

ELECTROPHOTOGRAPHIC (LASER) PRINTER ARCHITECTURE: Electrophotography (EP), also referred to as xerography, is the underlying marking technology for laser printers and office copiers. There are six steps in a typical EP process: charging, exposure, developing, transferring, fusing, and cleaning. Figure 3 shows the architecture of a typical laser printer. Typically, an organic photoconductive (OPC) drum, also called a photoreceptor, rotating at a constant angular velocity is electro-statically charged through a charger roller. A latent image is then exposed onto the OPC drum by scanning a pulsed laser beam with a rapidly spinning polygon mirror and discharging specific locations on the OPC surface. A toner image is developed by electrostatically adhering toner particles to these areas of the OPC surface that were discharged by the laser beam. The developed image is then transferred electrostatically onto the output media (paper) through a charged transfer roller. The toner image on the paper is then fused to the paper through heat and pressure by the fuser. To prepare to print the next page, the surface of the OPC drum is cleaned to remove any residual toner by a cleaning blade that scrapes across the OPC surface.

LASER PRINTER SIGNATURES: Inherent artifacts generated by EP printers due to their physical components such as gear mechanisms, polygon mirror wobble, and optical photoconductor (OPC) angular velocity can be used as an intrinsic signature of the device. Laser printers can be characterized using intrinsic signatures such as banding [8]. Banding is an artifact caused by fluctuations of the OPC angular velocity and errors in the gear transmission mechanism. It appears as nonuniform light and dark lines perpendicular to the process direction. This is the direction in which the paper moves through the printer. Different printers have different sets of banding frequencies depending upon brand and model.

Banding based identification is based on frequency domain analysis of a one-dimensional projected signal of large mid-tone regions of the document, typically occurring in printed images. Fourier analysis of the signal yields the banding frequencies. The method is detailed in Figure 4. What may not be

Fig. 3. Architectures for typical laser (left) and ink-jet (right) printers.

immediately evident here is that the 193 cycles/inch peak corresponds to the tooth-to-tooth error of the large gear, and the 24 cycle/inch peak corresponds to the eccentricity error associated with the small gear.

In a text-only document, the absence of large midtone areas makes it difficult to capture suitable signals for banding analysis according to the method just described. In this case, texture features estimated from individual text characters, can be used to capture the intrinsic signature. Texture is a consequence of the fluctuations in the developed toner due to electromechanical imperfections. A set of texture features are based on the graylevel co-occurrence matrix (GLCM) [9], [10]. These features are estimated from printed text regions and are classified using pattern recognition techniques such as Support Vector Machines (SVM), Principal Component Analysis (PCA) and Gaussian Mixture Models (GMM). Other techniques that can be used to intrinsically characterize EP printers include measures of image sharpness, toner fusing characteristics, dot gain, and asymmetry of toner distribution [11]. In addition, an optical effect due to the toner particles lying on top of the paper is characteristic of EP printers [12]. A surface profiling apparatus can display how the printed areas extend above the surface of the paper.

INKJET PRINTER ARCHITECTURE: The inkjet mechanism consists of three principle components – the print head, the carriage, and the paper advance mechanism. Figure 3 illustrates the operation of a typical inkjet printer [13]. The paper is picked up and advanced in the process direction under the carriage by the paper advance mechanism. The carriage moves the print head back and forth across the paper in the scan direction. Drops of ink are fired onto the paper by a print head consisting of a nozzle plate containing several columns of nozzle openings and reservoirs for one or more different color inks. As

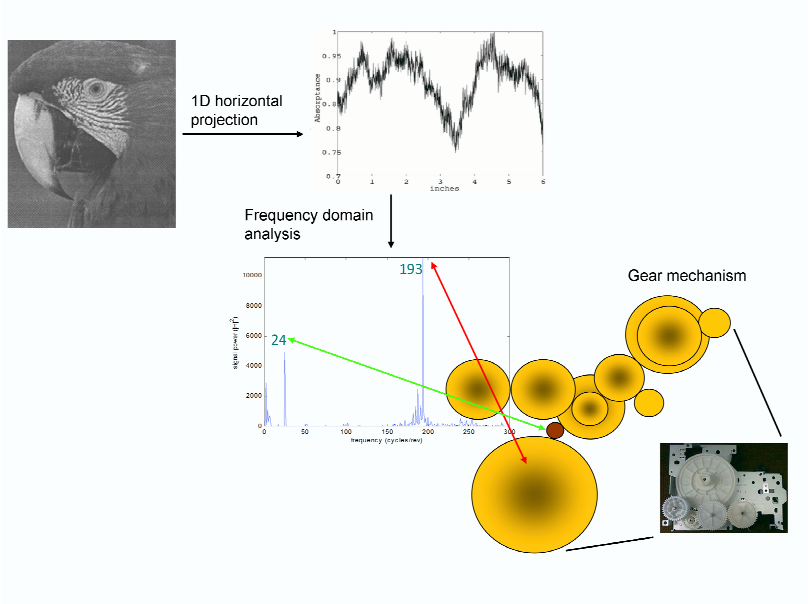

Fig. 4. Intrinsic signature of a laser printer based on banding. A 1-D signal is obtained from the horizontal projection of a printed image. Frequency analysis of the projection signal provides a set of banding frequencies that are characteristic of the gear train mechanism of the laser printer that produced the image.

illustrated in Fig. 5, the nozzles for each colorant are arranged in one or more staggered columns (two for the case of Fig. 5). By appropriately timing the firing of the nozzles in each column, it is possible to achieve an effective vertical resolution that is equal to the vertical offset between adjacent columns. In this way, the nozzles in each column can be spaced far enough apart and the adjacent columns spaced far enough apart to ease fabrication requirements, provide better structural integrity for the nozzle plate, and provide the necessary room for fluid channels and firing circuitry. Each column of nozzles allows the simultaneous printing of several rows of pixels during a single pass of the print head across the paper. Once the print-head has completed an entire pass in the scan direction, the paper is advanced again in the process direction; and a new pass is completed. This process is repeated until the print job is completed, at which time the paper advance mechanism ejects the paper into the output tray.

Several print options exist for inkjet printers which control print resolution, speed, directionality, and the number of printing passes over each point on the paper. The pixels that are printed in a given pass across the page comprise a subset of the pixels in a horizontal band with height equal to the height of the print head. This horizontal band of pixels is called a swath. In single-pass print modes, the printhead passes only once over each position on the paper, so the swaths do not overlap. For a multipass print

Fig. 5. Illustration of the process of printing a 3 pixel wide vertical line in a two-pass, bi-directional print mode. The print mask consists of a two-dimensional array of 1's and 2's. The print mask is tiled over the entire page. Pixels on the page are printed on pass 1 (right-to-left) or pass 2 (left-to-right) according to whether they are labeled with a 1 or 2 from the print mask.

INKJET PRINTER SIGNATURES: The combination of inkjet print options can lead to a very complex intrinsic signature with many different identifiable features. Figure 6 shows the appearance of a typical dot printed with a single pass, 300 dpi resolution print mode with different carriage speeds and printing directions [13]. It illustrates the fact that as print speed increases, the dot shape becomes more asymmetric,

and thus more dependent on the printing direction. Other artifacts that are related to print speed are tails and satellites which occur when the drop of ink breaks up as it exits the print nozzle. If the secondary droplet breaks away completely from the main droplet it forms a satellite (see center and right in Figure 6), and if it breaks away only partially, it forms a tail (see left in Figure 6). Tails and satellites usually trail the main dot relative to the direction of travel of the pen.

Another potentially useful inkjet print artifact is dot placement. Dot placement errors can be caused by paper advance errors, carriage positioning errors, or misaligned nozzles in the print head. Each ink drop travels roughly perpendicular to the surface of the nozzle plate at the nozzle position. Due to structural characteristics of the pen, the nozzle plate may not be flat. This will cause drops from different nozzles to fire in different directions, thereby creating characteristic patterns in the printed content. This is referred to as a toe-in or dimple effect [14]. Other characteristic features of inkjet printers such as the fluid dynamics of the inkjet nozzle, ink chemistry and periodic variation caused by missing jets or paper advance errors are all potential signatures [12].

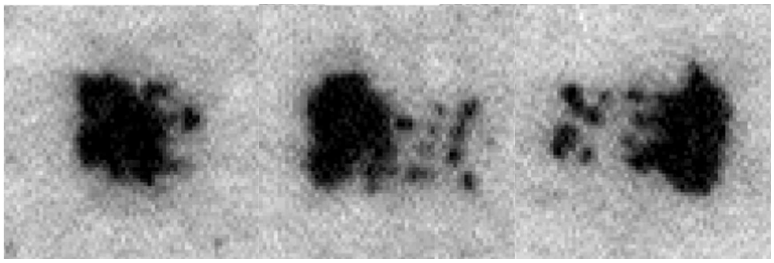

Fig. 6. Typical dots printed by a 300dpi inkjet printer: 15 inch/second left-to-right print mode (left), 45 inch/second left-to right print mode(center), and 45 inch/second right-to-left print mode (right). Dots were captured at 7000 dpi using a QEA IAS-1000 imaging system.

To identify the intrinsic signature of an inkjet printer for security and forensic purposes, image analysis techniques have been used in recent years [11], [12], [15]–[17]. The majority of the approaches combine a variety of image analysis techniques with different classification algorithms to either distinguish different printing technologies (inkjet vs. laser EP) [11], [18] or distinguish between make and models [11], [16], [19]. It has been shown that a variety of image features and print quality metrics can be used to discriminate among inkjet printers. For example, quantitative analysis of 14 pt. character “i”s using features such as line raggedness, dot roundness, and background noise have been used to characterize different inkjet printers [11].

The applicability of texture for classification of inkjet printers has also been investigated [16] by using

gray-level co-occurrence features. The features that provide the best classification results can be selected by performing stepwise discriminant analysis (SDA). Using these procedures, different inkjet printer models can be correctly classified.

Another characteristic that can be used to discriminate among inkjet printers is spur marks. Spur marks are formed on a printout by the paper conveyance gears of inkjet printers and are clearly distinguished from the background by infrared oblique lighting and gradient image processing [20]. Inkjet printers can be classified by type of spurs and their arrangement. These technique allows identification of model and manufacturer of the printer, and is significant not only for counterfeit detection but also in the field of forensic document examination. An overview of other characteristics of inkjet printing and methods of printer identification using these characteristics can be found in [12].

EXTRINSIC SIGNATURES FOR PRINTING: Printers are complex electromechanical devices. Imperfections in the printer mechanism such as imperfect gear meshing or motor speed fluctuations are always present. These imperfections directly affect the printed output. For example, as discussed earlier, fluctuations in the optical photoconductor drum angular velocity will cause inter-scanline spacing to vary which creates banding in the printed page. The effects on the printed output can be directly correlated with the mechanical properties of the printer. It is because of this direct correlation that these features can be used as an intrinsic signature of the printer. The intrinsic signature can be used to determine the device that created a document, and in some circumstances also provide a level of tamper-proofing for the document. However, in many security applications there is a need to embed additional content into the document that cannot be achieved with intrinsic signatures such as a secure hash of the document, serial number of the printer, or date and time of the printing.

Various methods exist for embedding additional content into a document which fall under two basic categories. The first contains methods that embed security information into the document before it is sent to the printer. These methods are typically designed such that the embedded security features are able to survive the printing process. The second category contains those methods which embed the security features at the printer mechanism level. Performing the embedding in the printer allows a broader domain for marking the print and makes attacking the security features more difficult.

Embedding at the Document Level: Early techniques for embedding information into a printed document relied on modification of the electronic document in such a way that the embedded information survived the printing process. Many of these techniques are extensions of digital watermarking methods widely used to secure digital images. Once the electronic document is marked and printed, the embedded information can be extracted through analysis of a scanned image of the document.

One of the earliest methods for securing printed text involves the shifting of elements in a text document [21]. Individual bits of data are embedded into the document by imperceptibly shifting textual elements approximately 1/600th inch such as lines, words, or individual characters. No information about the original document is necessary to detect the shifts since the information is embedded differentially by only shifting every other line. This type of encoding is robust to scan-print attacks and photocopy generation loss.

Word and character coding allow a higher data density, but are not as robust as line coding due to the fact that each shift is encoded in a smaller portion of the printed page. Also most word processors will vary the spacing between adjacent words and characters, so estimation of shifts using the differential method will not work unless the original document is also available for comparison. These shifts could instead be used as a fragile watermark to detect alterations to a document.

The shifting method deals with encoding information in text, but documents may also contain halftone images. Halftoning is the process of converting a continuous tone image into an image having only a finite number of levels, typically two for printed images. Numerous methods have been developed for watermarking halftone images. Most involve modifying the halftone patterns used when printing the image. The three basic methods are the use of multiple dithering matrices, conjugate halftone screens, angular variation of the halftone screen [22], or angular variation of the halftone dots themselves [23]. In the first method, the dithering matrix changes from tile to tile and can be used to encode information. Detection involves measuring the statistical properties of the halftone patterns and their variation across the image. The second method involves conjugate halftone screens, two screens are used to form two halftone images and the data are embedded through the correlations between two screens. The third basic method involves encoding the data in the angular orientation of the screen in each halftone cell. In this case, each angular orientation can represent multiple bits depending on the number of angles at which the halftone screen can be generated and detected.

Another method of data hiding using halftone patterns relies on images that are printed opposite each other on either side of the page using conjugate halftone patterns such that when the page is held up to a light source a fake watermark will appear [24]. This technique requires a high degree of control over the registration of each side of the document to make sure the halftone patterns line up. A similar technique known as visual watermarking can be used for one-sided printing using a transparent screen for verification.

Watermarking of images in documents can also be done using continuous-tone image watermarking techniques [25]. These methods first embed a watermark into the continuous-tone image. The marked

image is then printed at a high resolution to create the document. To detect the watermark, the document is scanned and transformed back into a continuous-tone image after which an appropriate method for detecting the watermark is used. The type of watermark embedded has to be one that can survive the print-scan process.

Detectability of the embedded information and the printed image quality can both be improved by considering the printer's halftoning process while embedding [26]. This approach uses a modified version of direct binary search (DBS) halftoning in which each iteration jointly optimizes both the watermark detectability and perceptual image quality metrics of the halftone image. This method was shown to be robust against many common image processing operations such as JPEG compression and histogram equalization when compared to prior methods which do not take into account the printing process.

Embedding at the Printer Mechanism Level: The previously mentioned document watermarking methods embed information into the document before it is printed. Several methods exist which embed information into the document at the hardware level of the printer. These techniques exploit the way that the printer puts marks on the paper. This is different than modifying the file to be printed or the printer driver. Embedding at the hardware level allows access to a much larger marking domain and the potential for increased security. Additionally, circumvention of the emdedding of such marks is more difficult since the embedding step exists in the hardware of the printing device instead of as a software module or device driver. Changing the document itself will not affect the embedding.

An embedding method developed by printer manufacturers to help trace counterfeit currency uses a pattern of yellow dots overlaid on top of the printed document. [27] A rectangular grid of 15 by 8 dots is repeated over the entire page. Since the dots are printed in yellow, they are invisible to the naked eye under white light. Typically about 10 bytes of information is encoded in this grid, including date and time of printing, serial number, and parity information for error correction.

This embedding scheme has the advantage that it is independent of image content. However, this method does not protect the content of the document. The dot pattern only indentifies the printer that created the dot pattern and not necessarily the printer that created the document content. For example, a blank page could be printed on a color printer to lay down the dot pattern, after which the actual content could be printed by a monochrome printer that does not lay down a dot pattern. If the pattern was somehow content dependent, then perhaps a hash of the document could additionally be embedded to verify the content.

Laser pulse width modulation (PWM) is a technology used in some EP printers to control dot size and placement. This capability can be accessed to embed information into halftone images [28]. Since the

Fig. 7. Process for extracting information from halftone images marked using pulse width modulation (PWM).

electrophotographic process is often unstable for development of isolated single-pixel dots, clustering dots in pairs leads to more stable development. Data is embedded into the halftone by shifting the centroids of dot pairs such that they lie between points on the halftone lattice.

Figure 7 shows the block diagram for extracting the embedded information from a halftone document containing an extrinsic signature based on PWM. The printed document that contains the information is first scanned. The scanned image is preprocessed using morphological filtering to remove noise caused by the printing and scanning processes. Then the preprocessed image is analyzed using centroid, skew-angle, and lattice detection to extract the embedded information.

Another approach is to modulate the laser intensity in a laser printer, which allows per-scan-line changes in dot size. The effects of this type of embedding are shown in Figure 8. A simple set of signals which can be used for embedding is a set of sinusoids at various frequencies and amplitudes such that they lie below the human visual sensitivity threshold curve. For example, in Figure 8, each line is embedded with a different frequency sinusoid, each of which could represent a singe bit or symbol. This figure contains three columns containing text characters, a halftone patch, and an enlarged portion of a vertical edge. No signal is embedded in the first row. The second and third rows are embedded using 20 cycle/inch and 40 cycle/inch sinusoids respectively. Here the embedding power was set very large to emphasize the effect of this type of embedding on different elements that may appear in a printed document. The embedded signal is most visible in the halftone patch, and can also be seen in vertical edges which are present in

Fig. 8. Effects of large amplitude exposure modulation. 1^{st} line no modulation, 2^{nd} line 20 cycles/in, 3^{rd} line 40 cycles/in.

many text characters and in borders of forms.

If the embedded document has any large midtone gray patches, the signal is easily detectable using Fourier analysis techniques. However, several issues are encountered when attempting to do this. One is the assumption that every portion of the image consists of a midtone gray level. White and black parts of the image, those which contain no toner or are saturated with toner, are not useful for detecting the embedded signal. In addition, synchronization of the signalling periods becomes difficult. The issue of synchronization can be solved by using Gold sequences and repeating each symbol multiple times within the image [29].

To detect the embedded signal, a scanned image is first segmented into multiple sub-images. The embedded data is estimated from each sub-image and is correlated with the set of all possible embedded symbols to determine the actual embedded symbol. Using a 5-bit Gold sequence, approximately 20 bits of data can be embedded per inch in an image. To embed information into a text document using laser modulation, a slightly different approach needs to be taken [30]. Looking again at Fig. 8, we notice that the embedded signal affects straight edges. In fact, An estimate of the edge profile will, in the ideal case, be similar to the embedded signal.

To make use of this observation, each line of text in a document is treated as a signaling period during which one symbol is transmitted. Detection of the symbols involves several steps. First the document is scanned at a sufficiently high resolution, typically 600dpi or higher. Next, all characters in each line of text are segmented from the scanned image. Each character is then filtered using a threshold edge

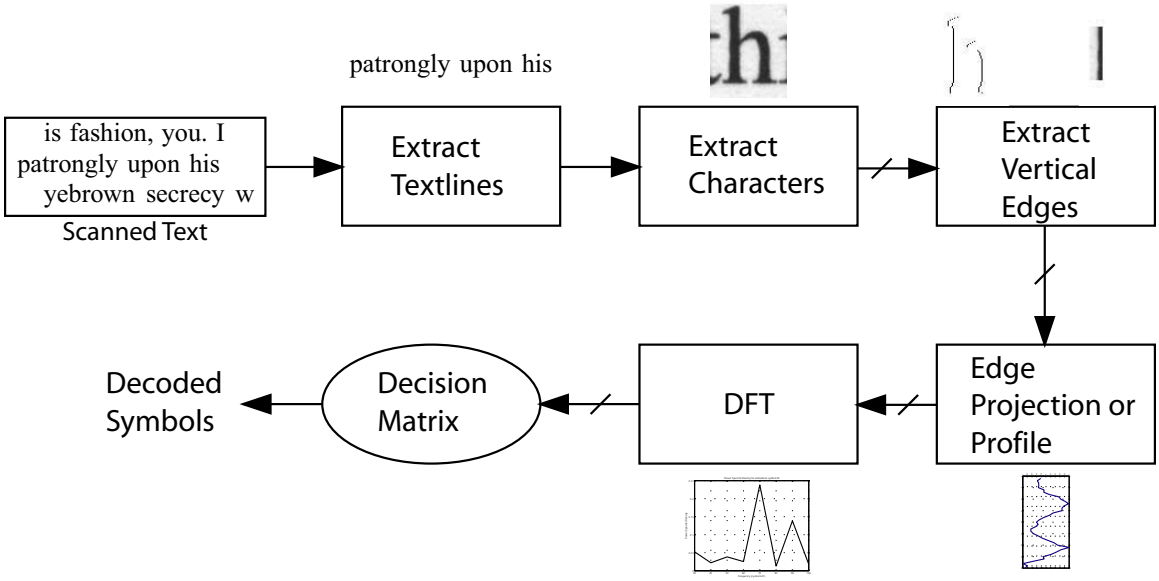

Fig. 9. Process for extracting embedded information from text.

detector and morphological operations to find all the left edges of the characters. A appropriate detector is then used to determine which symbol was embedded in the line. One such scheme is able to embed 7 bits per line of text or as much as 200-400 bits/page.

Embedding an extrinsic signature into a document containing neither text nor images, such as a form, requires a different approach from those presented for text and halftone images. Typical security documents such as bank notes, statements, and event tickets, are type of forms which typically contain a frame or border around the edge of the document. A similar technique as described for text embedding can be used to embed information into the vertical edge of a frame. However, because the frame is typically much longer than a text character and has no breaks, different encoding and detection schemes need to be employed.

ANTI-FORENSICS AND SPOOFING: Every security system has its limitations, and current techniques for securing a printed document or scanned image are no exception. Two types of attacks are possible. One where the signature is removed and another attack where the signature is replaced by another signature (spoofing). Other attacks such as a "scan-print" attack used by counterfeiters are unique to these types of devices. The success of these attacks is dependent upon the document or image content.

In the case of printed text documents, simply by scanning the document using optical character recognition (OCR) software to extract the text, and then re-printing it on another printer would remove any

extrinsic or intrinsic signature. However the document may then be labeled as "suspect" if a particular signature that should be in the document is not found in the document. Scan-print attacks could be detected by use of the signatures in the scanner and printer. Similarly, printed halftone images could be scanned, converted to continuous tone, and then re-printed after using standard watermarking attacks to remove any embedded watermark [31].

Spoofing the original printer or scanner intrinsic signature may be more difficult for signatures that originate at the device mechanism level since attacks would require modification of the device firmware. We have shown that it is possible to "replace" banding patterns in printers used to form intrinsic and extrinsic signatures but this type of attack would be very difficult for the average user to do. With respect to scanners some of the attacks reported for digital cameras that exploit the sensor pattern noise are possible [3], [4].

SECURITY PROTOCOL AND PRIVACY: There are two major components to any security system: security primitives and protocols. The primitives are tools and techniques, such as the data-hiding and feature extraction methods introduced above. The protocol describes how the security primitives are used to protect content. For example, a watermarking protocol would describe how the message to be embedded is processed, e.g. encrypted, before it is embedded in the document, and where the keys are maintained. Nearly every failure in a security system is due to a protocol failure. For example, a computer system may have a very secure password selection primitive. However, due to the complexity of the password, a user may write it on a slip of paper, and attach it to the computer. In this case, the protocol has failed, rather than the primitive. Printers and sensors are integral components of the digital document world. As described in this paper, many effective security primitives exist for printers and sensors. One of the future challenge is to integrate these primitives into security protocols that are needed for different application scenarios. A successful document security protocol will need to consider the strength and vulnerability of the security primitives as well as all workflow associated with the generation, distribution and storage of the document.

The methods presented in this paper have many applications in law enforcement such as tracking, counterfeiting, and child pornography. The downside is that they provide a mechanism for a simple device, a printer or a digital camera, to spy on its user. A typical user cannot turn off these signatures, particularly the intrinsic signature, without very detailed knowledge of how the device operates. This could have dire consequences for many important uses of these devices in our society. For example a whistleblower who would like to share documents with a regulatory agency could be in danger in that their printer could be identified as the one that produced the documents. A citizen who would like to

anonymously report a chemical spill using a digital camera is also threatened with possible discovery even though these acts are protected by Federal law (31 U.S.C. Sec. 3730(h)) and many state laws. It is also possible to develop signal analysis tools and system protocols that can be used to effectively defeat or turn-off a devices intrinsic and extrinsic signatures to protect a users privacy for legal and ethical uses of the sensor device. It is important to note that the intention is not to create a set of hacking tools that can be used to defeat the ability of the output of the sensor to be identified to a particular device since it is obvious that sensor forensics have many important legitimate uses.

CONCLUSIONS: The use of printers and scanners as an interface to the digital world in our society will not disappear any time during the foreseeable future. Security mechanisms are required for this unique interface just as security is required for digital media such digital images, audio, and video.

What is interesting and challenging about printers and scanners is that one can exploit how the devices generate their output to provide security features. Preventing forgeries and unauthorized duplication, as well as determining the source of illicit content, is just as important in the physical world as it is in the digital one. Printer and scanner forensics is a growing area of research building upon a multitude of disciplines ranging from image processing and communications, to mechatronics and psychophysics.

ACKNOWLEDGMENTS: This work was 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.

REFERENCES:

[1] M. Mukhtar, P. Meckl, and G. T.-C. Chiu, "Color registration error reduction in document scanner using iterative velocity command synthesis," *Proceedings of the 2008 ASME Dynamic Systems and Control Conference*, Ann Arbor,Michigan, October 2008.

[2] G. C. Holst, *CCD Arrays, Cameras, and Displays, Second Edition*. JCD Publishing & SPIE Press, USA, 1998.

[3] J. Lukas, J. J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205– 214, June 2006.

[4] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security,*, vol. 3, no. 1, pp. 74–90, March 2008.

[5] T. Gloe, E. Franz, and A. Winkler, "Forensics for flatbed scanners," *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX*, E. J. D. III and P. W. Wong, Eds., vol. 6505, no. 1. SPIE, 2007, p. 65051I.

[6] H. Gou, A. Swaminathan, and M. Wu, "Robust scanner identification based on noise features," *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX*, E. J. D. III and P. W. Wong, Eds., vol. 6505, no. 1. SPIE, 2007, p. 65050S.

[7] N. Khanna, A. K. Mikkilineni, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Scanner identification using sensor pattern

noise," *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, CA, January 2007.

[8] G. N. Ali, P.-J. Chiang, A. K. Mikkilineni, J. P. Allebach, G. T.-C. Chiu, and E. J. Delp, "Intrinsic and extrinsic signatures for information hiding and secure printing with electrophotographic devices," *Proceedings of the IS&T's NIP19: International Conference on Digital Printing Technologies*, vol. 19, New Orleans, LA, September 2003, pp. 511–515.

[9] A. K. Mikkilineni, O. Arslan, P.-J. Chiang, R. M. Kumontoy, J. P. Allebach, G. T.-C. Chiu, and E. J. Delp, "Printer forensics using svm techniques," *Proceedings of the IS&T's NIP21: International Conference on Digital Printing Technologies*, vol. 21, Baltimore, MD, October 2005, pp. 223–226.

[10] G. N. Ali, P.-J. Chiang, A. K. Mikkilineni, G. T.-C. Chiu, E. J. Delp, and J. P. Allebach, "Application of principal components analysis and gaussian mixture models to printer identification," *Proceedings of the IS&T's NIP20: International Conference on Digital Printing Technologies*, vol. 20, Salt Lake City, UT, October/November 2004, pp. 301–305.

[11] J. F. Oliver and J. X. Chen, "Use of signature analysis to discriminate digital printing technologies," *Proceedings of the IS&T's NIP18: International Conference on Digital Printing Technologies*, San Diego, California, September 2002, pp. 218–222.

[12] D. Wolin, "Document verification and traceability through image quality analysis," *Proceedings of the IS&T's NIP18: International Conference on Digital Printing Technologies*, San Diego, California, September 2002, pp. 214–217.

[13] E. Bernal, J. P. Allebach, and Z. Pizlo, "Improved pen alignment for bidirectional printing," *The Journal of Imaging Science and Technology*, vol. 51, no. 1, pp. 1–22, Jan./Feb. 2007.

[14] J. H. Lee and J. P. Allebach, "Inkjet printer model-based halftoning," *IEEE Transactions on Image Processing*, vol. 14, no. 5, pp. 674–689, May 2005.

[15] P. Doherty, "Classification of ink jet printers and inks," *J. Am. Soc. of Quest. Doc. Exam.*, vol. 1, no. 1, pp. 88–106, 1998.

[16] O. Arslan, R. M. Kumontoy, P.-J. Chiang, A. K. Mikkillineni, J. P. Allebach, G. T.-C. Chiu, and E. J. Delp, "Identification of inkjet printers for forensic applications," *Proceedings of the IS&T's NIP21: International Conference on Digital Printing Technologies*, vol. 21, Baltimore, MD, October 2005, pp. 235–238.

[17] V. Talbot, P. Perrot, and C. Murie, "Ink jet printing discrimination based on invariant moment," *Proceedings of the IS&T's NIP22: International Conference on Digital Printing Technologies*, Denver, CO, September 2006, pp. 427–431.

[18] S. J. Simske, J. S. Aronoff, M. Sturgill, F. Collins, G. Golodetz, and R. Israel, "Security printing deterrents: A comparison of TIJ, DEP and LEP printing," *Proceedings of the IS&T's NIP23: International Conference on Digital Printing Technologies*, Anchorage, AK, September 2007, pp. 543–548.

[19] G. Gupta, S. K. Saha, S. Chakraborty, and C. Mazumdar, "Document frauds: Identification and linking fake document to scanners and printers," *International Conference on Computing: Theory and Applications (ICCTA 07)*, March 2007, pp. 497–501.

[20] Y. Akao, K. Kobayashi, S. Sugawara, and Y. Seki, "Discrimination of inkjet-printed counterfeits by spur marks and feature extraction by spatial frequency analysis," *Proceedings of the SPIE International Conference on Optical Security and Counterfeit Deterrence Techniques IV*, R. L. van Renesse, Ed., vol. 4677, no. 1, 2002, pp. 129–137.

[21] J. T. Brassil, S. Low, and N. F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," *Proceedings of the IEEE*, vol. 87, no. 7, July 1999, pp. 1181–1196.

[22] M. S. Fu and O. Au, "Data hiding in halftone images by stochastic error diffusion," *IEEE International Conference on Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP 01)*, vol. 3, 2001, pp. 1965–1968.

[23] O. Bulan, V. Monga, G. Sharma, and B. Oztan, "Data embedding in hardcopy images via halftone-dot orientation

modulation," *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, January 2009.

[24] G. Sharma and S. Wang, "Show-through watermarking of duplex printed documents," *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VI*, vol. 5306, January 2004.

[25] M. Barni, C. I. Podilchuk, F. Bartolini, and E. J. Delp, "Watermark embedding: hiding a signal within a cover image," *IEEE Communications Magazine*, vol. 39, no. 8, pp. 102–108, August 2001.

[26] D. Kacker and J. P. Allebach, "Joint halftoning and watermarking," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1054–1068, April 2003.

[27] (2005, July) Investigating machine identification code technology in color laser printers. [Online]. Available: http://www.eff.org/wp/investigating-machine-identification-code-technology-color-laser-printers

[28] S. Suh, J. P. Allebach, G. T.-C. Chiu, and E. J. Delp, "Printer mechanism-level information embedding and extraction for halftone documents: New results," *Proceedings of the IS&T's NIP23: International Conference on Digital Printing Technologies*, Anchorage, Alaska, September 2007, pp. 549–553.

[29] P.-J. Chiang, A. K. Mikkilineni, E. J. Delp, J. P. Allebach, and G. T.-C. Chiu, "Extrinsic signatures embedding and detection in electrophotographic halftone images through laser intensity modulation," *Proceedings of the IS&T's NIP22: International Conference on Digital Printing Technologies*, Denver, CO, September 2006, pp. 432–435.

[30] A. K. Mikkilineni, P.-J. Chiang, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Channel model and operational capacity analysis of printed text documents," *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, CA, January 2007, p. 65051U.

[31] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks," *IEEE Communications Magazine*, vol. 39, no. 8, pp. 118–126, Aug 2001.