Signature-Embedding In Printed Documents for Security and Forensic Applications

Preeti Mahar

Email: udhveermahar12@gmail.com

Abstract- Despite the increase in email and other forms of digital communication, the use of printed documents continues to increase every year. Many types of printed documents need to be \secure" or traceable to the printer that was used to print them. Examples of these include identity documents (e.g. passports) and documents used to commit a crime. Traditional protection methods such as special inks, security threads, or holograms, can be cost prohibitive. The goals of our work are to securely print and trace documents on low cost consumer printers such as inkjet and electrophotographic (laser) printers. We will accomplish this through the use of intrinsic and extrinsic features obtained from modelling the printing process. Speci¯cally we show that the banding artifact in the EP print process can be viewed as an intrinsic feature of the printer used to identify both the model and make of the device. Methods for measuring and extracting the banding signals from documents are presented. The use of banding as an extrinsic feature is also explored.

Index Terms- document security, secure printing, printer identification, banding.

I. INTRODUCTION

In today's digital world securing di®erent forms of content is very important in terms of protecting copyright and verifying authenticity. Many methods[1]{[7] have been developed to protect audio, video, digital documents, images, and programs (exectable code).

In this paper, we will be concerned with the securing of printed documents, which we will refer to as \doc-uments". The securing of documents is not new. In 1282 AD physical paper watermarks began to appear.[8]These were created by placing thin wires in the mold used to create the paper. The purpose of these marks is to identify the paper maker or the speci¯c mold used to create the paper. By the early eighteenth century these types of watermarks started to appear in bank notes to deter counterfeiting and also on regular parchment to designate a trademark or a particular date or place.

Today, paper watermarking is still used as can be seen in most bank notes and some o±cial documents, but it is usually accompanied by other security features. Security ¯bers or threads can be embedded within the paper or woven into it during manufacture. Special inks which change color or react to certain chemicals which might be used to remark a document have been proposed.[9] Additionally, new methods using embedded holograms or microtext are being introduced.[10, 11] These methods are used to verify the authenticity of a document and usually do not carry any other information. For more detail on these types of security features.In digital data hiding, any information (a watermark), such as copyright and owner information, can be embedded within a media data element such as an image or video sequence.[4] The watermark could be visible or non-visible, but in either case should be easily recoverable from the watermarked data.[5] Additionally the watermark must be able to survive if the host data is manipulated.

We believe that a marking scheme analogous to digital watermarking but for documents is very important.

II. HIDING DATA WITH HALFTONE PATTERNS

The previous method deals with encoding information in text, but documents may also have halftone images. Halftoning is the process of converting a continuous tone image into an image having only a number of levels typically 2 for printed images.[17] When viewed from a distance, these images resemble the original. Numerous methods have been developed for watermarking halftone images. Most of these methods involve modifying the halftone patterns used when printing the image. The three basic methods are the use of multiple dithering matrices, conjugate halftone screens, or angular variation of the halftone screen.[18] In the ¯rst 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.[18] 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 the halftone screen can be generated and detected at.

Another recent method of data hiding with halftone patterns has been described in[19] in which watermarks are embedded in duplex printed pages such that when the page is held up to a light source a fake watermark will appear. This method relies on halftone images that are printed opposite each other on either side of the page

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 is also described in[20] which can be used for one sided printing with veri¯cation using a transparent screen.

III. DATA HIDING WITH WATERMARKING TECHNIQUES FOR CONTINUOUS TONE IMAGES

Watermarking images in documents can also be done using continuous tone image watermarking techniques.[4, 5, 7] These

methods ¯rst embed a watermark into the continuous tone image and then print it 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 when viewed as an attack channel. The watermarking method described in$_{21}$\{$_{23}$ has been shown to be very robust against many types of attacks, including the print-scan attack and those involving global a±ne or local non-linear transformations. Being able to survive these two types of transformations is important because a document might be wrinkled or torn. First a compressed and encrypted message is encoded into a reference watermark creating a small block. The block is then °ipped and mirrored to create a macroblock consisting of 4 copies of the original block. The purpose of the °ipping is to visually decorrelate the embedding structure and also to assist in later estimation of local non-linear transformations. The macroblock is then tiled and embedded into the image which is then printed.

An autocorrelation detection scheme as described in$_{24}$ can be used to estimate any global a±ne transformations that have been applied to the scanned document. Local non-linear transformations can then be estimated using a similar method within each macroblock.

Until recently, none of the methods which watermark continuous tone images before printing have explicitly taken into account the printing process itself. The method described in$_{25}$ jointly optimizes the printed image quality and the detectability of the watermark. This approach uses direct binary search (DBS) halftoning$_{26}$ and a spread spectrum watermark.$_{27}$ The halftoned image is modeled as a bitmap. Because the detection process relies on a reconstructed continuous tone version of the document, and not the speci¯c halftone patterns used in its creation, there are multiple bitmaps of the same watermarked image which will yield good detection results.

Assuming that the bitmap image is M £N pixels, there are then 2MN possible bitmaps, only a subset of which will visually resemble the original image data and simultaneously allow detection of the watermark. Each of these bitmaps will di®er in visual quality and the goal is to pick the one which best maximizes both visual quality and watermark detectability. This is achieved by using a modi¯ed version of DBS such that at each iteration both the watermark detectability and perceptual image quality metrics are used to jointly optimize the halftone image. This method is shown to be more 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.

IV. OUR APPROACH

At Purdue University we are developing forensic signatures for consumer printers based on knowledge of the printer process and the analysis of printed documents resulting from a given printer. Our intention is to develop these methods for both inkjet (IJ) and electro photographic (EP or laser) printers.$_{1}$We believe that secure printing is based on the concept that the printer output, the document, is an e®ective means for identifying features of the printer. These features, which are printer speci¯c, can be used for

document security. For example, in the case of a suspected forgery we ideally should be able to tell what type of printer was used to create the document. In our work at Purdue the focus is on extracting features from the document and developing methods to securely hide information in documents based on these features. We propose to develop two strategies for printer identi¯cation: intrinsic and extrinsic signatures.$_{1, 13}$

We are developing image analysis techniques to extract features from a printed document that can be used as an intrinsic signature. The intrinsic signature will be detected by scanning the printed page with a high resolution scanner and treating it as a high resolution image. We will then extract features from the image and use them to classify the document with respect to the printer. We will then use the features that describe the intrinsic signature to design the extrinsic signature.

In contrast to currently used document watermarking methods which embed the watermark into the document before it is printed, we propose to create the watermark by modifying the print process, this is the extrinsic signature. This will be accomplished by modulating the process parameters in the printer mechanism to encode identifying information such as the printer serial number and date of printing. We believe that moving this embedding step into the printer hardware will deter possible attempts to modify the hidden information before it is printed. If these steps were instead handled by a print driver or some other software beforehand, then a malicious user could reverse engineer the embedding software and re-engineer it to suit his own needs.

V. BANDING IN EP PRINTING

Our current work has focused on intrinsic feature detection of EP (laser) printers. In order to gain insight into the types of features that can be used to describe these printers, an understanding of the EP printing process is necessary. The ¯rst thing to note is that in the printed output from any printer there exist defects caused by electromechanical °uctuations or imperfections in the print mechanism.$_{13}$ Because these \print quality defects" are directly related to the printer mechanism, they can also be viewed as an intrinsic signature or feature of the printer.

A. Banding as an Intrinsic Feature

Figure 1 shows a side view of a typical EP printer. The print process has six steps. The ¯rst step is to uniformly charge the optical photoconductor (OPC) drum. Next a laser scans the drum and discharges speci¯c locations on the drum. The discharged locations on the drum attract toner particles which are then attracted to the paper which has an opposite charge. Next the paper with the toner particles on it passes through a fuser and pressure roller which melt and permanently a±x the toner to the paper. Finally a blade or brush cleans any excess toner from the OPC drum.

In EP printing, the major artifact in the printed output is banding which is de¯ned as the artifacts thatare due to quasiperiodic °uctuations in process direction parameters in the printer. These are primarily due to °uctuations in the angular velocity of the OPC drum and result in non-uniform scan line spacing. This causes a corresponding °uctuation in developed toner on the printed page.$_{28}$ The appearance of the banding artifact is 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 °uctuations in the printer mechanism, mostly from gear backlash. Because these °uctuations are related to the gearing, the banding frequencies present in the printed page should directly re°ect mechanical properties of the printer.

To measure the banding frequencies of an EP printer, mid tone gray level patches created with a line ¯ll pattern were printed and analyzed.[13] Figure 2 shows a 25% line ¯ll pattern. This pattern was printed on a set of EP printers and then each patttern was scanned at 2400dpi. Each scanned image, img (i; j), was then projected

Laser Beam
D Paper
C
B
A
F
E
Fused Toner
Particles
Pressure Roller
Fuser Roller
Transfer Roller
Process Direction
Developer
Roller
Cleaning Blade Charge Roller
OPC Drum

Figure 1. Diagram of the EP process: (A) charging, (B) exposure, (C) development, (D) transfer, (E) fus-ing, (F) cleaning

1/600 inch 3/600 inch

Figure 2. Midtone pattern 25% ¯ll used for banding

Characterization horizontally to produce proj(i) = P_j img(i; j) shown in Figure 3a. A Fourier analysis of the projection was then obtained and shown in Figure 3b which shows spikes at 132 cycles/inch and 150 cycles/inch

Table 1 show a list of printers and their principle banding frequencies as found by this method.

0 2000 4000 6000 8000 10000 12000 14000
5.85
5.9
5.95
6
6.05
6.1
6.15
6.2
6.25
6.3
x 105
i
proj(i)
Horizontal Projection of 25% Fill Pattern from HP lj6MP
(a) Projection of 25% ¯ll patern fromHP lj6MP
0 50 100 150 200 250
0
2
4
6
8
10
12
14
16
18
x 105
Frequency (cycles/inch)
Amplitude (graylevels)
FFT of Projection of 25% Fill Patch for HP lj6MP
(b) FFT of the projection showingpeaks at 132 and 150 cycles/inchFigure 3. Projection and FFT analysis of 25% ¯ll pattern printed on HP lj6MP

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. Our interest is to be able to detect these signals in text. This will require a di®erent processing technique due to the low SNR of the banding signal with respect to the text and because of the limited number of cycles of the banding signal which can be captured in the length of one text character.

B. Banding Modelling and Analysis

In this section we will describe our model of banding and our initial analysis approach. Our ultimate goal is to reliably detect the banding frequencies from a standard printed page. We believe it is important in some of our forensic applications to be able to do this without using speci¯c test documents.

i. Banding Modelling

Our model is shown in Figure 4. Two paths are shown in this ¯gure, one for processing actual documents, and another for processing ideal documents. These are referred to as the actual path and the ideal path respectively.

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

Table 1. Banding Frequencies for Several Printers.

PS
File
Print
PS −> TIFF Add Ideal
Banding
Scan Morphological
Filter
Morphological
Filter
Run
Extractor
Run
Extractor
Run
Analysis
Run
Analysis

nideal(i,j) yideal(i,j)

b

ideal

(i)

yactual(i,j) n^

actual

(i,j)

n^

ideal

(i,j)

Figure 4. Banding Analysis Model

A random document generator is used to generate full page text documents that we will use to characterize the printer. We used a modi¯ed version of a Markov chain random text generator29 (the \Monkey") which we trained on text available from the Gutenberg project.30 We used \The Adventures of Sherlock Holmes" by Sir Arthur Conan Doyle. The program ¯rst estimates the conditional probabilities of all the characters in the training data from order 0 to order 4. It then generates a user speci¯ed length of text following these transition probabilities and produces output into a LATEX formatted ¯le to allow easy formatting and conversion into PostScript (PS).

We refer to this system as the Forensic Monkey Text Generator (FMTG).

Following the actual path, we start with a PS representation of a document generated using the FMTGdescribed above. The PS ¯le is ¯rst sent to a printer which will create the printed document. This document is then scanned at 2400dpi and stored as a TIFF image which is then processed to estimate the banding frequencies .The ideal path is used to construct a simple model of the banding process and gain some insight into how the banding manifests itself in the printed document. The PS representation of the document is ¯rst converted using ghost view into a TIFF image at 2400dpi, the same resolution as is used in the scan step on the actual path. This image can be thought of as the ideal text, nideal(i; j), since it is binary with the background having gray level 0, or white, and the text having gray level 255, or black. It is assumed that 0=white and 255=black. Next an ideal banding signal is added to the ideal text to generate the image yideal(i; j) which will be the ideal representation of the output of the scan process in the actual path. All processing and analysis is performed on 1200x1200 pixel blocks. Figure 5 shows a block of ideal text. Let nideal(i; j) = ½ 253; nideal(i; j) belongs to a text character

0; else

(1)

where text characters have a gray level of 253 and the background has gray level 0. The reason for choosing not to represent the graylevel of the text as 255 will become apparent when we add the ideal banding signal. The origin is de¯ned as the top-left corner of the block with the i ¡ axis going downward and the j ¡ axis going toward the right.

Each block is then broken into slices nideal(i) for ¯xed j, an example of which is shown in Figure 6 corre-

sponding to the 596th slice marked in Figure 5. Within each slice we de¯ne runs, rideal

k (m), which are sections of the slice that are part of a text character and long enough to capture at least one cycle of the smallest banding frequency to be estimated. The subscript k

denotes the run number, starting with k = 1 for the ¯rst run in slice 1, and ending with the last run in slice 1200. The index m denotes the position in the run starting from m = 0. Next we add an ideal banding signal to nideal(i; j) to create yideal(i; j), the ideal representation of a block of text in the actual path. We will assume that the printer in the ideal path is an HP lj5MP, and that only the 37 cycles/inch banding signal is present. Figure 7 shows an ideal banding signal with an amplitude of 2 gray levels and frequency 37 cycles per inch as de¯ned by

bideal(i) = a ¤ sin(2¼f

i

dpi

); (2)

where a is the amplitude in gray levels, f is the frequency in cycles/inch, and dpi is the resolution of the signal in dots per inch. This signal only varies in the i direction because, as stated earlier, the banding signal is a print defect in the process direction only. The addition of the banding signal to the ideal block of text is a special process. The signal only manifests itself in printed areas meaning that in the case of the ideal text block it will only appear on top of a text character and not in the white background areas. To form the banded image, yideal(i; j), the following operation

is performed,

yideal(i; j) = ½ nideal(i; j) + b(i); if nideal(i; j) = 253

nideal(i; j); else (3)

where the banding signal is added only in printed areas. Figure 8 shows the same slice seen in Figure 6 but now with the added banding signal. Figure 9a shows the banded run from this slice. The average value of the run is approximately 253, and the banding signal itself is seen as a gray level variation between 251 and 255.

ii.   Banding Analysis

Since it is the banding signal that is of interest, a measure of the SNR between the banding signal and the \noise", which in this case is the text, might give some insight into what estimation techniques should be used. To simplify the situation, we will only examine a single slice. Additionally we will assume that the text character pro¯le is a square pulse with width 500 pixels and that the spacing between lines, or character pro¯les in the slice, is 300 pixels. This is representative of 12point text. Since the banding signal only appears in printed areas,we can safely examine a single 500 pixel run containing the pro¯le of one text character. The SNR is the ratio of 0 200 400 600 800 1000 1200

−3

−2

−1

0

1

2

3

i

Amplitude (in Graylevels)

Ideal Banding Signal b(i)=a*sin(2*□ *i*f/dpi), f=37(cycles/inch), dpi=2400(dots/inch)

Figure 7. Ideal banding signal with amplitude 2 and frequency 37 cycles / inch

0 200 400 600 800 1000 1200

0

50
100
150
200
250
300
i
Graylevel (0=white 255=black)
Slice yi d e a l(i,596)= ni d e a l(i,596) □ □ bi d e a l(i)
Top of letter 'l' Bottom of
letter 'l'
Top of letter 'o'
Inside of letter 'o'
Bottom of
letter 'o'
Graylevel 251
Graylevel 255
One Run rideal
k (m)
length 222

Figure 8. Slice from a block of ideal text with banding signal

the energy in the banding signal divided by the energy in the text pro¯le.

$$SNR = \frac{E_{banding}}{E_{textprofile}} = \frac{\sum_{i=1}^{500} b^2(i)}{\sum_{i=1}^{500} 255^2} = 6.2285 \times 10^{-8} \quad (4)$$

Clearly trying to extract the signal directly from the slices will be problematic, hence we process the runs instead of the slices. Extracting the runs from the ideal text is trivial since the text and background graylevel values are well de¯ned. The simplest method in this case is to use a thresholding technique to look for runs of pixels whose values are greater than 0. For actual text this will not work since the edges of the text are not well de¯ned and the background is not uniform graylevel 0. To remedy this problem, we ¯rst process the block of text with a 5x5 close-open morphological ¯lter. This operation will produce a mask which marks the locations of the text characters with graylevel $_{255}$, and the background with graylevel 0. This mask is then used to extract the runs and their locations are then mapped back onto the original block for analysis. Starting with the extracted run from an ideal slice, such as that shown in Figure 9a, ¯rst the mean of the run is removed forming

$$r_{ideal}^0 k (m) = r_{ideal} k (m) ¡ E[r_{ideal} k (m)]: \quad (5)$$

The mean shift removes the DC component of the signal, as shown in Figure 9b. Next the signal is windowed using a raised cosine window forming

$$r_{ideal}^{0w} k (m) = r_{ideal}^0 k (m) \times \cos(\frac{1}{4} \times \frac{m}{N ¡ 1} ¡ \frac{1}{2}) \quad (6)$$

where N is the length of the run $r_{ideal}^0 k$. Again the mean is subtracted from the signal to remove its DC componentto form $r_{ideal}^{0w0} k (m) = r_{ideal}^{0w} k (m) ¡ E[r_{ideal}^{0w} k (m)]: \quad (7)$This process of preparing each run for frequency analysis is shown in Figure 9 along with the FFT of $r_{ideal}^{0w0} k (m)$.

In this ideal case a peak is clearly seen centered at 36.92 cycles/inch, very near to the actual embeddedbanding frequency of 37 cycles/inch .This same methodology is used to analyze

actual text in our initial experiments. Figure 10 shows a block of actual text as well as a close up of the letter 'l' from the ¯rst line of text in the block. Notice in these images that the actual text is very noisy and the characters and background are not uniform in gray level. Shown inFigure 11 are three runs from this text block. The sharp peak in the ¯rst run, and the sharp dip in the second run correspond to an excess and de¯ciency of developed toner on the document. The ¯rst run has a peak near the expected banding frequency of 37 cycles/inch although the maximum amplitude was measured at 102.56

0 50 100 150 200 250
0
50
100
150
200
250
300
m
Amplitude (in Graylevels)
Plot of Run rideal
k (m) from yideal(i,596), mean=253.0387
(a)

0 50 100 150 200 250
−3
−2
−1
0
1
2
3
m
Amplitude (in Graylevels)
Plot of Run rideal,
k (m)
(b)

0 50 100 150 200 250
−3
−2
−1
0
1
2
3
m
Amplitude (in Graylevels)
Plot of Windowed Run r ideal,w
k (m) and Raised Cosine Window length 222, mean=−0.0262
(c)

0 50 100 150 200 250
−3
−2
−1
0
1
2
3
m
Amplitude (in Graylevels)

Plot of Windowed Run rideal 'w'

k

(d)

0 10 20 30 40 50 60 70 80 90 100

0

0.2

0.4

0.6

0.8

1

1.2

1.4

Frequency (cycles/inch)

One sided Fourier Transform of rideal 'w'

k (m), maximum at 36.92 cycles/inch

Amplitude

(e)

Figure 9. Processing of runs: a) Original Run rideal

k (m), b) rideal0

k (m) = rideal

k (m)¡E[rideal

k], c) rideal0w

k (m) = rideal0

k (m)¤

cos(¼ ¤

m

N¡1

¡

¼

2), d) rideal0w0

k (m) = rideal0w

k (m) ¡ E[rideal0w

k], e) FFT of rideal0w0

k (m)

(a) (b)

Figure 10. a) Block of text from HP lj5MP b) Letter 'l' from ﬁrst line

cycles/inch. The second run has a peak located at 28.13 cycles/inch. The third run has a peak at approximately 42 cycles/inch. From our analysis of the runs in actual text, we believe that it is possible to estimate the banding frequency using our model. We are currently examining weak signal detection methods for extracting the banding frequency.

130

140

150

160

170

180

190

0 50 100 150 200 250

Graylevel

m

r5(m), location i=581 j=898, length 210,

mean=1.800048e+02

(a)

180

182

184

186

188

190

192

194

196

198

200

0 50 100 150 200 250

Graylevel

m

r15(m), location i=188 j=473, length 210,

mean=1.876857e+02

(b)

176

178

180

182

184

186

188

190

0 50 100 150 200 250

Graylevel

m

r20(m), location i=185 j=478, length 212,

mean=1.843066e+02

(c)

0

0.5

1

1.5

2

2.5

3

0 10 20 30 40 50 60 70 80 90 100

Amplitude

Frequency (cycles/inch)

R 'w'

5(f), location i=581 j=898, length 210

max 102.56

37 cpi

(d)

0

0.2

0.4

0.6

0.8

1

1.2

1.4

1.6

0 10 20 30 40 50 60 70 80 90 100

Amplitude

Frequency (cycles/inch)

R 'w'

15(f), location i=188 j=473, length 210

max 28.13

37 cpi

(e)

0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0 10 20 30 40 50 60 70 80 90 100
Amplitude
Frequency (cycles/inch)
R 'w'
20(f), location i=185 j=478, length 212
max 8.21
37 cpi
(f)

Figure 11. a-c) Runs from actual text Figure 10a, d-f) Corresponding FFT of the processed runs a-c

C. Banding as an Extrinsic Signature

We have also examined the possibility of using banding as an extrinsic feature. Prior work has been reported on reducing the banding artifacts in the print process by controlling either the OPC drum velocity itself or modulating the laser pulse width as a function of the OPC drum velocity.28, 31 In the ¯rst method, a closed loop controller varies the velocity of the motor controlling the OPC drum based on the real time velocity that is measured using an encoder. The second method uses the fact that the velocity of the OPC drum dictates the scan line spacing assuming that the laser scanning speed is constant. When the OPC drum velocity is low, the scan lines are closer together and so the pulse width is decreased to reduce the amount of developed toner on the printed document. When the OPC drum velocity is high, the scan lines will be further apart and so the pulse width is increased to increase the amount of developed toner on the printed document. Both methods have been shown to work very well.

Using either of the banding reduction methods, it would be possible to modulate any existing bandingfrequencies in the print process to encode information. Additionally we can inject arbitrary arti¯cial banding frequencies into a document. We have been successful in embedding arti¯cial banding frequencies into a document by using the ¯rst method. Because of the electromechanical limitations imposed by the motor controlling the OPC, we have not been able to inject frequencies higher than 50 cycles/inch. We are currently working with the second method which should allow the injection of frequencies above 100 cycles/inch.

VI. CONCLUSION

Using print quality defects as an intrinsic signature of a printer is possible as shown for banding artifacts in EP printers. We believe that by successfully extracting the banding features from a document it is possible to classify the document based on the speci¯c make and model of device which created it. We need to better model this process by employing more sophisticated statistical analysis tools.