

Fingerprinting Blank Paper and Printed Material by Smartphones

Waldemar Berchtold, Markus Sütter, Martin Steinebach

Abstract

This work shows a fingerprint method for the unique identification of blank and printed paper by a smartphone. This allows a secure authentication by authorities or end users of products or documents. The digital file includes no hidden data. The fingerprint method uses uncontrollable printing variabilities and paper structure as features. The uncontrollable variabilities are mapped into a binary sequence, which is used as representation of the features and acts as our fingerprint. The variabilities can be extracted from low and high quality paper as well as from printed material created with low-cost office printers and high-end offset printing machines. Based on this fingerprint, various applications can be realized where the distinction between original and copy or forgery is essential, such as piracy of packaging, tickets, coupons or official documents. From the results of the evaluation it can be concluded that the proposed method is independent of the smartphones used, the paper, the printing technology and the color temperature of the ambient light. Furthermore, the test results show that the proposed method works robustly at different distances, from the smartphone camera to the paper.

Introduction

Product piracy and counterfeiting have a negative impact on public health and safety, as well as on the sales and profits of the companies involved. A study by the EOECD and the EU Intellectual Property Office EUIPO [1] has observed a growing market of trade in counterfeit and pirated goods in recent years. In 2013, about 2.5% of goods were counterfeit and in 2016, it was 3.3% of world trade. In addition, the World Health Organization estimates that one in ten medical products in developing countries is sub-standard or counterfeit [2].

This is a problem because counterfeit medicines can result in patients not receiving the right treatment or even being poisoned by contaminated or toxic products. Companies, along with customs authorities, use many different techniques to detect and stop counterfeits. Nevertheless, the number of counterfeit goods reaching customers has steadily increased in recent years. There are many different technologies available to detect counterfeits, ranging from watermarks and special paper to RFID chips and markings in the form of holograms on packaging or products. Many of these features can help customs authorities, product experts and companies detect counterfeits.

European Union Regulation (EU) 2016/161 requires that every pharmaceutical product sold be marked with a unique ID. This is implemented by printing a matrix code on the packaging that carries this unique ID, as well as a seal that alerts customers to opened packages. This ID is stored in a database, but only manufacturers, pharmacies and hospitals are linked to this database in the case of pharmaceuticals. This results in some disadvantages,

but the biggest disadvantage is that the customer still cannot be sure whether the offline or online pharmacy has sold him a counterfeit product by simply copying the package including the matrix code. This shows that the process is not yet complete to successfully counteract consumer product piracy.

In the prior art and related works, these challenges are addressed with different approaches. One approach is the use of watermarking, where some marginal dots and patterns are added to individualize each copy, with the changes invisible to humans. The watermarking approach is well researched and used in some commercial products, such as AlpVision or Snaptrust. Another approach is to use paper fingerprinting methods. The authors of [6] present a technique to detect the fiber structure of paper with a microscope. Buchanan et al. [7] showed that unique identification is possible by scanning the surface of blank paper with a laser. A different approach is taken in [8], where paper is re-identified by shining an overhead projector through the paper and capturing this with a camera.

The goal of this work is to allow customers to verify the authenticity and integrity of a document or product using their smartphone. To this end, this work shows the possibility of extracting unique features and using them as fingerprints.

Challenge and Requirements

One challenge with fingerprints is to find suitable features. The features should have a good compromise between a certain robustness against environmental influences and everyday wear and tear, but at the same time fragility in case of attacks.

The features used must be unique to each copy to avoid collisions, i.e., a manufacturer may want to print a large number of identical copies or use the same paper, but still be able to distinguish the individual patterns.

Also, the physical size of the area used for the fingerprint should be as small as possible so that it can be used in practice for documents and packaging, where space is usually limited.

Since we are allowing a user to capture the relevant region with their smartphone, the fingerprint mechanism must be robust to a number of factors. The hardware in smartphone cameras is heterogeneous. Camera resolution and post-processing steps vary by manufacturer and device. Ambient light varies by time of day and location. Substrates vary in surface and structure, as do printers and printing methods, inks, and finishing. Printed material tends to degrade and lose color intensity over time, scratches in the surface or wrinkles in the substrate may occur. A fingerprint mechanism must be invariant to these conditions to be applicable in practice.

Concept

In our concept, a manufacturer defines the Region of Interest (ROI), which is an area on his product or document. This ROI can be a logo or another area, but it is recommended to define an area typical for the manufacturer. At the end of the manufacturing step, an image of the ROI is taken and the fingerprint is extracted. The manufacturer stores the fingerprint in a database and provides a link to the database by, for example, storing the URL in a barcode and printing the barcode next to the ROI.

The customer can verify it by taking a photo of the ROI and the barcode. The fingerprint is extracted from the ROI and compared to the database. If there is a match, the product is authentic, otherwise it is a fake. Since the fingerprint is the topic of this article, we will not discuss securing the URL in the barcode further. We will only mention that misleading the user to a database of the counterfeiter is possible and can be excluded with a digital signature.

Fingerprint Algorithm

This section describes the creation of a fingerprinting process for blank paper and printed products. The system does not create features in a pre-process, but the fingerprint is designed to focus on uncontrollable production variability caused by the papermaking and printing process.

Production variability of printed products has been well researched. In this paper, we focus on the standard production variability considered in the ISO print quality standards. We analyze the features there and check their suitability for use. We check if they contain enough entropy to be extracted with common smartphones. For this, we consider the two ISO standards ISO/TS 15311-1:2019 [9] and ISO/IEC 24790:2017 [10]. An obvious caveat to using print quality standards to find good measurement and fingerprinting methods is the focus of each standard on accurate reproducibility of measurement results. The standards clearly define the parameters of the measuring equipment that must be calibrated before use and use standard lighting and imaging conditions for each measurement. Measuring under such precise conditions is not possible with a smartphone. We will therefore try to appreciate the suitability of the metric as a unique feature and the difficulty of performing measurements with a smartphone.

Uniformity

The properties addressed by the ISO/TS 15311 standard are color, gloss, detail reproducibility and uniformity with banding, mottling, graininess, show-through and rub-through resistance. We will focus only on uniformity in this paper, as it is the most promising property to meet the above requirements. Uniformity metrics such as banding, mottling, graininess, show-through, and print-through resistance deal with larger, monochrome print areas and the variations that occur in those areas.

Banding is the occurrence of repetitive, one-dimensional patterns in uniform areas. ISO/IEC 24790:2017 evaluates the occurrence of such patterns by first measuring the reflectance of a large area (150 mm x 100 mm) with an RGB camera. After applying the fast Fourier transform to the resulting brightness image, a low-pass filter is applied to extract only frequencies below 0.5 cycles per millimeter, since banding is typically low frequency. By finding local extrema in the resulting spectrum, the banding metric is evaluated.

Show-through is typically a measure of how a substrate makes ink visible on the reverse side of a page. The measurement in ISO/TS 15311-1:2019 begins by scanning one color value of the substrate on the front and back of a page and another in the center of each process color block on the blank page. Show-through could be an interesting component for a fingerprint, but in our application scenario, making this measurement is difficult to implement and can lead to many acquisition errors.

Mottle and Graininess are defined as aperiodic noise in the brightness of a uniform image area. Mottle is defined as noise with low spatial frequencies of less than 0.4 cycles per millimeter in all directions. Graininess, on the other hand, is the higher frequency noise, i.e., above 0.4 cycles per millimeter. The standard extracts measurements for this characteristic in a similar way to banding, by first capturing the area of interest with an RGB camera or scanner and then converting the image to CIE color space. In this method, only the Y component is used. A Daubechier wavelet transform is applied and certain wavelet values corresponding to the target cycles per millimeter are extracted (see table) by setting all coefficients of all other scale levels and the remainder to zero. The metric is calculated based on the variance of the inverse transform of the extracted spatial frequencies. In this paper, the feasibility of using Mottle and Graininess as features for the fingerprinting mechanism will be investigated in the following parts of this paper.

Scale Level	Frequency in (cy/mm)	
8	11.8110 to 5.9055	High frequencies to be removed
6	2.9526 to 1.4736	
5	1.4763 to 0.7382	Frequencies for graininess
4	0.7382 to 0.3691	
3	0.3691 to 0.1846	Frequencies for mottle
2	0.1846 to 0.0923	
1	0.0923 to 0.0461	

Scale levels of wavelet transform at 47.2 px/mm (1200 DPI)

Fingerprint Methode using Variances in Uniformity

The previous section provided an overview of possible uncontrollable production variations. The referenced standards cover print quality assessment, but the features can also be used to perform robust fingerprinting of individual prints. We will focus on one feature in this paper, mottle and graininess, the noise variations of homogeneous color blocks. To extract the frequencies used in the standard, it is necessary to achieve at least 3 samples per millimeter. This is possible with common smartphones. Based on the metric for extracting mottle and graininess, we have developed a fingerprint mechanism for surfaces with uniform color. To perform and evaluate the extraction of such a fingerprint, we first defined a specific test image that guides the region-of-interest extraction and can always be printed from the

same file. This test image consists of a single, monochrome block in process color (CMYK) surrounded by four finder patterns. Figure 2 shows such an example.

Image Acquisition

An Android application was created to capture the images and was responsible for controlling the lighting, autofocus, and auto-exposure, as well as writing the raw formatted images to predefined directories. As one of the first measures against the defined robustness problem of varying lighting conditions, we activated the display at full brightness when we took a picture with the front camera, while we activated the LED flash when we used the rear camera. To have more control over image processing, we saved all images in a RAW format, which saves the output of the sensor data without demosaicing, white balance, or further post-processing. This also resulted in all images captured this way being at the full resolution supported by the chip. The application used the Android camera2 API to control image capture and lighting.

Region of Interest Extraction

As the first step after image acquisition, we extract the Region Of Interest (ROI) based on the four-finder pattern in the corners outside the ROI. Using the estimated module size of the finder patterns, we estimate the pixels per millimeter of the entire image and derive the corner points of our ROI. Using the estimated corner points and the target image size, we then calculated a transformation matrix that mapped the corner points to a rectangle of the target size (e.g., for a 30 mm x 30 mm square and a target px/mm of 20, we mapped the ROI to a rectangle of size 600 x 600 pixels). This meant that images that were too large were reduced in size, losing information, while images that were too small were enlarged, requiring interpolation. Using this transformation matrix and depending on the type of input image, we either applied a perspective warp transformation directly or demosaiced the raw image first and then transformed it. Demosaicing is done via bilinear interpolation using OpenCV's demosaicing function.

Wavelet Decomposition

The extracted region of interest is transformed to the CIE XYZ color space, keeping only the luminance Y channel. For this step, we follow ISO 24790 and use the formula: $Y(x,y) = 0.2126 * R(x,y) + 0.7152 * G(x,y) + 0.0722 * B(x,y)$. This luminance image is transformed into wavelet space with Daubechier wavelets of order 16, giving us 8 levels. We delete all unused planes and feed the remaining coefficients with the inverse wavelet transform to obtain an image with only the frequency bands used. The resulting image is cropped by about 30 pixels on all four sides to reduce edge effects. Furthermore, the values of the inverse wavelet transform are normalized to a range of [0, 1]. The final output is a 540 x 540 pixel array of floating point numbers between zero and one. Figure 1 shows the output image and the eight levels after the inverse wavelet transform, starting with the output image in the upper left corner the levels in ascending order.

Matching and Similarity Scoring

Finally a scoring function is performed for the comparison and matching. Because we were comparing noise patterns we

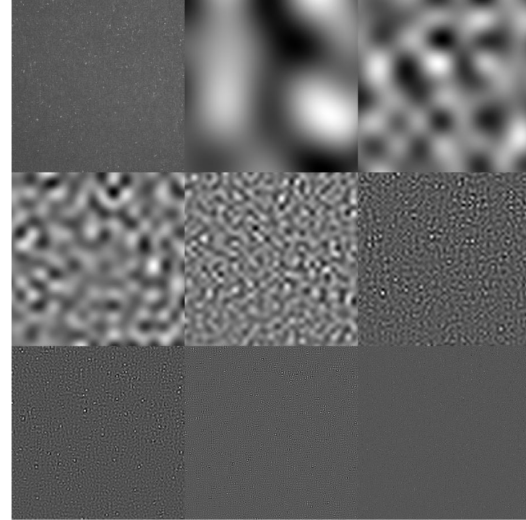


Figure 1. The initial image and eighth levels of a wavelet decomposed region of interest, histogram-stretched for visualization starting with the initial image in the upper right corner and the levels arranged in ascending order from left to right and top to bottom.

were inspired by the noise pattern matching of [11] which uses a correlation coefficient as a scoring mechanism. The normalized correlation coefficient has the benefit of being brightness invariant and was therefore a good match for our scoring function as the intensities of extracted reflection patterns could vary depending on the outside light. In OpenCV, the matchTemplate function is used to find a template image in a larger target image and implements a normalized correlation coefficient as TM_CCOEFF_NORMED. Because the extracted fingerprints are of the same size as the reference images and our extraction is accurate enough to not need a sliding window, we use this function but with the template and the target being of the same size. This yields a single correlation value between -1 and 1 which we can use as a score. With two identically sized images I (the new fingerprint) and T (the reference) with width w and height h, the correlation coefficient CCN is calculated in OpenCV as follows:

$$T'(x,y) = T(x,y) - \frac{1}{w \times h} \times \sum_{x',y'} T(x',y') \quad (1)$$

$$I'(x,y) = I(x,y) - \frac{1}{w \times h} \times \sum_{x',y'} I(x',y') \quad (2)$$

$$CCN = \frac{\sum_{x,y} (T'(x,y) \times I'(x,y))^2}{\sqrt{\sum_{x,y} T'(x,y)^2 \times \sum_{x,y} I'(x,y)^2}} \quad (3)$$

Balanced Saturation

If a matched fingerprint was found by the previously described step, it is necessary to ensure that the fingerprint was not created by an attacker and added to an ROI. Therefore it is necessary to look at the saturation of the recorded ROI. For this purpose, the ROI is transformed into the HSV color space. Then, the magnitude of the transformed values is scaled to the value range 0 and 255. The same is done with the pattern in the database. Then

the results are subtracted from each other using the pixel position and the mean and variance are calculated. If the variance is small, it can be assumed that the pattern is original, otherwise it is a copy or a forgery. The threshold of 1570 is used for the variance to distinguish between an original and a forgery.

Evaluation

We first give the details of the test setup and the parameters used in the evaluation. Based on this the robustness of the fingerprint is evaluated.

Methodology

To evaluate the implementation, we designed a test page in Adobe Illustrator with five blocks that were 30 mm x 30 mm. This size was chosen because images captured at 20 pixels per millimeter would have a size of 600 x 600 pixels, which is the digital image size chosen by the standard. The blocks were created to represent exactly one of the basic process colors (CMYK) and one of the blocks was left blank to understand the property of the substrate itself. One block is shown as an example in Figure 2. The test page was exported as a PDF in the standard PDF/X-3:2002 format, which allows embedding of a CMYK color space to ensure that all printers and drivers receive the same color information.

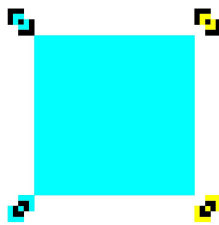


Figure 2. An example cyan block with the four surrounding finder pattern.

Four different printers were selected for the consumer printer evaluation and the same .pdf file was printed multiple times on each printer. Two printers were consumer inkjet printers, one was a consumer laser printer, and the last printer was a professional office laser printer (HP OfficeJet 5220, Canon Pixma IP4000, HP Color LaserJet M276nw, BizHub C458). To further evaluate functionality for different substrates, the consumer prints were made on two different brands of paper, both being office copy paper. For an overview of all consumer prints performed. Since one of the motivations for the developed technique was to protect packaging and labels, we also purchased a number of packages that had the same process color blocks printed on them. These prints were produced using professional, large-format offset and digital presses (Heidelberg Speedmaster XL105-8P, MAN Roland R704+L, HP Indigo 30000, HP Indigo 12000). Although different machines were used for production, the substrate was the same. The packaging material is usually coated with a protective varnish after printing. This varnish was applied to all offset and digital prints, except for one of the offset prints, which was left uncoated.

The images of these prints were taken with two different, relatively recent smartphones with front and rear cameras, with the rear camera images lit with the LED flash and the front camera images lit with the display white at full brightness (Huawei Mate 9, Nokia 5). The rear camera of another smartphone was

later used to check functionality on a random new device (Samsung Galaxy S8). Different lighting conditions were tested using LED table lamps that allowed four color temperature settings (3000K, 4000K, 5000K and 6500Kelvin).

To define reference image conditions, i.e., conditions that produced good reference images and that we could consistently use across all test images as base positions and lighting conditions, we established a set of parameters for reference images, which we then modified according to test requirements. The height was set at 14 cm, since at this distance the sampling rate was close for both the front-facing and rear-facing cameras, but slightly above 20 px/mm. For the reference images, the overhead lighting and LED lights in the room were turned off, resulting in a relatively dark environment since the images were taken in a room with no direct outside light. The blocks were rotated so that they were as straight as possible under the camera, meaning the angle was always as close as possible to a multiple of 90°. The position of the test image was also adjusted so that the brightest part of the LED light or display was always aligned as close as possible to the center of the image.

Parameters

In this section we will explore the correlations for different levels of images taken with different cameras of each process color for each print to determine good parameters for a high recognition rate. We further want to analyze the results for each process color and the substrate as well as the results for front and back cameras to determine which configuration is best suited. The parameters that are best suited in the extraction process are those that generate the highest possible correlation for the same printed test image while generating the lowest possible correlation for every other test image in the set. Figure 3 shows a box plot of the correlations of all cyan blocks of the consumer prints taken with back-facing cameras. The green boxes denote the correlations for the same blocks while the red boxes show correlations between all other cyan blocks. Each green box is made up of 24 comparisons while each red box is made of 1104 comparisons. The acceptance threshold is set to 0.335. Levels 3, 4 and 5 seem to be

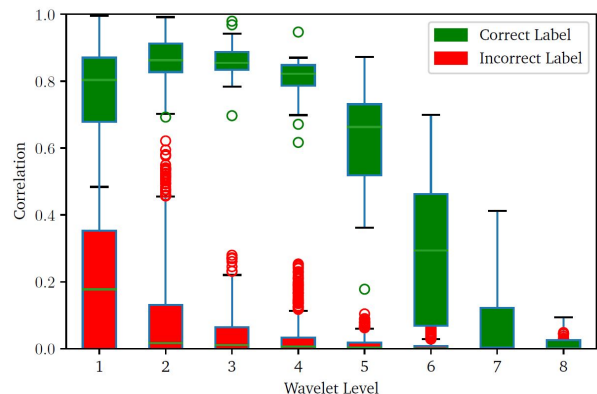


Figure 3. Correlations for the right and wrong label for the back camera tests of the cyan blocks for all consumer prints.

most successful in reliable recognition, while the images seem to be recognizable even in wavelet level 2. As expected, levels 6-8 seem to be too noisy to be reliable and level 1 probably transport

too little information. Level 2 delivers only a small gap between the correct and incorrect lable and thus not be considered in the fingerprint.

Robustness

We will evaluate the proposed fingerprinting approach with the previously mentioned parameters to see its robustness when using a different smartphone, different lighting conditions, rotating the camera, changing the position, and the influence of the substrate.

Cameras The results of the evaluation show that the technology works well with the two different rear cameras with LED flash. To check whether other rear cameras were still successful, the Consumer Prints were photographed with the rear camera of a Samsung Galaxy S8 smartphone and the results were compared with the reference pictures of the other two smartphones in the same way as before. The correlation of the images shows the same good results as with the two smartphones Huawei Mate 9 and Nokia 5, so we conclude that the approach is independent of the camera used to a certain extent.

Lighting Using two TaoTronics TT-DL27 table lamps with adjustable light temperature and intensity, we analyzed the changes in correlation under changing lighting conditions. For this purpose, we took images of the consumer prints of cyan process color blocks under five different lighting conditions to see if the process was still successful for each of them. Each image was taken using the Huawei's rear-facing camera. The other parameters were the same as for the baseline conditions, and the images for each print were taken sequentially to prevent movement or rotation of the image or the phone. The desk lamps were positioned to illuminate the test image from two sides at a distance of about 30 cm. The first image was taken in a dark environment with no direct external light, then images were taken at light temperatures of 3000, 4000, 5000, and 6500 Kelvin. The median correlation for the different illuminations was 0.72 and the standard deviation was 0.066, so the changing lighting conditions did not significantly affect the fingerprint correlations. Even though the reference images were taken in low light conditions, the light from the desk lamps had no effect on the results, regardless of the temperature of the light.

Rotation To evaluate the rotational robustness, all basic conditions were not changed, but the test image was rotated under the camera in steps of 15°. Two test images were selected for this test, a cyan block of the laser prints and a cyan block of the inkjet prints. As in the other evaluations, the rear camera of the Huawei was used as the imaging device. The median correlation for all rotations of the laser print was 0.64, and the median for the inkjet print was 0.7. At the original position, the correlation with the reference for the laser print was 0.74, while the same position on the inkjet printer had a value of 0.76; the lowest correlation was 0.47 with the laser print at an angle of about 210°. The standard deviation of the same print was about 0.071. Thus, the results show the invariance of the approach to rotation.

Position Since users hold the smartphone in their hand to scan an area of interest, we will evaluate the effects of the camera's po-

sition relative to the test image. To do this, we moved the camera away from the center of the image 11 times by 0.5 cm each time. The tests were performed for ink, laser, and offset printers, and the results are shown in Figure 4. All correlations are truncated at 0, although there are negative correlations in the range of about 0.2 in the original data. Each image is plotted at its position, labeled relative to the center of the test pressure in the x and y directions. The center image is taken as the reference and the surrounding images are then correlated to that reference. The black rectangle denotes the outer edges of the print image at a distance of 1.5 cm from the center in all directions. For any image outside the black rectangle, the LED light did not directly strike the printed image. It can be concluded that ink and laser printed material is position invariant as long as the light hits the area of interest. For offset printers, on the other hand, the results of the position of the incident light are crucial. A sufficiently high correlation can only be achieved if the light is centered.

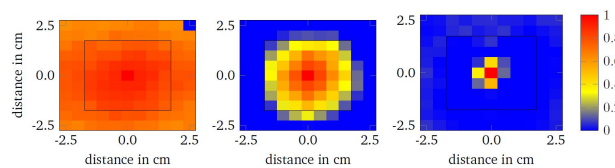


Figure 4. This heatmap shows the correlations at translated positions away from the center of an LED light, moved in steps of 0.5 cm. The x and y axis show the distance from the center in cm, the z axis is colored based on the correlation at that position (see the indicator on the right). From the left: inkjet, laser, coated offset.

Considering the corresponding images after the inverse wavelet transforms for the different printers used, Figure 5 gives an indication of why the substrate from the offset printers is more sensitive to the camera position than those from ink or laser printers. The coated substrate with a glossy surface shows very poor performance. We see the reason in the reflection of the substrate by the LED flash. There is a small feature circle in the center of the ROI and the area around the center is overexposed. As soon as the position changes, the circle changes its position in the ROI and the correlation decreases.

Height To check the robustness of the system to shooting at different heights, we used a camera tripod with three different height settings so that we could take pictures at 14 cm (the height in the reference conditions), 21.5 cm, and 26.5 cm. The images were taken using only the Huawei smartphone and in fixed lighting conditions. The camera's pixels per millimeter dropped to an average of 14.9 at 21.5 cm and to 11.9 at 26.5 cm. Whenever the height was changed, the camera was aligned to point at the center of the test image, as in the baseline reference image conditions. The extracted fingerprint at each height was then compared to the stored reference fingerprint. The shape and size of the light shining on the printed images changes at different heights, so the height should still have an impact on the correlation.

Substrate Impact Since the substrate alone produced almost as good results as the colored blocks, we wanted to clarify the question of the extent to which the surface structure of the substrate is responsible for the final fingerprint and the extent to which the

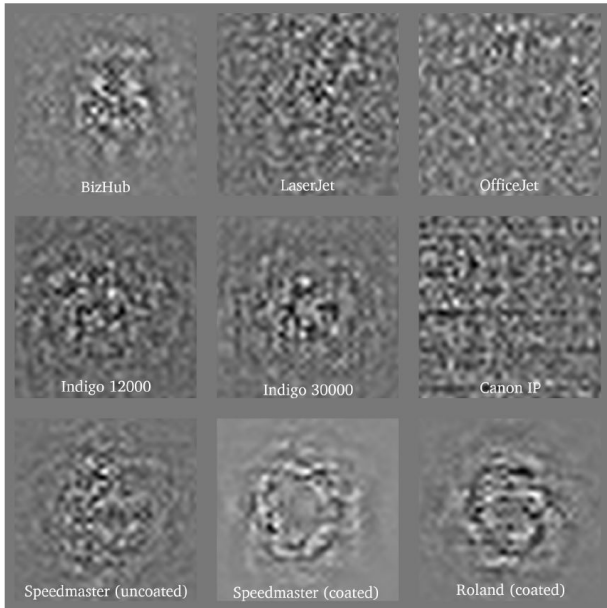


Figure 5. Extracted levels of a cyan block for each printer (histogram-stretched for visualization).

ink printed on the substrate alters this fingerprint. To address this, we first printed finder patterns only on a single piece of paper, similar to the substrate block in the original test page, using the Canon inkjet printer. Then we took an image of this substrate block in the usual way and extracted layers 3 and 4 of the wavelet decomposition. Then we printed cyan, magenta, yellow and key on it and fingerprinted the result again. The results in Figure 6 clearly show the extent to which the texture of the substrate can still show through in inkjet printers, especially with light yellow ink. The correlation is above threshold, except for Key. When Key is printed on the substrate, the printed area falls below the threshold. We also interpret the result to mean that the substrate has an important influence on the fingerprint, and soiling does not destroy the fingerprint to a certain degree as long as the contamination is homogeneous.

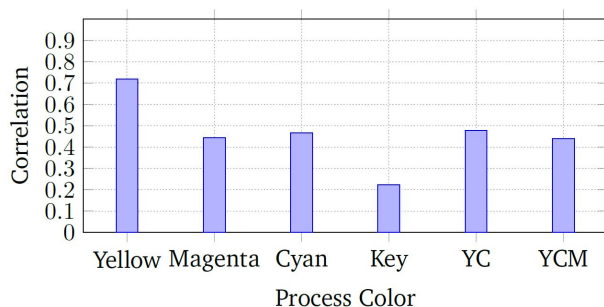


Figure 6. Correlations for different overprints (Canon inkjet).

Conclusion and Future Work

This work shows a general approach to fingerprint blank paper and printed matter based on paper and printing variances. The proposed method was implemented and evaluated for the

defined requirements. The results of the evaluation show a promising amount of unique, re-identifiable and extractable information in the noise of homogeneous regions of multiple prints of the same printer and input file. A number of different printers, substrates and smartphones were evaluated and the print could be successfully reidentified with the back facing cameras. The method showed robustness against the tested requirements related to variation in distance, rotation, ambient light and cameras. To improve robustness of the proposed fingerprinting method a user experience study could determine if the method is still functional when confronted by real users. Future work could also test other features from the referred ISO standard to see how they perform.

References

- [1] OECD/EUIPO OECD Publishing, Trends in trade in counterfeit and pirated goods, illicit trade, Paris/European Union Intellectual Property Office. <https://doi.org/10.1787/g2g9f533-en>, 2019.
- [2] Christian Lindmeier Daniela Bagozzi, 1 in 10 medical products in developing countries is substandard or falsified, Nov. 2017, Online; accessed 4-November-2019.
- [3] Laura Silver and Stefan Cornibert, Smartphone ownership is growing rapidly around the world, but not always equally, Feb. 2019.
- [4] AlpVision, Cryptoglyph, product authentication, anti counterfeiting, covert security, brand protection, <https://www.alpvision.com/fingerprint-product-authentication.html>.
- [5] Snaptrust, Anti-counterfeiting protection, <https://snaptrust.com/en/solutions/solution>.
- [6] H.J Tiziani T Haist, Optical detection of random features for high security applications, *Optics Communications*, 1998.
- [7] James D. R. Buchanan, Russell P. Cowburn, Ana-Vanessa Jausovec, Dorothee Petit, Peter Seem, Gang Xiong, Del Atkinson, Kate Fenton, Dan A. Allwood, and Matthew T. Bryan, Fingerprinting documents and packaging, *Nature*, vol. 436, no. 7050, pp. 475–475, July 2005.
- [8] Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao, Texture to the rescue: Practical paper fingerprinting based on texture patterns, *ACM Trans. Priv. Secur.*, vol. 20, no. 3, pp. 9:1–9:29, Aug. 2017.
- [9] ISO/TS 15311-1:2019 graphic technology – print quality requirements for printed matter – part 1: Measurement methods and reporting schema.
- [10] ISO/IEC 24790:2017 information technology — office equipment — measurement of image quality attributes for hardcopy output — monochrome text and graphic images.
- [11] J. Luka, J. Fridrich, and M. Goljan, Digital camera identification from sensor pattern noise, in *IEEE Transactions on Information Forensics and Security*, 2006, p. 205–214.

JOIN US AT THE NEXT EI!

IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!



- **SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •**
- **INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •**

www.electronicimaging.org

