Model Based Print Signature Profile Extraction for Forensic Analysis of Individual Text Glyphs

Stephen B. Pollard, Steven J. Simske, Guy B. Adams

HP Laboratories
HPL-2010-173

Keyword(s):

Security printing, forensic imaging, anti-counterfeiting, inspection

Abstract:

Forensic analysis of individual printed items, including single characters, enables the addition of some level of security to any printed item (label, document, package, etc.). In this paper, we present a model-based approach for extracting a signature profile around the outer edge of virtually any text glyph. We show that for two high-resolution imaging devices (the Dyson Relay CMOS Imaging Device, called DrCID, and a high speed line-scan camera) this signature encodes that part of the glyph boundary that is due to the random fluctuation of the print process, enabling significantly higher levels of forensic discrimination than previously shown. The model-based approach enables a security workflow where the line-scan device is integrated into production line inspection with later forensic investigation in the field using the DrCID device. We also develop a simple shape descriptor to encode the signature profile, making it easier to manipulate, test and store. We argue that the shape descriptor provides forensic-level authentication of a single printed character.

External Posting Date: October 21, 2010 [Fulltext] Approved for External Publication
Internal Posting Date: October 21, 2010 [Fulltext]
To be presented at IEEE Workshop on Information Forensics and Security - WIFS'10, Seattle, December 12-15, 2010.

Model Based Print Signature Profile Extraction for Forensic Analysis of Individual Text Glyphs

Stephen B. Pollard [#1], Steven J. Simske [*2], Guy B. Adams [#3]

[#] *Hewlett Packard Laboratories, Long Down Avenue, Stoke Gifford, Bristol, BS34 8QZ, UK*

[1] stephen.pollard@hp.com

[3] guy.adams@hp.com

[*] *Hewlett Packard Laboratories, 3404 E. Harmony Rd., MS 36, Fort Collins CO 80528, USA*

[2] steve.simske@hp.com

***Abstract*— Forensic analysis of individual printed items, including single characters, enables the addition of some level of security to any printed item (label, document, package, etc.). In this paper, we present a model-based approach for extracting a signature profile around the outer edge of virtually any text glyph. We show that for two high-resolution imaging devices (the Dyson Relay CMOS Imaging Device, called DrCID, and a high speed line-scan camera) this signature encodes that part of the glyph boundary that is due to the random fluctuation of the print process, enabling significantly higher levels of forensic discrimination than previously shown. The model-based approach enables a security workflow where the line-scan device is integrated into production line inspection with later forensic investigation in the field using the DrCID device. We also develop a simple shape descriptor to encode the signature profile, making it easier to manipulate, test and store. We argue that the shape descriptor provides forensic-level authentication of a single printed character.**

I. Introduction

Counterfeiting, warranty fraud, product tampering, smuggling, product diversion and other forms of organized deception are driving the need for improved brand protection. The potential for security printing and imaging to provide forensic level authentication is well recognized and offers the potential to form part of the general approach to product and document security [1].

Forensic analysis of printed material including documents, packaging and labels, can be classified into two broad categories: 1) device forensics/ballistics [2]-[4] where a document (or set of documents) is analyzed to see if it was printed on a specific device or class of devices; 2) print forensics [5], [6] wherein individual printed artifacts are uniquely identified. This second class, which is of interest here, allows the differentiation of individual instances of the same or highly similar documents - including high quality copies. In this way, for example, forensic information on an individual label can be used to test a high value products authenticity. In order to carry out this task in an effective manner, a central registry must be built to store the forensic information so that it can subsequently be tested in the field (see Figure 1 for an overview of a possible workflow).

WIFS'2010, December, 12-15, 2010, Seattle, WA, USA.
978-1-4244-9080-6/10/*$26.00 ©2010 IEEE.*

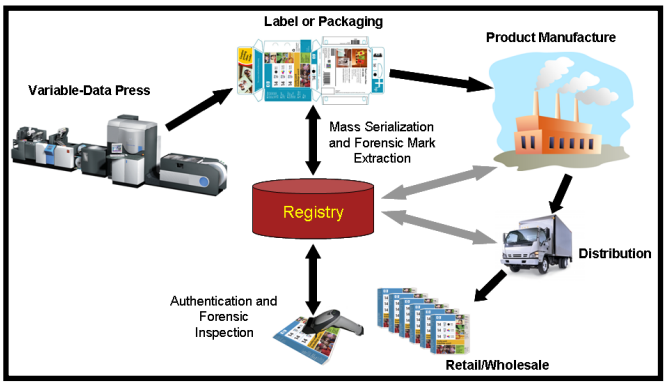

Figure 1. Diagram of a simplified workflow in which a variable data press is used to print labels or packaging that includes both serialization data and forensic marks which are stored in a registry at or shortly after printing. An inspection device can then be used in the field (at retail or wholesale) to compare the printed forensic mark to data stored in the registry to prove validity.

In order to perform a forensic inspection task of printed material, it is necessary to recover a description of all or part of the document at sufficient resolution to resolve those unique properties of the print that are extremely difficult to copy. For the majority of printing technologies such unique properties result from the unrepeatable statistical properties of the print process itself and its interaction with the underlying structural properties of the substrate material on which it is printed. The workflow is greatly simplified if we select an individual (or small number of) forensic mark(s) to identify a document. The forensic mark can be any form of glyph, character or printed shape of sufficient size to carry information to determine if the forensic mark under investigation is the exact same unique forensic mark that was previously printed. In this way, print is used as a security mechanism preventing the counterfeit and copy of documents and product packaging.

It is advantageous to build the registry during the print process itself. This can be achieved by including a high-speed, high-resolution scanning device in the paper path of the printer and to read out images of selected forensic marks as they pass beneath it. Unfortunately, it easy to introduce errors in the shape of scanned characters either through mechanical variation or calibration inaccuracies and in practice these geometrical differences between the images tends to dominate

the inspection process. This means that it is necessary to resolve the line-scan-introduced differences before the print differences and similarities of the images of the forensic marks can be analyzed. Furthermore, because the spatial-scale at which the forensic properties of the printing process are manifest is so high—typically less than 10μm—it is necessary to resolve these induced geometrical errors to a very high degree of accuracy.

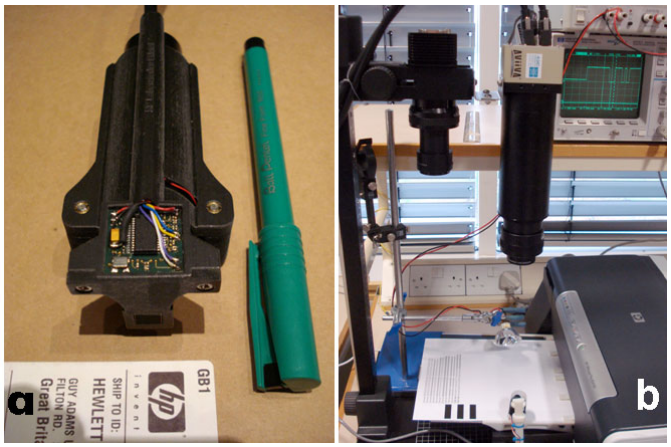

Figure 2. (a) DrCID with imaging window on the bottom edge; (b) Our experimental inline print and line-scan solution.

A. Previous Work

We have previously [7] demonstrated the utility of a low-cost USB-powered mini-appliance (Figure 2a) capable of resolving spatial features of 3.8 microns with 1:1 magnification. This is accomplished using a single Dyson relay lens in series with a mirror and a low cost 3-5 Mpixel CMOS image sensor. With a self-contained (white LED) illumination source, this Dyson relay CMOS imaging device (DrCID) affords the capture of individual typed characters with printing "parasitics"—such as the absorbance of ink into the fibers of the substrate (e.g. paper, cardstock, etc.) along with the droplet "tails" that exhibit micro-random aberrations as shown in Figure 4a.

We have also demonstrated [8] a prototype end-to-end solution where printed media is scanned at speed as part of an 'inline' print process. This is achieved with a high speed line-scan camera mounted above the output tray of an adapted HP K5400 office printer (Figure 2b). Currently we use an E2V 12K element 5μm pixel linear monochrome sensor that operates at 27K lines/s (0.14m/s theoretical surface speed) also with 1:1 optics. The experimental rig also features a high intensity halogen light source to enable exposure times shorter than the line period in order to minimize motion blur as the paper passes beneath it during the full speed page feed.

In general, the inline line-scan camera suffers from two sources of error: 1) calibration error with respect to the physical set up of the camera; 2) paper motion error. Calibration error results from a lack in precision in the alignment of the line-scan camera with respect to the direction of paper motion, and of average distance of the camera from the paper. This leads to small skew (sheer) and asymmetric magnification errors. Even if a line-scan system is brought into accurate calibration, there is no absolute guarantee that this can be maintained for all but the most rigid of mechanical arrangements. While the motion of the paper as it passes beneath the camera is reasonably constant, variations in gear timing, paper slip and vibrations can cause periodic small-scale perturbation in both the lateral and vertical/depth motions of the paper.

Most previous work in this area has been limited to pairs of images captured by a single class of imaging device. An early example [9] (see also [10]), recovers a print signature from low-cost digital optical-microscopes based on the radius profiles of binarized circular blobs (of physical diameter 0.07mm) averaged over up to 72 sectors of the circle (measured w.r.t. the centre of gravity of the blob). The blobs were located and registered using fiducial marks and compared based on a Euclidian distance metric. Previous work [7] with DrCID explored the use of any individual printable glyph or character as a forensic mark. Similar to [9] forensic authentication was based on the analysis of the perimeter of thresholded binary image components (in this case over 360 1° bins), but with a number of extra profile measures in addition to radius. Each pair of profiles was aligned to optimize the following normalized similarity metric:

$$S = 1-(SAD)/((SA1+SA2)/2)$$

where SAD is the sum of absolute differences and SA1 and SA2 are the sum of absolute values of the first and second profile measure respectively.

In [8] we adopted a model-based approach that separated the truly random part of the outline of the individual printed character, which we termed a signature profile, from the shared shape-conveying component. This allowed forensic level authentication to be achieved between the very different optical devices (DrCID and the line-scan camera) with the minimum of engineering effort and cost: we neither needed to use accurate calibration nor precise monitoring of the paper motion past the line-scan device. However, in this case the problem was greatly simplified by using a symmetric "o" character as the basis of the experimentation, modeling its shape as an ellipse. We adopted a similar approach in [11] to recover similar signature profiles with respect to square color barcodes. In this case, the orientation information conveyed by the non-payload indicia of the barcode allowed the signature profile to be extracted in an order fixed by the model (which was not the case for the ellipse model used in [8]). This allowed the introduction of a simple fixed order shape warp descriptor (which is typically less than 100 bits long for the examples presented in [11]) that can be extracted from the profile and used in batch inspection or other forensic security applications.

B. Contribution

Here we present for the first time the extraction of a general model based signature profile (MBSP) which is able to encode the random perturbations associated with virtually any printed character or glyph. We present a number of experiments to show how the MBSPs can be used for forensic inspection both

for intra (DrCID to DrCID) and inter device (DrCID to line-scan) comparisons. This allows almost any printed text glyph to be used as a forensic mark for a host of security applications. We further generalize the use of the shape warp descriptor introduced in [11] and show that a simple warp code is able to encode the signature profile in an effective manner, making it easier to manipulate, test and store.

II. METHOD

In order to generalize the use of models for the extraction of signature profiles from any text glyph it is necessary to (1) have a source of suitable models, (2) have a robust and accurate way to locate models in captured images, and (3) define the extraction of the signature profile with respect to the model. In this paper we concentrate, mainly, on the third aspect of this problem as this is where the novelty of our solution lies.

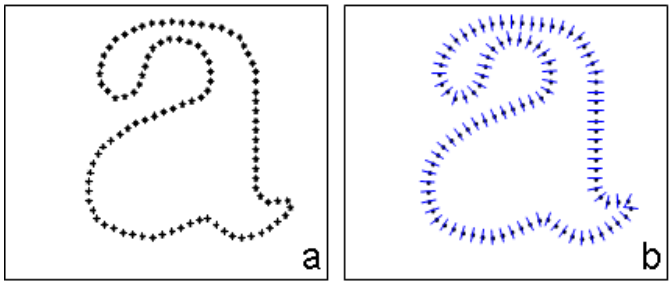

Figure 3. Simplified model for the outline of a Times lowercase 'a'. This model is composed of 100 feature points shown alone in (a) and with associated normals in (b). Note that in practice to avoid sampling artifacts models are an order of magnitude more dense than shown in this figure with typically between 1000 and 2000 feature points.

A. Model Based Signature Profiles (MBSP)

We define our models simply as a set of N uniformly spaced points (x, y coordinates) defining the outer edge of a character glyph and associated unit normal vectors (u, v). Figure 3 shows an illustration of a model of the outer contour of a Times lowercase 'a'. Using a model to extract a signature profile has 4 major advantages over the prior art, where typically a set of lines radiating from the centre of gravity of a forensic mark was used as a basis for characterizing its forensic properties [7], [9]. First and foremost, as discussed already, the signature profile so extracted comprises only the truly random perturbations introduced by the printing process rather than the general shape conveying properties of the outline. Second, using a model allows forensic comparison between very different images as we see in Figure 4 where DrCID and line-scan images are compared. Thirdly, non-convex shapes, such as the outline of the 'a' in Figure 3, have a uniform description free from multiple crossings, critical points and discontinuities that plague the simpler approach. And last but not least, provided the model is free from internal axes of symmetry (not true of the 'o' characters used in [8]) the MBSP recovers a description the order of which is fixed w.r.t. the model. This makes the matching process more simple and robust and facilitates the extraction of generalized shape warp codes as discussed in section 2.2.

Consider the signature profile extraction process shown in Figure 4. For each of the DrCID and line-scan images the model described as:

$$M = \begin{bmatrix} x \\ y \\ u \\ v \end{bmatrix} = \begin{bmatrix} x_1 & \dots & x_i & \dots & x_N \\ y_1 & \dots & y_i & \dots & y_N \\ u_1 & \dots & u_i & \dots & u_N \\ v_1 & \dots & v_i & \dots & v_N \end{bmatrix}$$

is matched to the outline of the text glyph subject to a homogeneous transformation of the form

$$H'_{xy} = \begin{bmatrix} x' \\ y' \\ {}_N1 \end{bmatrix} = TH_{xy} = T\begin{bmatrix} M_{xy} \\ {}_N1 \end{bmatrix} = \begin{bmatrix} t_{1,1} & t_{1,2} & t_{1,3} \\ t_{2,1} & t_{2,2} & t_{2,3} \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \\ {}_N1 \end{bmatrix}$$

(where ${}_N1$ is a vector of N ones) which covers both the similarity (rotation and scale) when matching to the DrCID image as in Figure 4c and affine (which also includes skew) when matching to the line-scan data in Figure 4d.

In order to extract each signature profiles a normal image is constructed. At each model point an interval along the normal direction is defined between two control points

$$N'_{xy} = M_{xy} - dM_{uv} = \begin{bmatrix} x \\ y \end{bmatrix} - d\begin{bmatrix} u \\ v \end{bmatrix}$$

and

$$N''_{xy} = M_{xy} + dM_{uv} = \begin{bmatrix} x \\ y \end{bmatrix} + d\begin{bmatrix} u \\ v \end{bmatrix}$$

where d is a fixed distance corresponding percentage of the model size (i.e. mean absolute distance of each model point from the centre of gravity of the model). Once N'_{xy} and N''_{xy} are transformed into the respective images of Figure 4 with appropriate similarity (in 4e) and affine (in 4f) transforms the loci of the control points are shown overlaid in red and yellow. By uniformly sampling the underlying image between these points (using standard bilinear interpolation to achieve sub-pixel accuracy) the required normal profile images in Figures 4g and 4h are constructed.

Many methods can be used to recover the signature profile from the profile image, including simple thresholding or maximum edge detection. We have found the following grayscale edge metric that combines all the data in the profile image to work well. For each column in the profile image the signature profile is defined as:

$$p_i = \sum_j jw_j e_{ij} \Big/ \sum_j w_j \,|\, e_{ij} \,|$$

where e_{ij} is an edge strength corresponding to the digital derivative of the profile image along the column i and w_j is a

windowing function (in our case a Gaussian with standard deviation ¼ the column height centered on the mid point of the column). Dividing by a normalizing sum of windowed absolute edge strength results in a measure that achieves robustness to both scene content and illumination variation.

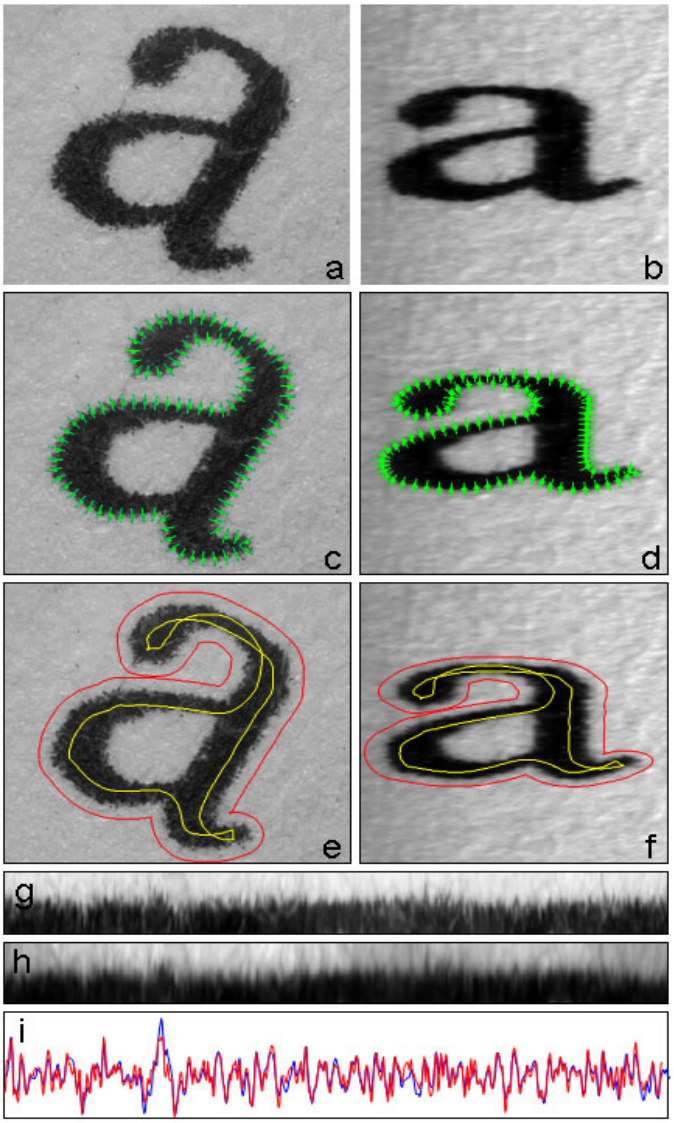

Figure 4. Illustrates, for a Times 12 point 'a', the extraction and matching of MBSPs. Where: (a) is a 900x800 (wide x tall) image captured by DrCID; (b) is a 400x400 image of the same character captured as it is printed by the line-scan camera; (c) and (d) show superimposed transformed model data with approximate normal vectors; (e) and (f) show the loci of sampled regions for the extracted normal profile images in (g) and (h) respectively. Each column of (g) and (h) corresponds to sampling on a vector between the loci along the normal vector for each individual (x, y) contour point of the model. Finally (i) shows matched MBSPs extracted from (g) and (h) and warped using DTW.

In [8] we show that it is possible to resolve the small but significant residual linear and non-linear errors that are due to inaccuracy in the model and the model fitting process as well as non-linear variation in the image (particularly for the line-scan image, but also significant for DrCID). First we condition the profile by removing low frequency variations (subtracting off a low pass filtered version of the profile; in our case a Gaussian with a large standard deviation; e.g. 9.0). Then, when comparing profiles rather than simply computing a SAD (sum absolute difference) error metric we use a modified form of variable penalty Dynamic Time Warping (DTW) [12]. That is the timeline of one signature profile is warped to reduce the SAD error with respect to the other but where the degree of warp incurs a proportionate matching cost (see [8] for details).

Notice, in Figure 4i that, despite the considerable difference in the spatial frequency content and the high degree of physical distortion (an almost a 50% scaling in the vertical direction) between the DrCID and line-scan data, the recovered signature profiles are quite similar and are brought into close correspondence using the DTW approach.

B. Shape Warp Coding (SWC)

In [11] a shape warp descriptor/code was introduced for the limited case of micro-color-tile inspection. It was shown that a shape distortion encoding distance (SDED) based on the SWC allows batch inspection and validation (i.e. the use of a small number of scanned deterrents to determine whether a batch of products is genuine or counterfeit).

Here we use the MBSP as the basis SWC for the general case of any irregular text glyph (i.e. one for which the matching process recovers a unique model location). We first divide the signature profile into N equal length segments. Then for each, compute a sum squared error (SSE) of the residual (which is akin to a local variance):

$$SSE_j = \sum_{p_i \in segment(j)} (p_i - \mu_j)^2$$

where p_i is the signature profile over the segment j and μ_j is its mean value over the that segment. We then use the mean (or median) value of the *SSE* (or a factor or multiple of it) as an atomic unit of encoding (a "digit"), to form an N-position string which is the *SWC*:

$$SWC(j) = \left\| SSE_j \Big/ SSE_{mean} \right\|$$

where $\|.\|$ is a rounding function. The SDED, for comparing the SWCs of any two forensic marks, is thus defined as:

$$SDED = \sum_j \min\left(|\, SWC_1(j) - SWC_2(j) \,|, T_{\max} \right)$$

where T_{max} is an optional threshold to improve robustness. The SDED can be considered a form of modified Hamming Distance where the expected value of *SWC(*)* is 1 at each digit due to the normalization process described. For example, a pair of SWCs (N=50) extracted from DrCID data for the same printed 'a' and their absolute difference are:

SWC1 = 11011111201101111211211121111110112121121111010111
SWC2 = 11111111210100101211211121112111011111112111011210
DIFF = 00100000011001010000000000010000010100000000001101

for which the SDED is 11 (or 0.22 when normalized by N).

III. Experiments and Results

Results are presented for a number of experiments using data collected from our prototype integration of an HP Inkjet K5400 office printer and line-scan camera. An example line-scan captured image swath is shown in Figure 5. The 9 lowercase 'a's and 's's in each such image are also captured twice using the DrCID device, once approximately vertical and for a second time at a considerable angle (about 30° from vertical). For comparison, the same data was also printed on a HP Photosmart 2610 all-in-one (Inkjet) printer (PS2610 for short) and captured twice with DrCID.

In experiment 1, we compare MBSP to the prior art method described in [7] for just the data captured by DrCID (the prior art method is not applicable to the distorted line-scan data). Specifically, we compare 4 sets of DrCID data with and without rotation totaling 72 individual 'a' and 's' images that are each compared to the 71 other images of the same letter (of which just 36 comparisons are valid and 2520 are not). In Figure 6, we plot the similarity metric S, from section 1.1, for each comparison of each character using each method (using best of the metrics generated by the prior art which was max-radius; see [7] for details). As can be seen, the results are far better for MBSP where there is a very clear gap between the distributions of valid matches and those for incorrect comparisons.

In Figure 7 we look at the distributions of similarity scores for the 2520 false matches for the modeled based approach. Concluding that the distributions are reasonably close to (but not exactly) Gaussian and assuming the same is approximately true for valid matches (where the sample is much smaller) then we can use a Z-score approximation (it is an approximation as these are sample, rather than population, statistics) to measure the separation of the two populations

$$Z = \left|\overline{S}_V - \overline{S}_F\right| / \left(\sigma_V + \sigma_F\right)$$

that is the absolute difference of the mean similarity scores for veridical and false matches divided by the sum of their standard deviations.

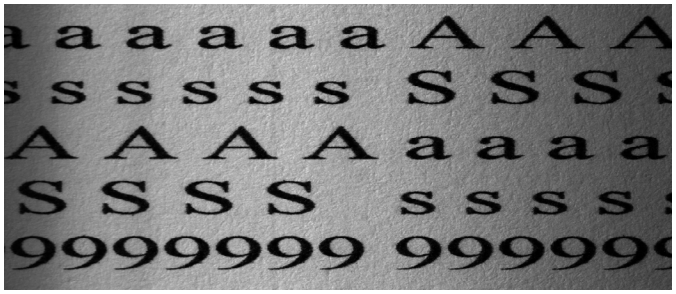

Figure 5. Swath of image data captured by line-scan camera. Only the lower case 'a's and 's's were used in the experiments presented here.

For the MBSP data in Figure 6 this results in Z-scores of 18.1 and 13.7 respectively for the 'a' and 's' data corresponding to infinitely small probabilities of false authentication (compared to Z-scores of 3.2 and 2.8 by the previous method [7] – in fairness that method reported much better results when the forensic mark was not rotated).

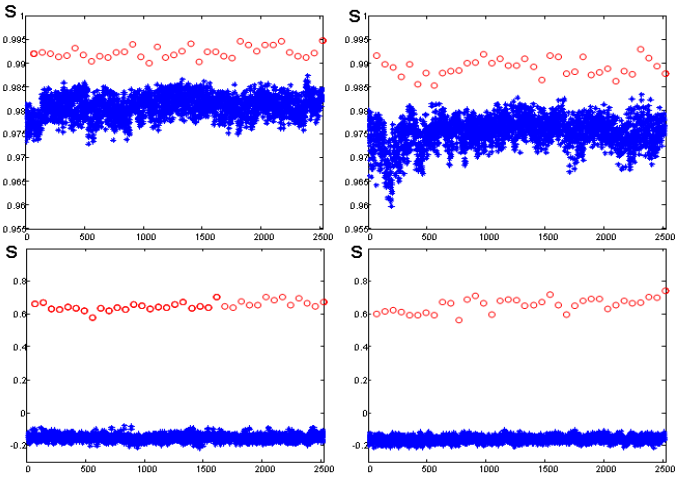

Figure 6. Results of experiment 1. Similarity data S for prior art method [7] top and MBSP at the bottom for 'a's on the left and 's's on the right. Valid matches are red circles and false matches blue stars. Note that as the range of similarity is small for the prior art (0.955 to 1) compared to the MBSP (-0.2 to 0.8) as for the former it also encodes the shape of the text glyph rather than just the perturbations.

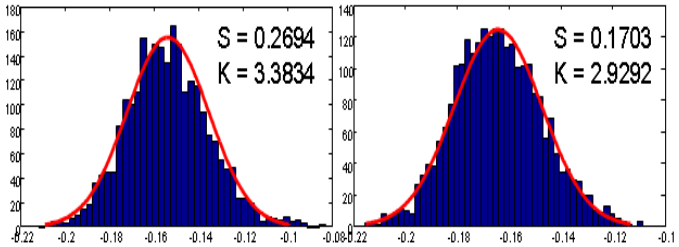

Figure 7. Histograms and Gaussian distributions for the false matches of experiment 1 for the MBSP method; 'a's on the left and 's's on the right. Skewness and Kurtosis are close to Gaussian (0, 3) but given the large sample size they do show statistically significant deviations except for the Kurtosis of the 's' data.

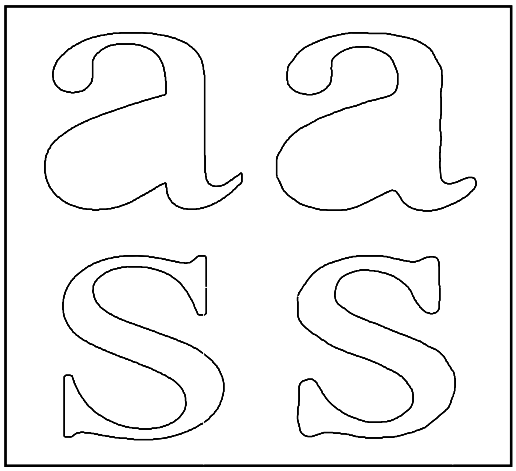

Figure 8. Left images show 'a' and 's' outline models recovered from the 12 point Times Roman Font. Right images show the result of a combination process in which 36 outlines recovered by DrCID are combined by first selecting a seed and then transforming (using a similarity transform) each of the other outlines to the seed. Model points are selected uniformly in the seed and updated to the mean of the closest points in the transformed outlines. This then forms the seed for an iterative refinement process.

In experiment 2 we compare two different sources of model data (see Figure 8). One is based on the Truetype font and the other is built by combining DrCID images of all 36 instances of each character used in the previous experiment. The latter uses a form of Least Squares Congealing [13] operating on binary edge data rather than image intensities. Figure 9 plots statistics for veridical and false matches for intra-device (DrCID to DrCID with rotation) and inter-device (DrCID to line-scan camera). In each case, the built model performs significantly better than that derived directly from the font. This is due to the vagaries in the printing process that result in numerous changes to the font outline in the print driver, firmware and hardware. Interestingly, the comparison with the PS2610 printer also shows an improvement for the built model even though the same model, built using DrCID data from the K5400 prints, was used (Figure 9, right).

In experiment 3, we performed of a series of SWC experiments computing SDED measures between the valid and false matches for the rotated DrCID data as the number of segments N and atomic unit of coding were varied. Figure 10 shows results for the default atomic unit set to mean SSE (which was found to be optimal) for a range of SWC length N between 50 and 400 samples with best forensic security at 200 samples where the probability of false validation is less than 10^{-9}.

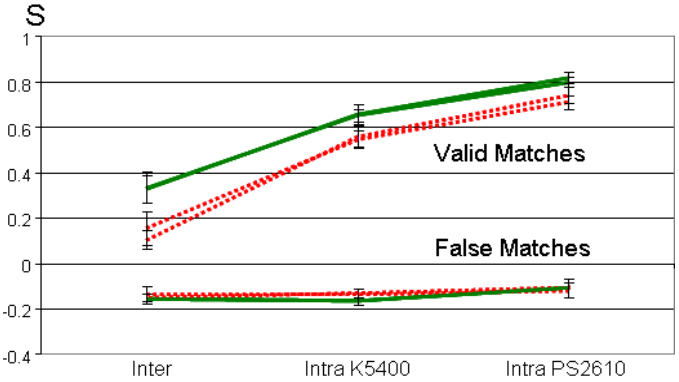

Figure 9. Results of experiment 2. Valid and false mean similarity scores (standard deviations shown as error bars) for font model (red dots) and built model (green solid) for near identical 'a' and 's' data. Each of 3 experimental conditions (inter: between DrCID and line-scan; and 2 intra: DrCID alone for K5400 and PS2610 print data) show improvement in mean similarity score for valid matches for built model over font model. Improvements for PS2610 are due to the larger print perturbations for that device compared to the K5400.

IV. Discussion & Conclusions

We have shown, for the first time, a general method for using a model to extract a print signature from the outer boundary of a text glyph. It has been shown that this approach provides levels of forensic security that far exceed those of the prior art. Even for the difficult case where a forensic mark is scanned at print time using a line-scan camera, sufficient discrimination is achieved (Z-scores of 5.5 and 6.2 for 'a's and 's's corresponding to probabilities of a false validation of less than 2.3×10^{-8} and 10^{-9} respectively) despite the considerable degradation of the inline device. We have also demonstrated the utility of shape warp coding that is supported by the model based approach. This provides degraded but still excellent levels of security in a compact and tractable fashion Such intermediate levels of verification are useful because, they support a tiered approach where the ability/need to fully forensically verify the validity of a forensic mark is reserved for a privileged user and/or device with access to a less public database. They also have the potential to be robust to damage without modification – a possibility which will be the focus of future research.

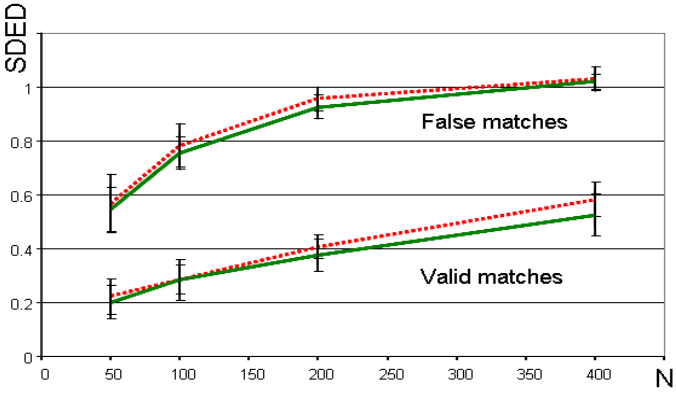

Figure 10. Results of experiment 3. Valid and false mean SDED values (standard deviations shown as error bars) for 'a's (red dots) and 's's (green lines) for range of sample sizes N. As SDED is a difference score false matches have higher values than valid ones.

Acknowledgement

We would like to thank Helen Balinsky for her insightful comments regarding the work presented in this paper.

References

[1] D. Pizzanelli, *The Future of Anti-Counterfeiting, Brand Protection and Security Packaging V*, Pira International Ltd., Leatherhead, UK, 2009. (see http://www.intertechpira.com)

[2] E. Kee and H. Faird, "Printer profiling for forensics and ballistics", *ACM MM&Sec,* pp 3-10, 2008.

[3] S.J. Simske, M. Sturgill, P. Everest, and G. Guillory, "A system for forensic analysis of large image sets," Proc. IEEE WIFS 2009, pp. 16-20. 2009.

[4] P-J. Chiang, N. Khanna, A. K. Mikkilineni, M. V. Ortiz Segovia, S. Suh, J. P. Allebach, G. T-C. Chiu & E. J. Delp "Printer and scanner forensics: examining the security mechanisms for a unique interface", *IEEE Signal Processing Magazine* ***72***, 2009.

[5] J. J. Plimmer, "Choosing correct forensic marker(s) in currency, document and product protection", *SPIE-IS&T* ***6075***, 2008.

[6] P. V. K. Borges, J. Mayer, E. Izquierdo, "A practical protocol for digital and printed document authentication", *EUSIPCO* ***15***, 2007.

[7] S.J. Simske and G. Adams, "High-resolution glyph-inspection based security system", *IEEE ICASSP*, 2010.

[8] S.B. Pollard, G. Adams and S.J. Simske, "Resolving distortion between linear and area sensors for forensic print inspection", *IEEE ICIP,* 2010.

[9] B. Zhu, J. Wu and M.S. Kankanhalli, "Print signature for document authentication", *ACM CCS*, pp 145-154, 2003.

[10] A. Idrissa, T. Fournel & Alain Aubert, "Secure embedded verification of print signatures", *J. Phys.: Conf. Ser.* ***206*** *012036*, 2010.

[11] S.J. Simske, S.B. Pollard & G. Adams, "An imaging system for simultaneous inspection, authentication and forensics", *IEEE IST*, 2010.

[12] D. Clifford, G. Stone, I. Montoliu, S Rezzi, F.P. Martin, P. Guy, S. Bruce and S. Kochhar, "Alignment using variable penalty dynamic time warping", *Anal. Chem. 81*, pp 1000-1007, 2009.

[13] E. Learned-Miller, "Data driven image models through continuous joint alignment", *IEEE PAMI*, **28(2),** 2006.