Detecting Fraudulent Bank Checks

Saheb Chhabra, Garima Gupta, Monika Gupta, Gaurav Gupta

Chapter 14

DETECTING FRAUDULENT BANK CHECKS

Saheb Chhabra, Garima Gupta, Monika Gupta and Gaurav Gupta

Abstract Bank checks have been subjected to fraud for centuries. Technological advancements enable criminal actors to perpetrate innovative frauds that are very difficult to detect. One example is the use of erasable ink that allows alterations to be made to a bank check without raising suspicion. Another example is the misuse of a victim's handwritten signature by scanning it and then printing on a check. Since most banking systems accept scanned copies of checks for clearance, identifying erasable ink alterations and printed signatures on digital images can be very challenging. This chapter describes automated, low-cost, efficient and scalable solutions to these problems. A solution is proposed for determining whether or not a check is genuine or merely printed. A solution for detecting erasable ink alterations localizes the erased regions in the visible light spectrum. A solution for detecting printed signatures focuses on the high-density noise introduced by scanners and printers.

Keywords: Bank check fraud, check alteration, check forgery, image processing

1. Introduction

Rapid advances in modern scanning technology have greatly simplified the task of converting documents to a digital format. Some digitized documents are very important and their unauthorized use could result in monetary, organizational, social or individual losses. Criminal entities often alter or counterfeit documents for malicious purposes. The wide availability of high-resolution scanners and printers has made it very easy for criminals to carry out alterations and produce high-quality counterfeits. It is very difficult for an ordinary person – sometimes, even document experts – to distinguish between genuine and counterfeit specimens with the naked eye. Bank checks are examples of high-value

documents that have been leveraged in a variety of frauds for centuries, but more so in recent years due to the availability of high-resolution scanners and printers and the acceptance of scanned copies of checks for clearance by banks.

Document fraud can be classified as static document fraud or dynamic document fraud. A static document holds the same information that was recorded on it at the time it was proclaimed usable, until the time it is declared invalid. A static document contains a combination of fixed and unique information. Examples of static documents are academic transcripts, banknotes, printed invoices, birth certificates, marriage certificates, driver's licenses and passports. A common way of perpetrating fraud involving a static document – aside from tampering – is to scan the original, make changes using a software tool and print a high-quality fraudulent copy.

A dynamic document is similar to a static document, except that it has a provision for the issuing party to write in or mark additional information (using a pen or a stamp) before the document is declared usable. Examples of dynamic documents are bank checks, examination forms and visas. A dynamic document fraud typically involves an alteration of the content generated by the issuing party for malicious reasons. A fraudster could generate a base document (i.e., dynamic document before the issuing party writes on it) using a technique for counterfeiting a static document and then write the desired content before the document is declared usable. Alternatively, a fraudster could write the desired content on a genuine base document. Yet another method of conducting dynamic document fraud is to alter the content created by the issuing party using physical means such as erasing, chemical washing or overwriting. Dynamic document fraud detection is a much more complex problem than static document fraud detection.

According to the Australian Payment Clearance Association [2], losses due to fraudulently-altered checks in 2015 were 80% more than the losses in 2013. Moreover, losses due to non-originated counterfeit checks in 2015 (i.e., fakes produced on counterfeit paper via laser printing or desktop publishing) registered a three-fold increase over 2013. Meanwhile, the Reserve Bank of India [15] reports that 1,197.2 million bank checks were cleared during the 2015-2016 fiscal year. In another report, the Reserve Bank of India [14] estimates that losses due to bank fraud nearly doubled from INR 10.071 billion during the 2013-14 fiscal year to INR 19.361 billion during the 2014-15 fiscal year.

Technological advancements in printing and scanning have enabled fraudsters to perpetrate innovative frauds that are difficult to detect. One example is the use of erasable ink that enables a variety of al-

terations to bank checks. Another example is forging a handwritten signature by scanning it and printing it on a check. Most banks accept scanned copies or digital photographs of customer checks for rapid and convenient online clearance. Identifying check alterations that leverage erasable and printed signatures in digital images of checks received by a bank can be very challenging. In addition to being accurate, check fraud detection solutions should be fast and inexpensive.

This chapter proposes efficient, inexpensive and scalable methods for detecting bank check fraud. One method determines if a check is genuine or printed. Another method detects check alterations by focusing on erased regions using the visible light spectrum. A third method distinguishes printed signatures from real handwritten signatures based on high-density noise introduced by scanners and printers.

2. Related Work

Counterfeit documents are typically detected by human experts who manually analyze suspect documents using a microscope and video spectral comparator, a process that is time-consuming, inefficient and non-scalable. Several automated methods have been developed to identify counterfeit documents. Gupta et al. [6] have identified several characteristics of printed documents that distinguish them from genuine documents. They discovered that the unique color count in a printed document is much larger than that in a genuine document. They also analyzed variations in intensity and the use of the gray level co-occurrence matrix to identify printed documents; this work has indirectly helped develop the proposed method for identifying printed checks. Furthermore, after a check is identified as a printed copy, the approach presented in [7] may be used to forensically link it to a source printer.

Garain et al. [4] have proposed a general framework for authenticating security documents. Their approach extracts color features and statistical features from check images and uses them to distinguish fake documents from genuine documents. Kumar et al. [9] have developed a method for authenticating bank checks. This approach uses color features such as the 2-D histogram of hue-saturation as well as texture features.

Other researchers [10, 16, 17] have proposed techniques for distinguishing counterfeit (primarily printed) documents from genuine documents. Rajendar et al. [13] have focused on the manipulation of digital information during the check clearing process. However, their approach differs from the current work in that they do not address the task of detecting physically-altered checks on which erasable ink has been used.

Abd-ElZaher et al. [1] have deciphered information written in erasable ink that was removed using the eraser attached to a magic pen. They use a chemical solution (NaOH) and infrared radiation from a VSC-600 scan converter to detect alterations. However, their approach, which requires manual human analysis, is expensive, time-consuming and non-scalable.

Deng et al. [3] have studied trace copy forgery detection of handwritten signatures. Their efficient approach uses wavelet transforms for offline handwritten signature verification. Other researchers [8, 11, 12, 18] have developed methods for detecting and/or verifying forged and imitated signatures. However, the current work is unique because no published research has specifically addressed the problem of analyzing handwritten signatures versus printed signatures on scanned checks.

3. Experimental Setup

This research has sought to identify credible image processing features from scanned bank check samples that could help determine whether or not the checks are genuine. Interviews with experts provided valuable information about the types and nature of check frauds. Four features were considered: (i) pantograph; (ii) microline; (iii) user-written content; and (iv) signature. In the experiments, counterfeit checks were replaced with printed checks that were generated by printing high quality scanned blank checks using laser and inkjet printers. Also, fraudulent checks, which are referred to as altered checks in this work, were created using a magic pen to write information such as the payee name, amount (of money) in words and amount (of money) in numbers. A magic pen is a pen whose ink can be removed from a piece of paper using the eraser provided with the pen.

Additionally, the experiments evaluated checks that had printed signatures instead of handwritten signatures. Genuine and printed signature checks from four Indian banks, two public banks (SBI and PNB) and two private banks (AXIS and HDFC), were used in the experiments. An important point is that some premium customers receive permission from banks to print their signatures on checks (e.g., corporate executives who sign company checks). All other checks with printed signatures are potentially fraudulent. Therefore, checks with printed signatures are scrutinized carefully by bank personnel.

Printed check and altered check samples used in the experiments were created based on information obtained from experts and in the supporting literature [1]. The sample checks were scanned at 600 dpi resolution using a Canon 9000F Mark II flat-bed scanner. Two printed check samples were generated for each genuine check using an HP Color LaserJet

Table 1. Check features and regions of interest.

Features	Regions
Pantograph	1
Microline	3
Alteration	4
Signature	1

Pro MFP M177 laser printer and a Brothers DCP-T500W inkjet printer. The 600 dpi resolution was selected for scanning because it is the industry standard (all the banks whose checks were used in this study process checks at this resolution). Additionally, the 600 dpi resolution provides all the feature values that can be processed in a reasonable time. The legacy 300 dpi resolution produces scanned checks with poor or missing features while the higher 1200 dpi resolution requires significant scanning time and processing cost. Nevertheless, experiments were also conducted on scanned check samples at 300 and 1200 dpi resolutions. Altered check samples were created by writing information on the checks using a magic pen, erasing some of the information and writing new information using the same pen.

Table 1 lists the four primary features of checks examined in this research: (i) pantograph; (ii) microline; (iii) alteration; and (iv) signature. Each feature has one or more regions of interest (ROIs), yielding a total of nine regions of interest.

Table 2. Check samples and scanned images examined in this study.

Bank	Genuine	Printed		Altered	Printed Signature		Total	Sub-Images per Sample	Total Processed
		Laser	Inkjet		Bank	Self			
SBI	10	10	10	10	3	10	53	9	477
PNB	10	10	10	10	1	10	51	9	459
AXIS	10	10	10	10	0	10	50	9	450
HDFC	10	10	10	10	1	10	51	9	459
Total									1,845

Table 2 provides information about the check samples and scanned images examined in this study.

4. Fraud Detection Methodology Overview

Checks were scanned at 600 dpi resolution (Figure 1). Each check was aligned horizontally in order to be accepted as input. The Canon

Figure 1. SBI bank check image showing sub-regions.

9000F Mark II scanner used in the experiments automatically corrects the alignment of a check image. However, bank personnel typically use software tools that ensure the proper alignment of check images before they are processed.

The first step involved the extraction of the regions of interest for localizing features such as the pantograph, microline, payee name, amount in words, amount in figures and signature (Figure 1). Predefined margins were created for checks from each bank so that the required features could be extracted in a convenient manner.

After the regions of interest were extracted, the check fraud detection workflow presented in Figure 2 was applied to the scanned images. The workflow comprises three parallel blocks.

The first block in the workflow is designed to identify whether or not a check has been printed. The processing focuses on one region for the pantograph and three regions for the microline. Three regions are used for the microline in order to deal with checks that have been handled roughly (i.e., old checks and folded checks).

The second block is designed to identify whether or not a check has been altered. The identification of alterations focuses on four regions of interest, payee name, amount in words (line 1), amount in words (line 2) and amount in figures.

The third block is designed to determine whether or not the signature on a check has been printed. It focuses on a single region of interest corresponding to the signature.

The outputs of the three blocks may be presented to bank security personnel to verify whether or not a check is genuine. In the case of

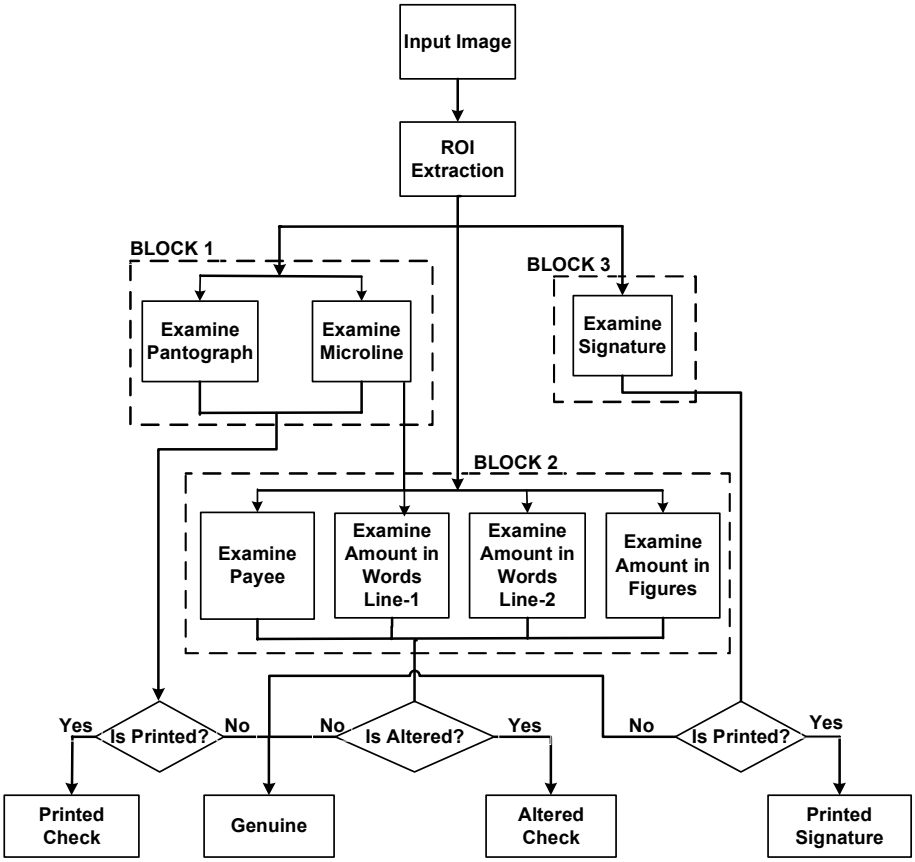


Figure 2. Check fraud detection system workflow.

an altered check, the fraud detection workflow also identifies the check regions that were modified.

5. Details of the Fraud Detection Methodology

This section presents the details of the check fraud detection methodology, including the underlying theory.

5.1 Check Pantographs

A pantograph is an anti-copying security feature printed on a bank check. It contains the word VOID that is hidden by artwork. The word VOID becomes visible when a scanned bank check is printed or a check is photocopied, indicating that the check is not genuine.

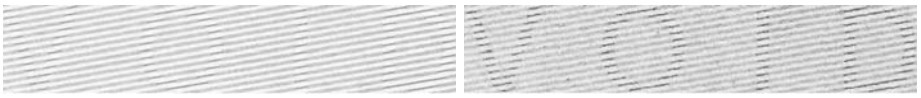


Figure 3. Pantographs on genuine (left) and printed checks (right).

The following observations were made upon studying genuine and printed checks.

- The word VOID is much more visible on a printed check compared with a genuine check (Figure 3).
- Some broken lines are seen on a printed check because standard printers are unable to print at very fine resolutions.
- The noise induced by a printer (especially an inkjet printer) is clearly visible to the naked eye.

Based on these observations, two sub-features, surface roughness and unique color count (UNCC), were selected to distinguish between genuine and printed pantographs. Significant increases in surface roughness and unique color count occur due to the colored dots (noise) that are typically generated when printing with a laser or inkjet.

Surface Roughness Sub-Feature. This sub-feature captures the roughness of a pantograph by taking the sum of the absolute gradients of the grayscale image I_G of the pantograph along the horizontal axis. The sum is then divided by the size of the image:

$$Roughness = \frac{\sum abs(G_x)}{Image\ Size} \tag{1}$$

where G_x is the gradient of the grayscale image and Image Size = image rows $\times$ image columns.

Unique Color Count Sub-Feature. This sub-feature expresses the total number of unique colors present in an image. Let $S_{xy} = f(x, y)$ be the intensity value at location (x, y) where $S_{xy} = [R_{xy}\ G_{xy}\ B_{xy}]$ is a row vector. Then, the matrix M is created by placing each intensity value in a separate row:

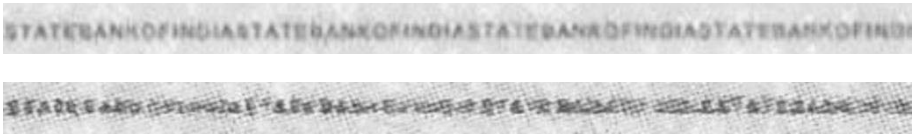


Figure 4. Microlines on genuine (top) and printed checks (bottom).

$$M = \begin{bmatrix} S_{11} \\ S_{12} \\ . \\ . \\ S_{1n} \\ . \\ . \\ S_{mn} \end{bmatrix} \tag{2}$$

The unique color count is the number of unique rows (each representing a unique color) in matrix M.

5.2 Check Microlines

The microline security feature is a micro-printed line of text on a check. The micro-print is miniaturized to the extent that the text cannot be read with the naked eye; instead, it appears as a complete or broken line. The font size of microline text is too small for it to be printed clearly by normal printers available in the market.

Figure 4 shows a genuine microline (top) and a printed microline (bottom).

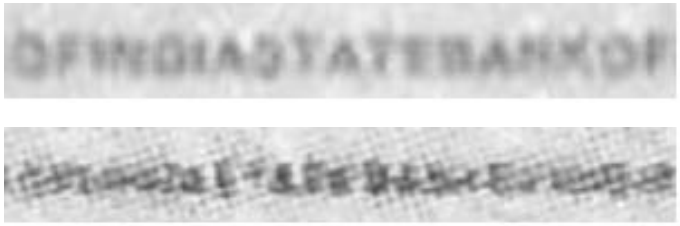
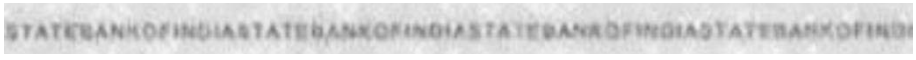


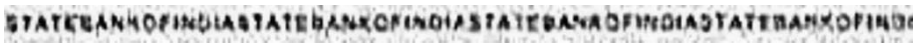
Figure 5. Zoomed views of microlines on genuine (top) and printed checks (bottom).

Figure 5 shows the zoomed views of the genuine and printed microlines shown in Figure 4.



(a) Original image.

(b) Intermediate line image.



(c) Final sharpened image.

Figure 6. Original, intermediate and image-sharpened microlines.

The following observations were made upon studying microlines on genuine and printed checks.

- The microline in a printed check appears as a complete line.
- The characters in the original microline are deformed in the microline of a printed check, where the letters merge with each other.

Optical character recognition (OCR) was performed on the check microlines using a Tesseract OCR engine (version 3.02) [5]. The hypothesis was that the number of consecutive pairs of characters obtained by optical character recognition of a printed microline is very small compared with that of the genuine microline. The reason is that multiple character deformities occur when printing a microline. The detection method involved the following steps:

- **Pre-Processing:** The microline was segmented and programmatically enhanced before the Tesseract OCR engine could process it. Since the segmentation process is highly dependent on the color of the microline, the goal of pre-processing was to highlight the microline and completely suppress the background.

  Let $F(x, y)$ be the original colored image (Figure 4) and S_{xy} be the intensity value at location (x, y) where $S_{xy} = [R_{xy}\ G_{xy}\ B_{xy}]$. In order to extract the required region (color of the microline, dark blue in this example) in the image $F(x, y)$, the original RGB image was converted to an HSV (hue, saturation, value) image and the saturation-channel image was processed because the microline region had a high saturation.

  The saturation-channel image (Figure 6(a)) was converted to a binary image using the Otsu threshold T (Figure 6(b)), which was then processed by applying dilation to merge the characters and

create a line image (Figure 6(c)). The sum of each row of the line image was then computed. The rows with sum values greater than 90% of the column of the line image were indexed. The indexed rows were then identified in the original image to produce an image containing only the microline text. Image sharpening was applied to enhance the microline and make the characters in the extracted line more recognizable by the Tesseract OCR engine (Figure 6(c)).

- **Feature Extraction:** Thirty images of the text in the microlines of checks from the four banks (e.g., STATE BANK OF INDIA on an SBI check) were provided to the Tesseract OCR engine. The engine processed each enhanced microline image and stored the output in a text file. Next, successive windows of three consecutive characters of the microline text were selected and matched against the optically-recognized characters stored in the text file. A "hit" occurred if all three characters matched correctly (i.e., they were recognized correctly by the engine); otherwise, a "miss" was recorded. Note that the windows started from the beginning of the microline and terminated at the end of the microline.

The experiments revealed that a genuine microline had on average more than six hits per 100 optically-recognized characters. In contrast, a printed microline check had almost no hits. It is anticipated that the accuracy of the microline feature could be improved with rigorous training of the Tesseract OCR engine for bank-specific check samples.

5.3 Check Alterations

A check alteration involves adding and/or replacing information on a check for malicious purposes. Altering bank checks is one of the easiest ways to perpetrate check fraud. This work focuses on the detection of erasable ink or removable ink used to alter bank checks. A fraudster often uses a magic pen with erasable ink; the ink is easily removed using the eraser attached to the end of the pen. The fraudster then offers the magic pen to the check writer to fill out the check; following this, certain information (e.g., payee name) is erased and replaced, and the resulting fraudulent check is submitted for clearance.

The following observations were made upon studying altered checks:

- Alteration of a check using a magic pen eraser affects the texture of the region of the check.

- The luminance and contrast of the check region are also affected and can be distinguished from the rest of the check.

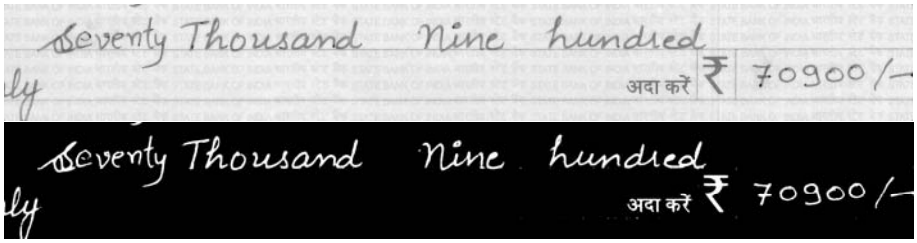


Figure 7. Original image (top) and text masked image I_M (bottom).

The following detection method based on gamma correction identifies the regions where an eraser was used:

- **Pre-Processing:** The four regions of interest – payee name, amount in words (line 1), amount in words (line 2) and amount in figures – were segmented based on the bank-specific margins.

  Let $f(x, y)$ be the original RGB image (top of Figure 7) and B_{xy} be the blue channel of image $f(x, y)$. The grayscale image $G(x, y)$ must be subtracted from B_{xy} in order to extract the dominant blue color region image I_B. This enables the extraction of the luminance from the normalized blue channel image B_{xy} (note that negative values are truncated). The dominant blue color region image I_B is given by:

$$I_B = B_{xy} - G(x, y) \tag{3}$$

  The highlighted image I_B was converted to the text masked binary image I_M (bottom of Figure 7) using the Otsu threshold T. The masked image I_M was used to remove the text region in further processing. Note that, although the experiments were only conducted for the most commonly used blue and black inks, the feature extraction method used in this work is applicable to any color of ink.

- **Feature Extraction:** Identification of the altered region involves the application of the gamma correction method followed by post-processing. Let $S_{xy} = f(x, y)$ be the intensity of an image at location (x, y) where $S_{xy} = [R_{xy}\ G_{xy}\ B_{xy}]$. Then, the gamma-corrected image is given by:

$$I_G = cS^{\gamma} \tag{4}$$

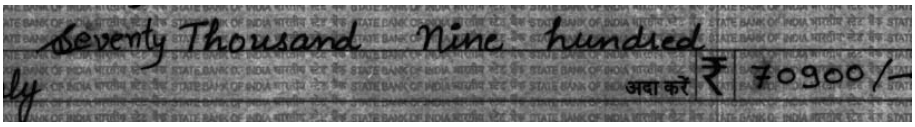


Figure 8. Gamma-corrected image I_G.

Figure 9. Gamma-corrected binary image I_{GB}.

Figure 10. Image showing the erased region.

where c and γ ($\gamma > 1$) are positive constants.

Figure 8 shows the gamma-corrected image I_G. Since the background of the image belongs to a brighter region, the value of γ must be greater than one to increase the contrast. The experiments used $\gamma = 9$.

The blue channel of the gamma-corrected image I_G was converted to a binary image, primarily because the background was blue. The noise from the binary image was then removed to obtain the gamma-corrected binary image I_{GB}.

Figure 9 shows the gamma-corrected binary image I_{GB} containing only the text and the erased region.

Finally, the masked image I_M was subtracted from I_{GB} to obtain the erased region. Figure 10 shows the image of the erased region.

5.4 Printed vs. Handwritten Signatures

A signature is a common feature in bank checks, certificates and other legal documents. When clearing a check, a bank attempts to match the signature on the check against a pre-stored scanned signature of the account holder. Several researchers have focused on the problem

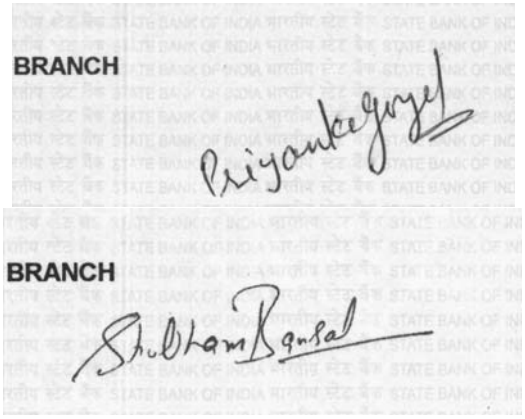


Figure 11. Handwritten signature (top) and printed signature (bottom).

of distinguishing between genuine and forged handwritten signatures. However, little, if any, research has attempted to distinguish printed signatures from handwritten signatures.

Figure 11 shows images of a handwritten signature (top) and printed signature (bottom). In order to distinguish between the two types of signatures, ideas were drawn from research that attempts to differentiate between printed characters and handwritten characters [2]. In particular, the research revealed that high-density black and dark colored dots are present in printed characters whereas handwritten characters have no such dots.

In a bank check clearance system, scanned copies of the printed signature and genuine signature are compared. Thus, noise from the scanner is present in both scanned samples.

In the case of a check with a genuine signature, the check is scanned to produce the "original" scanned signature for verification. However, in the case of a check with a printed signature, a genuine signature is first scanned and the scanned image is then printed on the check. When the check with the printed signature is to be verified, it is scanned to produce the "candidate" signature for verification. This leads to three distinct noise sources: (i) noise generated when scanning the signature N_S; (ii) noise generated when printing the signature N_P; and (iii) noise generated when scanning the signature for verification N_V.

In the case of a handwritten signature, only the scanner noise N_V (dark colored dots) is present. However, in the case of a printed signature, the noise introduced is amplified, corresponding to $N_S + N_P + N_V$.

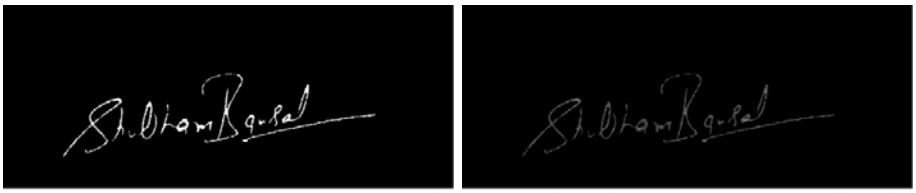


Figure 12. Mask image (left) and signature region image (right).

Therefore, the correlation of the RGB channel pixels in a printed signature is much less than that for a genuine signature.

The following correlation-based method was used to distinguish printed signatures from handwritten signatures:

- **Pre-Processing:** The first step was to segment the signature text region. Only the blue color channel was considered in the experiment, but the approach is applicable to the other channels. Note that the method for segmenting the blue color text in the signature region was the same as that used for check alteration detection.

  The mask image I_M (Figure 12 (left)) was superimposed over the original image to obtain the signature region image I_S (Figure 12 (right)).

- **Noise Removal:** The scanner introduces noise in a scanned image due to minute imperfections and dirt on the scanner lens and/or camera. A noise removal filtering function (discrete wavelet transform) was used to remove the noise from the image. Applying the discrete wavelet transform to the signature region image I_S yielded the discrete wavelet transform coefficients for the four sub-bands (approximate, vertical, horizontal and diagonal). The image generated through the approximate sub-band I_A was selected; this image contains low-frequency components indicating that the unwanted noise was removed.

- **Feature Extraction:** After obtaining the approximate sub-band image I_A, its RGB planes (I_{R_A}, I_{G_A}, I_{B_A}) were converted to separate column vectors and stored in a matrix M. The zero rows in M were removed because they belong to the background. Next, the cross-correlation C_{xy} was calculated for I_{R_A}-I_{G_A}, I_{R_A}-I_{B_A}

Table 3. Pantograph results for SBI checks.

ID	Genuine		Printed			
			Laser		Inkjet	
	UNCC	Roughness	UNCC	Roughness	UNCC	Roughness
1	21402	14.56680	40309	31.15814	53481	46.73548
2	17828	16.77730	41026	34.95251	55845	47.81659
3	19808	17.27510	42947	30.54739	52846	44.30893
4	23949	19.92390	46798	31.84794	57262	47.74739
5	18905	18.23660	39749	30.84759	54736	42.93744
6	24237	16.41492	41449	32.85495	52846	48.47393
7	21415	19.62349	42137	31.95751	50746	45.17336
8	20757	17.06158	46583	33.84748	51746	43.58479
9	17030	17.63441	38596	30.85754	48364	41.28025
10	24511	18.47682	43957	35.75568	59791	48.85941

and I_{G_A}-I_{B_A} using the equation:

$$C_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad (5)$$

This yielded three correlation values, C_{RG}, C_{RB} and C_{GB}, corresponding to the R-G, R-B and G-B channels, respectively. The high noise $N_S + N_P + N_V$ in a printed signature resulted in low correlation values between the channels. On the other hand, a handwritten signature with low noise N_V yielded high correlation values between the channels.

6. Experimental Results

This section describes the experimental results obtained by applying the methods proposed for detecting printed checks, altered checks and printed signatures.

6.1 Check Pantograph Results

Table 3 shows the pantograph results for SBI checks. The results clearly show that the unique color count (UNCC) and surface roughness values are high for printed checks. Since inkjet printers produce more noise than laser printers, the inkjet printer results have very high unique color counts and surface roughness values.

Table 4. Microline results for SBI checks.

ID	OCRed Characters	Matched Three Consec. Letters	OCRed Characters	Matched Three Consec. Letters
1	100	9	100	0
2	100	7	100	0
3	100	12	100	0
4	100	8	100	0
5	100	11	100	0
6	100	14	100	0
7	100	9	100	0
8	100	20	100	0
9	100	7	100	0
10	100	9	100	0

6.2 Check Microline Results

Table 4 shows the microline results for SBI checks. Note that the optical character recognition output corresponding to the printed microline text in the fifth (last) column has no matches in all ten test cases (i.e., no consecutive three letters from the original microlines matched the optical character recognition outputs). This is because the shapes of characters in the microline text were deformed during the printing process.

6.3 Check Alteration Results

The process for identifying check alterations is described in Section 5.3. A check is determined to be altered when an altered segment is present in the check. The threshold value used to classify alterations was a 200-pixel cluster (Figure 10). If the cluster size in a suspect check image is greater than the threshold, then the check is classified as an altered check. Note that the threshold depends on the handwriting of an individual. Since compact handwriting requires less space for alteration, a lower threshold would be needed.

6.4 Printed vs. Handwritten Signature Results

The results in Table 5 clearly indicate that printed signatures have low correlation values C_{RG} and C_{RB} for the R-G and R-B channels, respectively. The reason is the high noise density introduced by the scanner and printer.

Table 5. Signature results for synthetic SBI checks.

ID	Handwritten			Printed (Generated)		
	C_{RG}	C_{RB}	C_{GB}	C_{RG}	C_{RB}	C_{GB}
1	0.948287	0.883214	0.838135	0.461677	0.192432	0.941885
2	0.993438	0.892849	0.947063	0.471177	0.361397	0.981709
3	0.936733	0.811338	0.825890	0.322946	0.217322	0.983191
4	0.992668	0.909226	0.874532	0.778200	0.444900	0.868800
5	0.956653	0.853285	0.827092	0.876000	0.499600	0.861900
6	0.972817	0.977369	0.922073	0.769200	0.466300	0.927000
7	0.986645	0.825093	0.794458	0.437484	0.351723	0.937494
8	0.985777	0.816379	0.763721	0.539573	0.289031	0.967497

Table 6. Signature results for real SBI checks.

ID	Handwritten (Bank Samples)			Printed (Bank Samples)		
	C_{RG}	C_{RB}	C_{GB}	C_{RG}	C_{RB}	C_{GB}
1	0.968258	0.892728	0.825478	0.253335	0.165359	0.982213
2	0.987253	0.927229	0.676692	0.884461	0.315626	0.703555
3	0.935719	0.815278	0.861325	0.627446	0.464848	0.849006

Table 6 shows the signature results for real check samples obtained from SBI. Note that the results are very similar to those in Table 5 for the synthetic check samples created by the authors of this chapter.

Table 7. Pantograph results for SBI, AXIS, PNB and HDFC checks.

Bank	Genuine		Printed			
			Laser		Inkjet	
	UNCC Range	Roughness Range	UNCC Range	Roughness Range	UNCC Range	Roughness Range
SBI	17,000–25,000	14–20	38,000–47,000	30–35	48,000–60,000	41–48
AXIS	18,000–24,000	18–22	37,000–45,000	41–45	51,000–63,000	55–60
PNB	21,000–30,000	27–30	41,000–52,000	47–54	57,000–70,000	67–75
HDFC	9,000–15,000	14–17	33,000–39,000	23–27	70,000–88,000	57–65

6.5 Results for Checks from Multiple Banks

Tables 7, 8 and 9 show the results obtained for pantographs, microlines and signatures in checks from the four banks considered in this study. The range of each feature was calculated by applying each de-

Table 8. Microline results for SBI, AXIS, PNB, HDFC checks.

Bank	OCRed Characters	Matched Three Consec. Letters Range	OCRed Characters	Matched Three Consec. Letters Range
SBI	100	7–20	100	0
AXIS	100	8–17	100	0–2
PNB	100	6–18	100	0
HDFC	100	8–22	100	0

Table 9. Signature results for SBI, AXIS, PNB and HDFC checks.

Bank	Handwritten			Printed (Generated)		
	C_{RG} Range	C_{RB} Range	C_{GB} Range	C_{RG} Range	C_{RB} Range	C_{GB} Range
SBI	0.90–0.99	0.70–0.99	0.65–0.95	0.39–0.88	0.19–0.70	0.70–0.98
AXIS	0.86–0.99	0.71–0.98	0.63–0.94	0.27–0.85	0.16–0.50	0.73–0.97
PNB	0.85–0.98	0.72–0.99	0.65–0.91	0.30–0.89	0.23–0.48	0.78–0.98
HDFC	0.89–0.99	0.74–0.99	0.66–0.89	0.42–0.90	0.27–0.45	0.71–0.95

tection method to all the check samples from each bank. The detection methods work very well at 600 dpi resolution. The detection methods were also tested at 300 and 1200 dpi resolutions for each feature. At the 300 dpi resolution, the microline feature fails because all the characters in the microline text merge with each other. The pantograph and printed signature results are same; however, in the case of check alteration, the accuracy drops slightly. At the 1200 dpi resolution, all the features provide very good results compared with the 600 and 300 dpi samples, but the computation time is higher for the 1200 dpi resolution. The 1200 dpi resolution should become more feasible as powerful computer systems become cheaper and easily available.

7. Integrated Check Fraud Detection Tool

An integrated scanner-based tool that implements all the methods described above has been developed to assist bank personnel in detecting check fraud. The algorithms, which were written using Matlab 2013a, execute on a Dell Inspiron 14R N4010 workstation with 4 GB RAM and an Intel Core i3 M 380 2.53 GHz processor. The fraud detection tool, which can process a check within two seconds, is efficient, inexpensive

and works on low-magnification devices. Moreover, it is easily scaled to handle images with 600 dpi resolution taken by smartphones.

8. Conclusions

Counterfeit documents are typically detected by human experts who manually analyze suspect documents using a microscope and video spectral comparator. This process is time-consuming, inefficient and non-scalable; indeed, it is infeasible for deployment at large banks. In contrast, the proposed check fraud detection methods are automated, low-cost, efficient and scalable. One method effectively determines whether or not a check is genuine or printed. Another method detects erasable ink alterations on checks by localizing the erased regions in the visible light spectrum. A third method distinguishes printed signatures from handwritten signatures based on the high-density noise introduced by scanners and printers.

The proposed check fraud detection methods have certain limitations. The principal limitation is that the methods have to be tuned to specific bank check designs, including the color schemes. Other limitations, which will be addressed in future research, include processing torn and damaged checks, signatures in colors other than blue and checks with information written in inks of multiple colors.

References

[1] M. Abd-ElZaher, Different types of inks having certain medicolegal importance: Deciphering faded and physically erased handwriting, *Egyptian Journal of Forensic Sciences*, vol. 4(2), pp. 39–44, 2014.

[2] Australian Payments Clearing Association, Australian Payments Fraud: Details and Data – 2016, ABN 12 055 136 519, Sydney, Australia (`www.apca.com.au/docs/default-source/fraud-stat istics/australian_payments_fraud_details_and_data_2016.pdf`), 2016.

[3] P. Deng, L. Jaw, J. Wang and C. Tung, Trace copy forgery detection for handwritten signature verification, *Proceedings of the Thirty-Seventh Annual IEEE International Carnahan Conference on Security Technology*, pp. 450–455, 2003.

[4] U. Garain and B. Halder, On automatic authenticity verification of printed security documents, *Proceedings of the Sixth Indian Conference on Computer Vision, Graphics and Image Processing*, pp. 706–713, 2008.

[5] GitHub, Tesseract OCR (`github.com/tesseract-ocr/tesseract/wiki`), 2017.

[6] G. Gupta, C. Mazumdar, M. Rao and R. Bhosale, Paradigm shift in document related frauds: Characteristics identification for development of a non-destructive automated system for printed documents, *Digital Investigation*, vol. 3(1), pp. 43–55, 2006.

[7] G. Gupta, S. Saha, S. Chakraborty and C. Mazumdar, Document frauds: Identification and linking fake documents to scanners and printers, *Proceedings of the International Conference on Computing: Theory and Applications*, pp. 497–501, 2007.

[8] D. Kennard, W. Barrett and T. Sederberg, Offline signature verification and forgery detection using a 2-D geometric warping approach, *Proceedings of the Twenty-First International Conference on Pattern Recognition*, pp. 3733–3736, 2012.

[9] R. Kumar and G. Gupta, Forensic authentication of bank checks, in *Advances in Digital Forensics XII*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 311–322, 2016.

[10] C. Lampert, L. Mei and T. Breuel, Printing technique classification for document counterfeit detection, *Proceedings of the International Conference on Computational Intelligence and Security*, vol. 1, pp. 639–644, 2006.

[11] R. Patil and S. Takale, Signature verification by distance matrix method for bank check process, *Proceedings of the International Conference on Electrical, Electronics, Signals, Communication and Optimization*, 2015.

[12] G. Prakash and S. Sharma, Computer vision and fuzzy logic based offline signature verification and forgery detection, *Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research*, 2014.

[13] M. Rajendar and R. Pal, Detection of manipulated check images in a check truncation system using mismatch in pixels, *Proceedings of the Second International Conference on Business and Information Management*, pp. 28–33, 2014.

[14] Rediff on the Net, In a year, bank fraud doubles – Maharashtra and West Bengal lead the way in bank fraud, November 18, 2015.

[15] Reserve Bank of India, Handbook of Statistics on the Indian Economy, 2014-15, Mumbai, India (`rbidocs.rbi.org.in/rdocs/Publications/PDFs/00HC398B27C6AFF47039ABE93049886B494.PDF`), 2015.

[16] A. Sarkar, R. Verma and G. Gupta, Detecting counterfeit currency and identifying its source, in *Advances in Digital Forensics IX*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 367–384, 2013.

[17] J. Xie, C. Qin, T. Liu, Y. He and M. Xu, A new method to identify the authenticity of banknotes based on texture roughness, *Proceedings of the IEEE International Conference on Robotics and Biomimetics*, pp. 1268–1271, 2009.

[18] M. Yusof and V. Madasu, Signature verification and forgery detection system, *Proceedings of the Student Conference on Research and Development*, pp. 9–14, 2003.