



Chapitre d'actes

2016

Published version

Open Access

This is the published version of the publication, made available in accordance with the publisher's policy.

Forensic authentication of banknotes on mobile phones

Dewaele, Thomas; Diephuis, Maurits; Holotyak, Taras; Voloshynovskyy, Svyatoslav

How to cite

DEWAELE, Thomas et al. Forensic authentication of banknotes on mobile phones. In: IS&T International Symposium, Electronic Imaging 2016, Media Watermarking, Security, and Forensics 2016. San Francisco (CA, USA). [s.l.] : [s.n.], 2016. p. 1–8. doi: 10.2352/ISSN.2470-1173.2016.8.MWSF-083

This publication URL: <https://archive-ouverte.unige.ch/unige:145445>

Publication DOI: [10.2352/ISSN.2470-1173.2016.8.MWSF-083](https://doi.org/10.2352/ISSN.2470-1173.2016.8.MWSF-083)

Forensic authentication of banknotes on mobile phones

Thomas Dewaele, Maurits Diephuis, Taras Holotyak, Sviatoslav Voloshynovskiy, Stochastic Information Processing Group
7 route de Drize, CH 1227, Geneva, Switzerland

Abstract

Relatively cheap and high quality consumer scanners and printers have enabled the rise of the casual money counterfeiter. One who passes along home-made fake bills of low denomination in busy environments where the receiver is not likely to authenticate a bill. While this may be negligible on macro-economic scale, it does hurt consumers. In this paper we investigate several methods to identify counterfeit bills using an ordinary hand held mobile phone without any modification or special lighting. We demonstrate using a database of Swiss and Euro notes that variations of statistics along edges between a printing press, a laser and an inkjet are distinguishable with a mobile device. Furthermore, we show how random printing variations in the production of true banknotes can be used as a unique non-cloneable identifier for that particular bill.

Introduction

The forgery of banknotes is no longer limited to organizations or even countries that have the means to invest in professional printing equipment. Cheap high quality consumer scanners and printers have enabled the casual counterfeiter. Someone who copies a low denomination bills and passes them off in environments where people are not likely to check the authenticity, e.g. small shops during rush hour. For instance, counterfeiter Art Williams Jr. produced millions of dollars using commercially available paper, ink, printers and photo-editing software [25]. Similarly, Wesley Weber forged the CAD 100 bill using HP DeskJet printers and he is believed to have produced more than \$6-million in fake \$100 bills that made it into circulation [8].

Casual counterfeits are removed relatively quickly from circulation as they don't stand up to close scrutiny. The main victim is the last consumer to be handed the bill or the local retailer. In 2002, over 95% of the detected fake notes of \$20 and smaller denominations, which are those most commonly used by U.S. consumers, were casual counterfeits. The 5 remaining percent of high-quality counterfeits only accounted for less than \$220'000 in total [17].

Obviously, there are numerous security features embedded in banknotes to deter counterfeiting, be it high or casual low grade. Central banks and manufactures typically disclose as subset to enable the public to authenticate bills. Disclosed security features for the Swiss Franc, Euro and US Dollar include Intaglio printing, watermarks, Guilloch patterns holograms etc.

In practice however, very few members of the public are fully aware of all security features further illustrating why end consumers are the most likely victims of causal counterfeiting. It is therefore in this work, that we demonstrate a simple forensic tool that allows a consumer to verify the authenticity of a Swiss banknote using an ordinary mobile phone.

The deployed method has three main stages. A geometrical

alignment of the suspect Swiss banknote followed by two types of feature extraction to ascertain the characteristics of the manufacturing device. The first feature is build up on the fact that Swiss banknotes exhibit random fluctuations between printing stages. These fluctuations can be measured and tied in to the serial number of the bill.

Secondly, we show how a relatively simple feature vector build from the edge and contour characteristics can be used to discover the used printing technique.

Related work

Banknote authentication draws from a number of computer vision and image processing sub-domains to find discriminative features. A significant body of work uses flatbed scanner images from banknotes as a starting point, thus negating any geometrical distortions or lighting variations. Recently [30, 4] proposed a combination of five histogram shape descriptors from a co-occurrence matrix next to five texture descriptors. The resulting feature vector is used by a neural network to classify the denomination and serves as an indication of authenticity when the feature distance to a reference banknote is calculated. Work from [26] uses a combination of nine gray-scale, color, and geometrical features to determine if a banknote was manufactured using intaglio printing. Texture roughness features are deployed in [29] after which a 100 authentic banknotes are enrolled to determine the range variability of the final feature vectors for authentic notes. Vectors outside this range are deemed to have originated from fake bills. In [15] a relatively simple colour histogram is used as a feature, but the authors propose an enhanced similarity metric based on fuzzy hamming distances. Finally [14] models counterfeiting as essentially a 1-class classification problem in which the statistics of genuine banknotes are known. They propose dividing an image of a banknote into non-overlapping blocks and deploy a 1-class classifier per block, the results of which are fused.

Especially relevant to banknote authentication is the work that has focused on identifying the used printing technique from a sample. Work in this direction is mostly based on the analysis of the contours and edges of printed characters [7, 1, 24, 18, 22].

Banknote authentication using special sensors has been common practice for decades. If the hardware and infrastructure requirements can be met, these methods are tough to defeat. In [2] an infrared sensor was used to both detect the value and the authenticity of a note. Infrared sensors were also used in [16, 28, 21]. The research in [6] leveraged the intrinsic fluorescence lifetime of a genuine banknote, measuring it with a two-photon laser excitation microscope, and [3] based their approach on UV patterns of genuine banknotes. A 3d profilometry technique was used in [31]. Work in [5] exploited features that are only visible when a banknote is back lit with a strong (UV) light. A similar approach was used in [12] to reveal otherwise hidden

individual fibers. Finally, [10] studied refracted light patterns.

Mobile devices have been used to recognize the denomination of bill, primarily as a tool for the visual impaired. All of them use computer vision features such as SIFT or SURF, followed by geometric verification, for example RANSAC, to align the images prior to classification. [9, 23, 13, 27] Most close to this work is [19, 11] who also deployed mobile phones to authenticate banknotes based on high frequency features of the intaglio printing.

Contribution and research questions

Our contribution is twofold:

- We have found an individual banknote fingerprint linked with the particularities of banknote production. This feature can be used for banknote authentication by linking the individual banknote fingerprint with the banknote serial number.
- We have demonstrated a simple and efficient procedure for banknote authenticity verification based on design edge features.

Although, we performed our study on Swiss banknotes, the obtained results can be extended in a straight forward way to other currencies. We will highlight similar features in Euro banknotes.

In our study, we formulate our goal as a confirmation of the existence of a set of simple forensic features that can be used for reliable banknote authentication. To achieve this goal, we formulate a set of research questions:

- Q1: Can a simple set of forensic features be derived that can distinguish a genuine banknote from a fake?
- Q2: Can these features be reliably extracted from the photos acquired by modern mobile phones taking the variations in acquisition geometry, light, restricted resolution and non-linear lens distortions into account?
- Q3: Are these forensic features specific for each item or typical for a batch, i.e., the same printing machine?

Sample specific fingerprints

Swiss banknotes seem to exhibit printing alignment fluctuations between different printing passes. Specifically the position of printed text fluctuates with respect to the background as shown in Figure 1.

Characterization

The exact phenomenon that creates the offset in the positioning of banknote elements is unknown, but a simple experiment can be designed to decide whether the above features fluctuate randomly or the differences result from multiple presses and designs. The two main hypothesis for the cause of the variability in the alignment between different printing passes are:

H1: random offset hypothesis. Under this hypothesis, we consider that the offset between the different printing passes is due to random uncontrolled imperfections in the printing process. If the printing offset is random, then the offset \mathbf{X} , $\mathbf{x} = (\Delta x, \Delta y)$ in x and y direction between the printing passes is assumed to follow a Gaussian distribution:

$$\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\sigma}), \quad (1)$$

where $\boldsymbol{\mu}$ is the mean vector and $\boldsymbol{\sigma}$ is the covariance matrix.

H2: multiple design hypothesis. If the main cause driving the fluctuations is the existence of multiple designs, or due to different manufactures or printing presses, one expects the offsets to adhere to a Gaussian mixture model (GMM), i.e, a weighted sum of M component Gaussian densities given by:

$$\mathbf{X} \sim \sum_{i=1}^M w_i \mathcal{N}(\boldsymbol{\mu}_i, \boldsymbol{\sigma}_i), \quad (2)$$

with $\boldsymbol{\mu}_i$ and $\boldsymbol{\sigma}_i$ the mean and covariance matrix of the GMM components and w_i is the mixing parameter such that $\sum_{i=1}^M w_i = 1$. The expected results under the hypotheses **H1** and **H2** are visualized in Figure 2.

Implications

Whether **H1** or **H2** is a correct hypothesis **H** is important because it has significant implications on the maximum achievable authentication performance when using design-based features.

If **H1** is true, then the variance between two genuine banknotes will be higher than the variance between a genuine banknote and its counterfeit version. This would have two different consequences. Firstly, denomination specific authentication based on geometrical features would be impossible because the intra-class variance would be too high relatively to the inter-class variance. Secondly, this high variability between each banknote would be desirable when considering a banknote specific authentication since it would allow to easily extract a digital fingerprint from each banknote.

If **H2** is true, the variance between two genuine banknotes that belong to the same cluster i.e. that have the same design, could possibly be smaller than the variance between a genuine banknote and a fake banknote from an identical cluster. Therefore, if all the clusters centers were known in the chosen feature space, it would be possible to authenticate a banknote by first identifying in which cluster it belongs, and then analyzing the distance from the corresponding cluster center.

Experiment

High resolution scans at 1200DPI were acquired from 82 different Swiss 10CHF banknotes, from which the bottom right part was taken (Figure 3a). In this area two distinct printing passes can be observed: the big orange 10 (Figure 3b) is printed separately from the blue brown text and the Guilloché pattern (Figure 3c). Two templates were formed from these printing passes.

To determine the offset between the two printing passes, normalized cross correlation was used to align an image of a bill against both templates (Figure 4). The green channel was used because it is the one with the highest contrast in this particular case. The offsets can be seen in Figure 5a, which clearly support the random offset hypothesis **H1**.

The observed variability can originate from two main sources, either from the randomness of the printing itself, or from imprecisions of the measurement process. To exclude this possibility, all 82 banknotes were again matched against two templates, but two templates from an identical printing pass. The resulting offset fluctuations can be seen in Figure 5b. They show that the vertical and horizontal offsets are nearly constant for our banknote set. The standard deviation is approximately 0.02mm at 1200 dpi,



Figure 1: Comparison of two crops of different genuine CHF 10 banknotes. The text appears on different backgrounds that are not geometrically aligned.

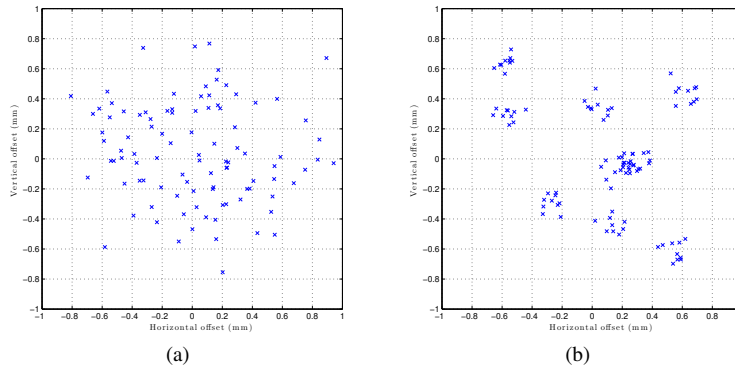


Figure 2: Expected offset results: (a) bivariate unimodal Gaussian model, expected result if H_1 is true and (b) a bivariate Gaussian mixture model ($M = 9$ components), expected result if H_2 is true.

which means the measuring device is nearly pixel precise. This further strengthens the hypothesis that the printing process is the leading cause of the observed variability between printing passes.

In conclusion, Swiss banknotes exhibit random fluctuations between printed matter, most likely from weak control of separate print stages. Specifically, text has a random offset with respect to background elements.

The implications of this result are twofold: it means that using geometrical structures in the feature selection would lead to bad performance of the authenticator when considering a denomination specific authentication, but it is a desirable property when considering a banknote specific authentication. It allows to extract a unique fingerprint from each individual banknote and to tie it to its serial number. As such it is a physical un-cloneable function (PUF), as even a copy made by the very same press will have a different offset.

Cloneability detection

Genuine banknotes are printed using high resolution printing technology whose detail can not be easily duplicated with commercial available equipment. Typically, laser and inkjet printers are unable to produce similar sharp edges due to the dithering and

satellite droplets respectively (Figure 6). This section will show how a mobile phone image may be used to distinguish between printing techniques using different types of feature extraction.

Feature extraction methods

In this section we show how a single edge transition based feature can be used to classify the printing method used for a suspect bill, thus establishing its authenticity. Although more advanced methods exist, ours is simple, parameter free and doesn't rely on any special equipment.

We will consider three models describing the edge transition: (a) the cross-correlation with a synthetic template, (b) the cross-section along the edge and (c) the projection across the edge.

Cross-correlation with a synthetic template

In this method, a small band with a width of m pixels is selected containing a sharp edge somewhere on a bill. In counterfeit banknotes the transition between light and dark printed material varies for each perpendicular cross-section. For a given cross-section across the edge, the position of the transition can be estimated by computing the normalized cross-correlation with a synthetic step function and locating the maximum. The final features

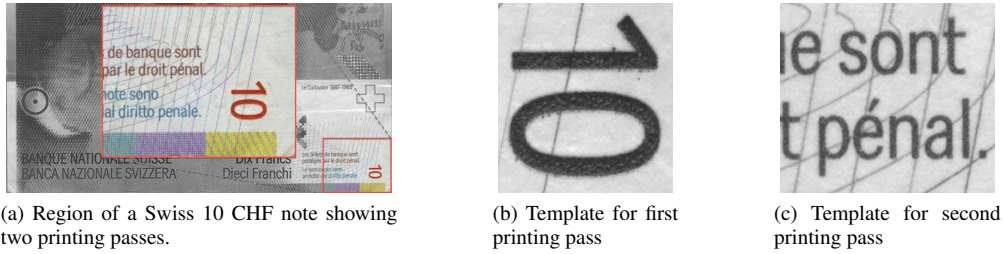


Figure 3: Region and templates used to quantify the variability in Swiss 10 CHF notes.

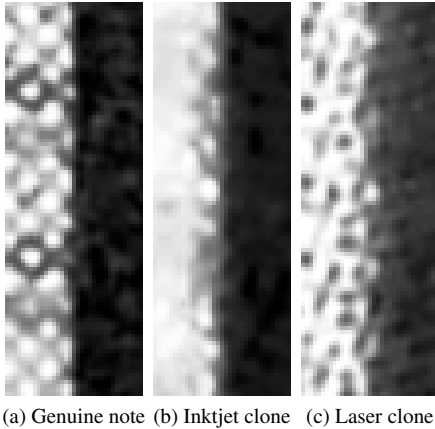


Figure 6: Edge samples from a CHF 20 note, captured with a Samsung Galaxy S3.

are computed from the first derivative of the location of the maximum cross-correlation. The three following measurements are extracted: its standard deviation, the mean of its absolute value, and the maximum of its absolute value.

Cross-sections along the edge

Another observation that one can make from Figure 6 is that when considering cross-sections along the edge, the intensity of the pixels is constant in the case of a genuine banknote. However, for fake banknotes, especially in laser printed ones, the variance of cross-sections along the edge seems much higher due to cluttered patterns. Therefore, this second feature extraction method consists sampling a set of cross-sections along the edge, and computing the standard deviation of their first derivatives. Figure 7 shows the cross-section along the edge for each of the three samples. Because it is hard to obtain a pixel-precise alignment, it is not possible to know the exact position of the transition. Thus, several cross-sections along the edge are considered and sorted by ascending standard deviation of their first derivative and only the n lowest ones are selected. This allows to capture the edge region with a greater probability. Consequently, the number of dimensions of the feature space with this feature extraction method is n , i.e., the number of cross-sections that are kept.

Projection across the edge

The previous two feature extraction methods mainly aim at detecting some sort of irregularities in the printing such as dithering or satellite droplets, but they do not really detect the sharpness of the transition per se. As a result, one can anticipate that they might not be efficient at recognizing inkjet printing, which proves to be much smoother than laser printing. Moreover, if the picture that the user wishes to classify is de-focused or has motion blur, the irregularities will be smoothed, which might lead to a fake banknote to be misclassified when using one of the previous two methods. This last method was designed to distinguish both cluttered printing and the sharpness of the transition.

For detecting the sharpness of the transition, the first derivative across a selected edge is taken. In order to additionally distinguish clutters, the first derivative is not computed for individual cross-sections, but on the average of all cross-sections across the edge, i.e. on the projection along the edge. Using this approach, the derivative has a high peak if (1) all the projected cross-sections have a sharp transition and (2) the transition is located at an identical place in all projected cross-sections.

Figure 8a shows the projections along the edge from Figure 6, and Figure 8b shows their respective first derivatives. It is clear in this last figure that for genuine banknotes, the peak is stronger. The resulting features are extracted from the first derivative and consist in the standard deviation, the mean of the absolute value, and the maximum of the absolute value, similarly to the first method. Therefore, the feature space also has three dimensions.

Experimental setup

The three methods were tested on CHF 20 and CHF 50, EURO 50 banknotes, and the edges were picked along the symbols for the visually handicapped which are located at the bottom of the obverse face of all Swiss francs banknotes. These subregions and the location of the cross-section and edges are illustrated in red in Figure 9.

Genuine, inkjet printed and laser printed banknotes were photographed in various orientations and illumination conditions using a Samsung Galaxy S3 and a Samsung Galaxy S4, placing the sensor between 60 and 100 millimeters away from the banknote.

To undo any geometrical distortions stemming from the fact that all images are acquired with a hand-held mobile phone all methods use an alignment phase. Bills are stitched onto a virtual template using SIFT [20] feature points followed by RANSAC. This can be done accurately enough such that further measured

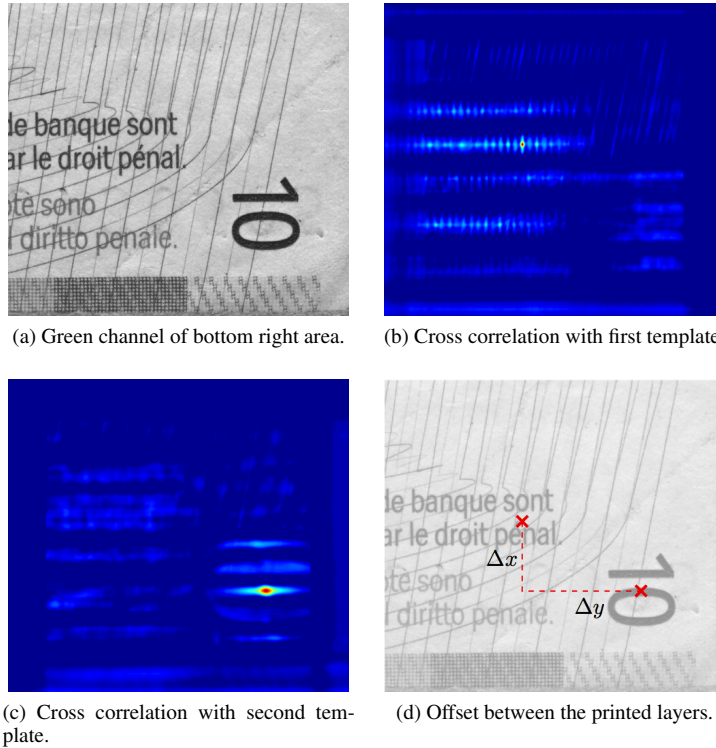


Figure 4: Determination of the offset.

distortions and random fluctuations originate from the printing process itself.

After that, the feature vector of each sample was extracted using the methods explained above. A band of pixel width m was extracted around each specified edge, and their respective feature vectors were averaged. Edge segments are always selected to be of length l . The following parameters were used: (a) using cross-correlation with a synthetic template $l = 50$ and $m = 10$; (b) using n cross-sections along the edge $l = 50$, $m = 3$ and $n = 3$, (c) using projections along the edge $l = 150$ and $m = 10$. Since all methods have a three dimensional feature space, they are visualized in Figure 10.

Then, LDA was performed, and each sample was projected on the axis perpendicular to the classification hyperplane. On this axis normal probability density functions were then fitted using the empirical data.

Lastly, ROC curves were computed, in order to analytically compare the performance of each method. For each method, two ROC curves were computed: using empirical data and using the fitted distributions mentioned in the previous paragraph.

For our experiments, we used a total 24 inkjet printed fakes on a Canon IP7250 and 16 laser printed fakes with a Samsung CLX6220, next to 42 genuine CHF 20 and CHF 50 banknotes. Note that the banknotes were not in mint condition; they have all been in circulation. Furthermore, the pictures were taken at various illumination conditions and various orientations.

Experimental results

Figure 10 illustrates the samples in the 3D feature space, allowing to visually inspect the separability of each method. The ROC curves computed from empirical data those and based on a Gaussian approximation of LDA projections are shown in Figure 11.

The ROC curves show that even if all methods initially seemed to perform quite well except for cross-correlation with a synthetic template, only the projection along the edge has an acceptable performance when considering a low false positive rate.

In all cases, all features for inkjet printed fakes are more similar to laser printed ones. The reason is two fold, laser printing produces the most cluttered patterns whereas the inkjet tends to smooth out transitions between dark and light, even more so then observed in genuinely printed notes. Features based on the projection across an edge are able to distinguish this the best.

Conclusion

We have demonstrated the possibility of banknote authentication using consumer smart phones. We have shown that Swiss 10 CHF notes exhibit random fluctuations that can be used as individual fingerprints linked to their serial number. Secondly, we have shown that a simple feature based on edge transitions can distinguish counterfeits made with inkjet and laser printers from genuine bills. This was tested on Swiss 20 and 50CHF notes, next to Euro 50 bills.

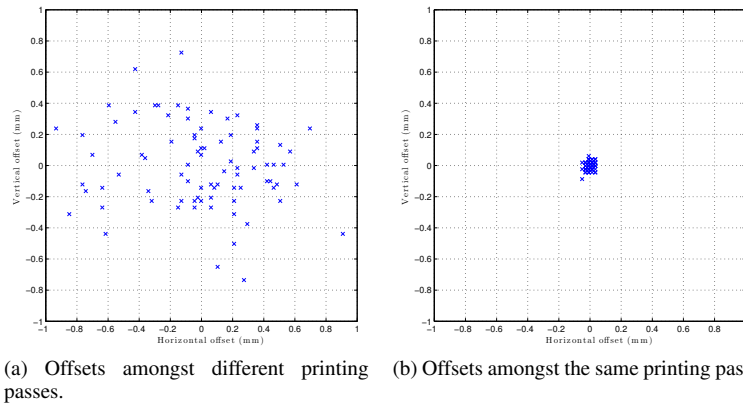


Figure 5: Statistics of the offsets for two design elements in Swiss 10 CHF banknotes.

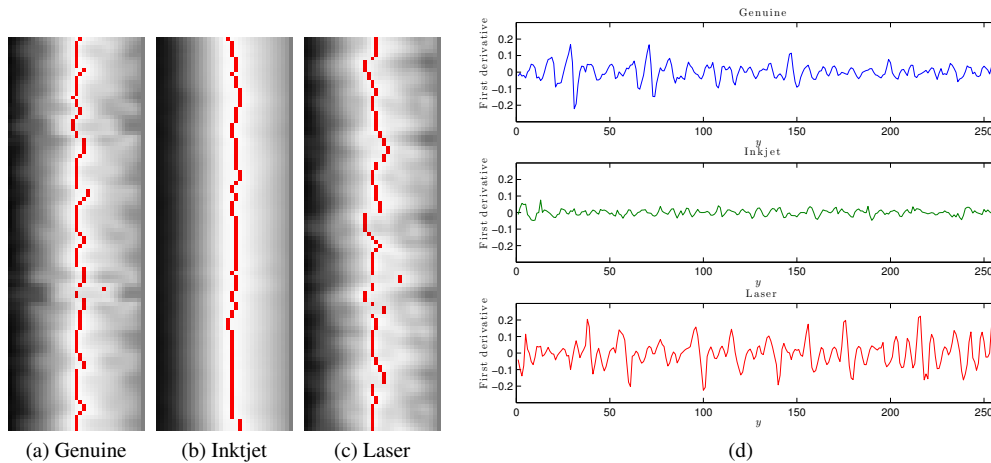


Figure 7: (a) Cross-correlations across the edge with the position of the maximum highlighted in red and (b) the first derivative cross-sections along the edge.

References

- [1] Guy Adams, Stephen Pollard, and Steven Simske. A study of the interaction of paper substrates on printed forensic imaging. In *Proceedings of the 11th ACM Symposium on Document Engineering, DocEng '11*, pages 263–266, New York, NY, USA, 2011. ACM.
- [2] Arcangelo Bruna, Giovanni Maria Farinella, Giuseppe Claudio Guarnera, and Sebastiano Battiato. Forgery detection and value identification of euro banknotes. *Sensors*, 13(2):2515–2529, 2013.
- [3] Seung-Hoon Chae, Jong Kwang Kim, and Sung Bum Pan. A study on the korean banknote recognition using rgb and uv information. In Dominik Slezak, Tai-hoon Kim, Alan Chin-Chen Chang, Thanos Vasilakos, Ming Chu Li, and Kouichi Sakurai, editors, *Communication and Networking*, volume 56 of *Communications in Computer and Information Science*, pages 477–484. Springer Berlin Heidelberg, 2009.
- [4] Jarrett Chambers. Digital currency forensics. Master’s thesis, Auckland University of Technology, 2012.
- [5] Chin-Chen Chang, Tai-Xing Yu, and Hsuan-Yen Yen. Paper currency verification with support vector machines. In *Proceedings of the 3rd International IEEE Conference on Signal-Image Technologies and Internet-Based System, SITIS '07*, pages 860–865, Washington, DC, USA, Dec 2007. IEEE Computer Society.
- [6] Thomas H. Chia and Michael J. Levene. Detection of counterfeit u.s. paper money using intrinsic fluorescence lifetime. *Opt. Express*, 17(24):22054–22061, Nov 2009.
- [7] Jung-Ho Choi, Hae-Yeoun Lee, and Heung-Kyu Lee. Color laser printer forensic based on noisy feature and support vector machine classifier. *Multimedia Tools and Applications*, 67(2):363–382, 2013.
- [8] Krystle M. Davis. Glorifying a master counterfeiter. ”<http://www.forbes.com/2009/06/29/art-of-making-money-opinions-/book-review-jason-kersten.html>”, June 2009. [Online; accessed February 6th 2015].
- [9] Michael Digma and Christian Elder. Mobile banknote recognition and conversion. Available at <https://>

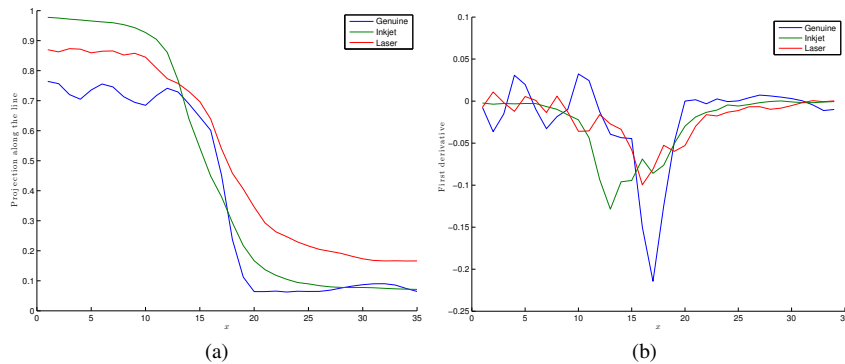


Figure 8: (a) Projections across the edge and (b) the first derivatives of projections across the edge.

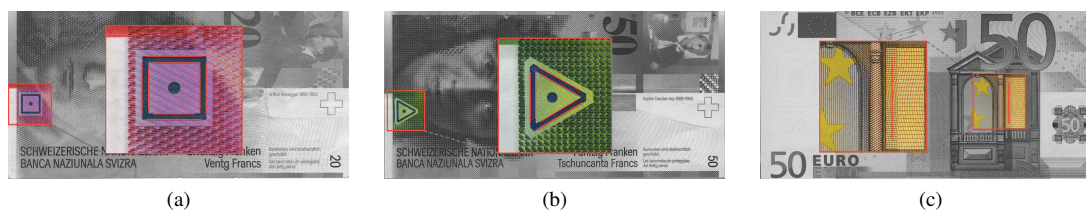


Figure 9: Area of verification used for the line transition evaluation.

- [//stacks.stanford.edu/file/druid:yt916dh6570/Elder_Digman_Foreign_Bill_Recognition.pdf](http://stacks.stanford.edu/file/druid:yt916dh6570/Elder_Digman_Foreign_Bill_Recognition.pdf), 2013.
- [10] A. Frosini, M. Gori, and P. Priami. A neural network-based model for paper currency recognition and verification. *IEEE Transactions on Neural Networks*, 7(6):1482–1490, Nov 1996.
- [11] Stefan Glock, Eugen Gillich, Johannes Georg Scheade, and Volker Lohweg. Authentication of security documents, in particular banknotes, August 2010. US Patent App. 13/389,769.
- [12] T Haist and H.J Tiziani. Optical detection of random features for high security applications. *Optics Communications*, 147(1-3):173–179, 1998.
- [13] F.M. Hasanuzzaman, Xiaodong Yang, and YingLi Tian. Robust and effective component-based banknote recognition for the blind. *IEEE Transactions on Systems, Man, and Cybernetics, part C: Applications and Reviews*, 42(6):1021–1030, Nov 2012.
- [14] C. Herley, P. Vora, and S. Yang. Detection and deterrence of counterfeiting of valuable documents. In *International Conference on Image Processing (ICIP)*, volume 4, pages 2423–2426, Oct 2004.
- [15] M. Ionescu and A. Ralescu. Fuzzy hamming distance based banknote validator. In *14th IEEE International Conference on Fuzzy Systems (FUZZ)*, pages 300–305, May 2005.
- [16] Ye Jin, Ling Song, Xianglong Tang, and Ming Du. A hierarchical approach for banknote image processing using homogeneity and ffd model. *Signal Processing Letters, IEEE*, 15:425–428, 2008.
- [17] Ruth Judson and Richard D Porter. Estimating the worldwide volume of counterfeit us currency: data and extrapolation. *FEDs Working Paper*. 2003.
- [18] Christoph H. Lampert, Lin Mei, and T.M. Breuel. Printing technique classification for document counterfeit detection. In *International Conference on Computational Intelligence and Security*, volume 1, pages 639–644, Nov 2006.
- [19] Volker Lohweg, Jan Leif Hoffmann, Helene Dörksen, Roland Hildebrand, Eugen Gillich, Jürg Hofmann, and Johannes Schaede. Banknote authentication with mobile devices. In *Proceedings of the International Society for Optics and Photonics (SPIE)*, volume 8665, pages 866507–866507–14, 2013.
- [20] D. Lowe. Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision (IJCV)*, 60(2):91–110, 2004.
- [21] Aoba Masato, Tetsuo Kikuchi, and Yoshitatsu Takefuji. Euro banknote recognition system using a three-layered perceptron and rbf networks. *IPSJ Transactions on Mathematical Modeling and its Applications (TOM)*, 44(7):99–109, may 2003.
- [22] John Oliver and Joyce Chen. Use of signature analysis to discriminate digital printing technologies. *NIP & Digital Fabrication Conference*, 2002(1):218–222, 2002.
- [23] Nektarios Paisios, Alex Rubinsteyn, Vrutti Vyas, and Lakshminarayanan Subramanian. Recognizing currency bills using a mobile phone: An assistive aid for the visually impaired. In *Proceedings of the 24th Annual ACM Symposium Adjunct on User Interface Software and Technology*, UIST '11 Adjunct, pages 19–20, New York, NY, USA, 2011. ACM.
- [24] S.B. Pollard, S.J. Simske, and G.B. Adams. Model based

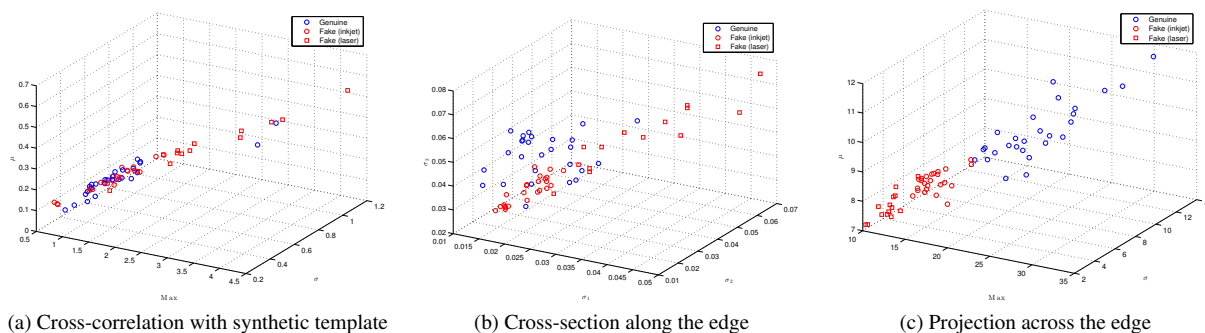


Figure 10: 3D feature space.

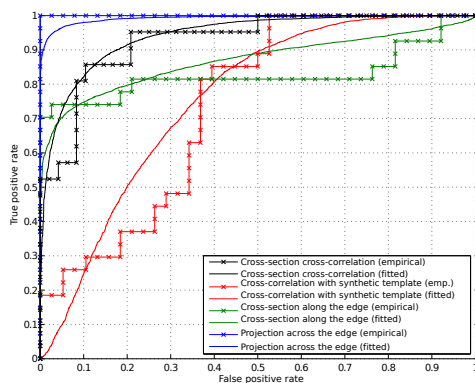


Figure 11: Comparison of ROC curves.

print signature profile extraction for forensic analysis of individual text glyphs. In *IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6, Dec 2010.

- [25] Grant Robertson. Funny money: How counterfeiting led to a major overhaul of canada’s money. ”<http://www.theglobeandmail.com/report-on-business/economy/currencies/funny-money-how-counterfeiting-led-to-a-major-overhaul-of-canadas-money/article554632/?page=all>”, Dec 2011. [Online; accessed February 6th 2015].
- [26] Ankush Roy, Biswajit Halder, and Utpal Garain. Authentication of currency notes through printing technique verification. In *Proceedings of the 7th Indian Conference on Computer Vision, Graphics and Image Processing, ICVGIP ’10*, pages 383–390, New York, NY, USA, 2010. ACM.
- [27] Ilya Toytman and Jonathan Thambidurai. Banknote recognition on android platform. Available at: http://www.stanford.edu/class/ee368/Project_11/Reports/Toytman_Thambidurai_Coin_counting_with_Android.pdf, 2011.
- [28] A. Vila, N. Ferrer, J. Mantecón, D. Bretón, and J.F. García. Development of a fast and non-destructive procedure for characterizing and distinguishing original and fake euro notes. *Analytica Chimica Acta*, 559(2):257–263, 2006.
- [29] Jianbin Xie, Chengang Qin, Tong Liu, Yizheng He, and Ming Xu. A new method to identify the authenticity of banknotes based on the texture roughness. In *Proceedings of the International Conference on Robotics and Biomimetics, ROBOT’09*, pages 1268–1271, Piscataway, NJ, USA, 2009. IEEE Press.
- [30] W.Q. Yan and J. Chambers. An empirical approach for digital currency forensics. In *IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 2988–2991. IEEE, May 2013.
- [31] Toru Yoshizawa, J Hidaka, and J Seto. Banknote verification using 3d profilometry techniques. ”<https://spie.org/x20198.xml>”, 2008. [Online; accessed November 5th 2014].