https://doi.org/10.2352/ISSN.2470-1173.2019.5.MWSF-544

Explaining and improving a machine-learning based printer identification system

Karthick Shankar, Zhi Li, Jan Allebach
Purdue University, West Lafayette, IN

Abstract

Counterfeiting of currency globally remains a significant problem to this day. According to the authorities, a large portion of this fake currency is produced by Small Office or Home Office inkjet printers. In this paper, we explain why a previously developed machine learning based Printer Identification System works with high accuracy and we investigate to improve the stability and generalization of the classifier.

We study the print patterns of 8 inkjet printers from different manufacturers. We look at the features of the data by reducing its dimensions using Principle Component Analysis. This shows significant separation between printers which implies that the Deep Neural Network was able to pick up on key differences. The results are also comparable with that of reducing dimensions with Linear Discriminant Analysis. The model however does have some limitations regarding ink density and print media. It always classifies an image amongst the trained printers and does not show anomalies. For this, we consider the Gaussian distribution of target printers to see how the probabilities fared when trained and fitted separately for each printer, thus having a set of images that do not fit in with any of the printers for which the classifier was trained. The results acquired from these methods have contributed to making a more real-world implementation of our classifier, named LAPIS (machine-Learning Applied Printer Identification System), for printer forensics.

Introduction and Related Works

In a 2006 report, the U.S. Secret Service estimated that 1 in 10,000 currency notes in circulation is a counterfeit. In Europe, as of a report published in 2015, there are about 800,000 counterfeit Euro notes pulled from circulation each year. Small Office Home Office (SOHO) inkjet printers account for over 50% of the production of counterfeit currency notes in Europe [1]. The "feel, look, tilt" methods proposed by the European Central Bank, while effective, can't distinguish between well-made counterfeit notes and authentic notes. The cheap Small Office Home Office printer market has greatly broadened the opportunities for abuse of trust through the generation of fallacious documents [2]. The process of printer forensics can aid this front by giving details about the printer that was used to print a particular currency note. Even knowing that a certain group of printers were not used in printing a counterfeit note can be valuable information to the authorities [3].

Tackling this issue of forgery has been attempted in numerous ways such as image texture analysis [4] and gray level co-occurance through watermarking [5]. However, the deep learning pipeline proposed in [1] provides an efficient and generalized approach. Numerous studies like [6] have provided general insight onto neural networks and their applications, but none exist particular to this application.

Previously, we designed 4 different printer intrinsic features to characterize the dot patterns at a microscopic level based on the analysis of the printer dot structure in highlight regions. We considered the spatial arrangement and size of individual ink drops in dispersed-dot, aperiodic (stochastic) halftone patterns [1]. We also proposed a machine learning based Printer Identification System that uses the Residual Neural Network and the Support Vector Machine classifier. Our evaluation showed that the proposed system produces robust and reliable results. However, further steps need to be taken to verify this. Deep Neural Networks achieve high classification accuracy by adjusting the features according to the pre-defined statistical loss. Therefore, there is no guarantee that this approach reflects the true nature of the problem. This is why we need to concretely identify what the Deep Neural Network picks up on. Attempts have been made in the past with textual documents as in [7] and [8]. However, this study proposes to broaden the scope of that. As a continued study, we focus on two problems:

- First, for the previously developed Printer Identification System, due to the nature of neural networks, it is challenging to incorporate the features produced by a pre-trained neural network. It is also challenging to understand how we can optimize a given model because because the neural network is usually treated as a "black box". Therefore, we aim to find the reason for the high accuracy of classification to help us understand the model better.
- Secondly, we aim to further improve the classification model, to improve the stability and generalization of the model.

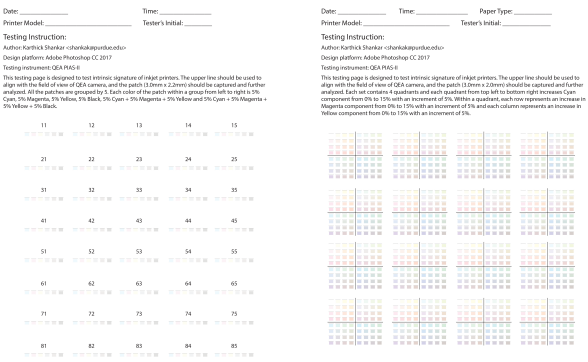
Experiment Setup

Data Acquisition

To collect data for this experiment, we use 8 different printers from 3 different manufacturers, namely HP, Canon and Epson. As a means of identification each of the printers are assigned alphabets ranging from A to H. We primarily use 6 of these for training and use the other 2 to test as anomalies "outside" the training set.

Since there may be microscopic variations in how a printer prints in different regions of the page, we designed a testing page, as shown in Figure 1a, containing multiple groups of patches all across the page. Each group has 6 patches, corresponding to varying percentages of CMYK colorants as follows:

- 5% Cyan
- 5% Magenta



(a) Phase 1 (b) Phase 2

Figure 1: Testing Phases

(a) Canon MG 2522 (b) Canon MX 922 (c) Epson XP 340

Figure 2: Sample Prints

- 5% Yellow
- 5% Black
- 5% Cyan, 5% Magenta, 5% Yellow
- 5% Cyan, 5% Magenta, 5% Yellow, 5% Black

For simplicity of reference, the last two items in the above list will be referred to as *555* patches and *5555* patches respectively. We chose 5% because the dots are dense enough to show characteristic spatial relationship while having reasonably low dot coalescence [1]. Each patch was designed to be $3mm \times 2mm$ so that it can be captured by the high resolution QEA PIAS-II camera with a resolution of 7663.4 dpi and a $3.2mm \times 2.4mm$ field of view. Each patch also has a black bar on top of it to help with alignment. Some images captured by this camera are shown in Figure 2.

From the printer side, all standard settings are used except for print quality which is set to "best" where possible with a resolution of 600 dpi.

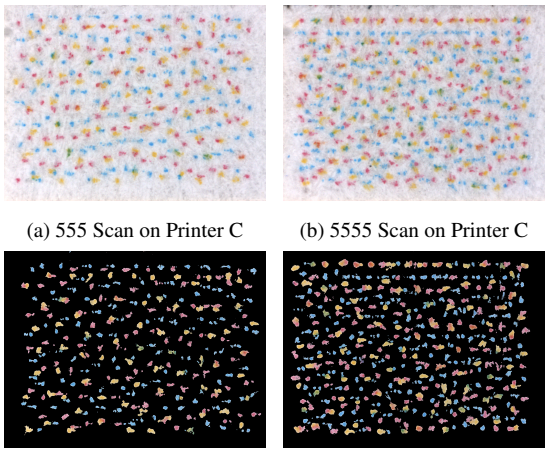
5555 patches and *555* patches have their own differences in terms of dot density as seen in Figure 3. SOHO inkjet printers try to "simulate" low percentages of black dots by increasing the percentages of the other colorants. This set of images with increased density also serves to expand our dataset.

Furthermore, to expand on the ability of the printer identification system, three different types of paper are used, namely linen, cotton and plain paper whose examples are shown in Figure 4.

In phase 2 of data collection, we collect samples of different colors separately as shown in the second version of the testing page in Figure 1b. We capture information about the different colored dots separately.

Data Preparation

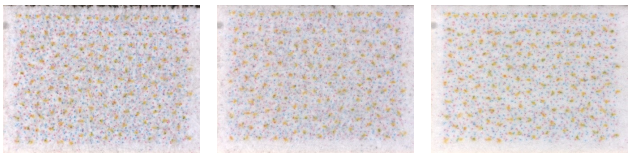
In the previous study, the scanned images were cropped into segments of 224×224 images to be fed into the residual neural



(a) 555 Scan on Printer C (b) 5555 Scan on Printer C

(c) 555 Black (d) 5555 Black

Figure 3: (a) and (b) show captured images of prints. (c) and (d) show colorant dots after media pixels are set to black ("Media Neutral").



(a) Plain Paper (b) Cotton Paper (c) Linen Paper

Figure 4: Different Types of Paper

network (ResNet50). However, this greatly reduces the amount of data we can capture in each segments. Thus, we increase the area of each segment to 448×448 and then resize it to 224×224 to use with ResNet50. We then generate 2048 features through ResNet50 using these segments, and analyze the features through the methods described below.

To include media-neutral images in addition to the different types of paper, we create another data set with the media pixels removed. By viewing the image in CIELab color space, we eliminate the media pixels which are represented as white pixels by filtering out pixels with high L^* components, i.e. high lightness components. This is computed by examining a measure of color saturation S in CIELab color space [1].

$$S = \frac{a^{*2} + b^{*2}}{L^*} \tag{1}$$

Since we have dispersed dots without much overlap as seen in Figure 3, we can eliminate media pixels by thresholding S.

Feature Analysis

We use the set of 2048 features generated by ResNet50 and analyze its separation using Principal Component Analysis (PCA). We also reduce the number of features from 2048 to 3 using PCA. This is to improve computation efficiency and to use only the most important features with maximum variance. PCA represents the pattern of similarity of the observations and the variables by displaying them as points in maps [9]. The possibility of overfitting the model is also reduced by reducing the amount of features [10]. To explain the performance of the previous Printer Identification System, we plot all the data points by

the first two or three PCA-reduced features generated from the plain paper patches. Our visualization in Figure 5a shows that by using PCA-reduced neural network features, the data points from different printers can be well separated by the model using the first two or three components.

To further cement the separation between printers, we apply Linear Discriminant Analysis (LDA) on our features. LDA is supervised and attempts to find a feature subspace that maximizes class separability [11]. If each of the printers P has a mean μ_i and the same covariance Σ, then the scatter between printer variability may be defined by the sample covariance of all the means.

$$\Sigma_b = \frac{1}{P}\sum_{i=1}^{P}(\mu_i - \mu)(\mu_i - \mu)^T \tag{2}$$

where μ is the mean of the means. Thus, the separation in a given direction $\vec{\omega}$ is given by

$$S = \frac{\vec{\omega}^T \Sigma_b \vec{\omega}}{\vec{\omega}^T \Sigma \vec{\omega}} \tag{3}$$

$\vec{\omega}$ is used to reduce the features from 2048 to 3 [12]. We analyze a visualization of the top 3 LDA-reduced features in Figure 5b. The clear distinction between printer clouds confirms the separation between printers.

We visualize the above two methods using the media neutral images as well. Figure 6a shows different sections of separation. There are two different sets of clouds, one containing the plain paper features and the other containing media neutral features. We hypothesize that this separation is a matter of scale and as such, we calculate the L2 norm of both datasets, say P, and normalize them separately as follows

$$P = \frac{P}{\sqrt{\Sigma_{k=1}^{2048} |P_k|^2}} \tag{4}$$

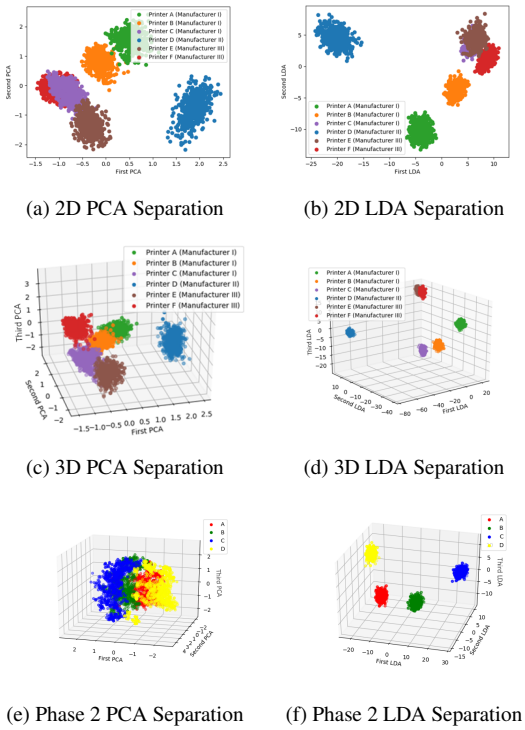
This puts all the clouds on the unit sphere, as shown in Figure 6b. The two sections of printer clouds only differ by one dimension. This difference is attributed to the fact that PCA has the feature with maximum variance in the first dimension. When comparing media-neutral and plain paper images, the feature with the highest variance is the one detecting media. Since that feature is binary (white background or black background), it visualizes the sections on opposite parts of the sphere.

However, even when using media neutral images alongside plain paper images, the separation between individual printers is visible.

The PCA-reduced and LDA-reduced plots for phase 2 of data collection is shown in Figure 5e. Printers retain their identity even when using colors separately which provides a much broader model. In Figure 7, which is the PCA cloud of only printer H, the points form a manifold. The surface generated by the points is visualized on top of the image. This unique surface provides more information than just a collection of points which can also attribute to the success of the model.

Classification

The previous study went into depth about using Support Vector Machine (SVM) to classify between printers using the PCA-reduced features. We get almost perfect results when testing that model with only plain paper. The following are the different attempted methods, each with their own successes and limitations.

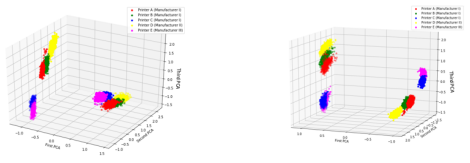


(a) 2D PCA Separation (b) 2D LDA Separation

(c) 3D PCA Separation (d) 3D LDA Separation

(e) Phase 2 PCA Separation (f) Phase 2 LDA Separation

Figure 5: Printer Separation



(a) Non-Normalized (b) Normalized

Figure 6: PCA on a combined set of Media Neutral and Plain Images

Support Vector Machine

As mentioned above, the previously developed Printer Identification System uses a Support Vector Machine (SVM) for classification because of several arguments that support high accuracy for it [13]. SVM works well when trained and tested with *555* patches or trained and tested with *5555* patches as shown in Figure 8a. It also works well when trained with *5555* patches on plain paper and tested with *5555* patches on cotton paper.

However, it fails when tested with media-neutral images and/or images with different dot densities. As mentioned above, *5555* patches have a more dense arrangement of dots as compared to *555* patches. Training on one and testing on the other results in very inaccurate classifications as seen in Figure 8c. We infer that the previous model is resistant to slight changes in media, but cannot tolerate significant changes like complete media removal.

We then build another classifier by expanding its training set. We train it with all the data, including different paper types, media neutral images and different dot densities. The result of testing on this is shown in Figure 9.

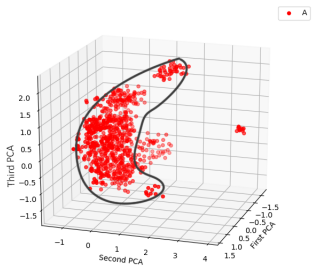
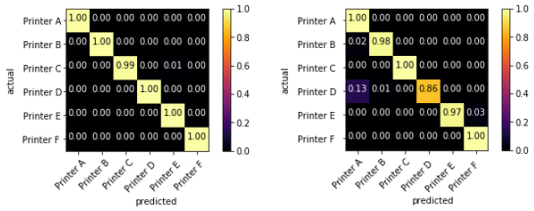


Figure 7: PCA point cloud of Printer H with manifold



(a) Train: 555 on Plain
Test: 555 on Plain

(b) Train: 5555 on Plain
Test: 5555 on Cotton

(c) Train: 555 on Plain
Test: 5555 on Plain

(d) Train: 555 on Plain
Test: 555 Media Neutral

Figure 8: Support Vector Machine Results

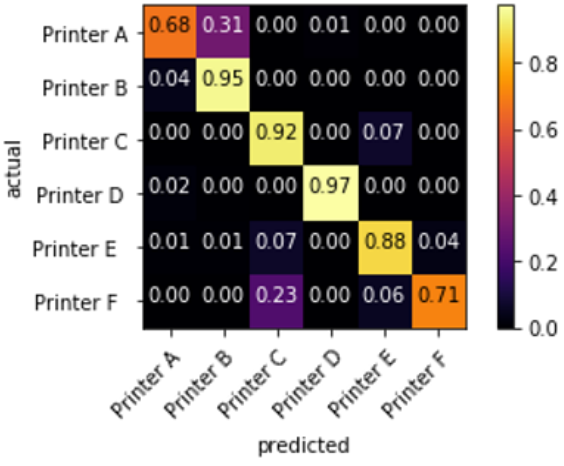


Figure 9: Trained with all data

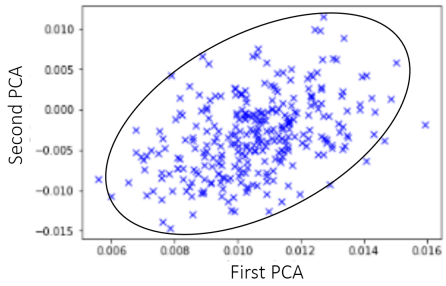


Figure 10: Gaussian Distribution of Printer A

Gaussian Anomaly Detection

Another problem in the previous classifier is that it is designed to pick one label from the six trained labels for an input image. This does not allow the classifier to detect anomalies, hence reducing the ability of generalization. Thus, we design a new non-discriminative classification framework that can detect an anomaly by analyzing the distributions of the data points. Based on the PCA analysis in Figure 5a, it can be observed that data points from the same printer tend to form their own cluster, which can be modeled with a Gaussian distribution [14]. Therefore, Gaussian distributions of target printers are also studied to see how the probabilities fared when trained and fitted separately for each printer.

For each printer $\mathbb{X}$, we use the data points to fit a unique Gaussian probability density function $N_{\mathbb{X}}(\mu,\Sigma)$ along with the mean μ and covariance matrix Σ. This Gaussian distribution $N_{\mathbb{X}}$ produces the probability ($P_{\mathbb{X}}$) of a given datapoint belonging to $\mathbb{X}$, which serves as a one-vs-all classifier. The point distributions are shown in Figure 10. Therefore, we can build a classifier by combining all the Gaussian distributions: a datapoint can be classified as from a given printer $\mathbb{X}$ only when $P_{\mathbb{X}} \gg P_i, i \neq X$ and $P_{\mathbb{X}} > 0.5$. In any other cases, this datapoint will be labeled as "unknown" or "anomaly" for further examination.

Single Class SVM

Since SVM generally had more stable results, we apply the same principles of Gaussian anomaly detection to use a single class SVM classifier instead. In this, 6 independent SVM classifiers are trained for each of the printers with the training set being split into two sections - one with the correct printer being labelled as 1 and the all the other data for all the other printers being labelled as 0.

Once trained, we use the image data from 2 previously unused printers (namely the HP DJ1112 and the EPSON WF2790) as a testing set and classify through each of the 6 SVM classifiers. If all 6 classifiers are unable to recognize the image, it is labeled as an anomaly. This implies that the image was not printed from any of the printers of the 6 classifiers. Every image that we tested outside of the 6 original printers was labelled correctly as an anomaly as shown in Figure 11.

Conclusion

We have analyzed and improved the previously developed Printer Identification System by visualizing the features from the ResNet neural network. We have trained the pre-existing model with different samples of images by varying dot density and paper types. We have also constrained our testing to the CMY space

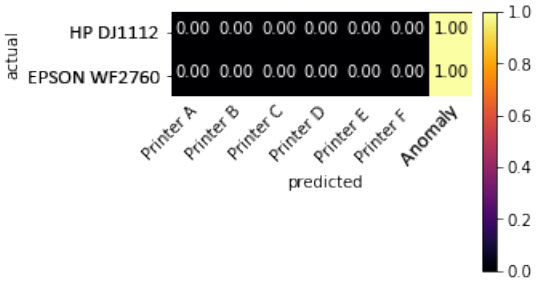


Figure 11: One Class SVM with Anomaly Column

instead of the CMYK space because many commercial SOHO printers try to be efficient with placement of black dots by printing a dense patch of colors instead. As mentioned above, the printers simply increase the density of other colorants to give the perceived effect of black. In addition, we have added an anomaly class to the classifier to ensure that other printers that are not included in this study are not incorrectly classified.

Acknowledgments

We want to thank Dr. Palghat Ramesh for suggesting the deep learning pipeline and giving us pointers along the way. We also want to thank Alexander Gokan for his contributions to this project.

References

[1] Z. Li, W. Jiang, D. Kenzhebalin, A. Gokan, and J. Allebach, "Intrinsic signatures for forensic identification of soho inkjet printers," *NIP Digital Fabrication Conference*, vol. 2018, pp. 231–236, 09 2018.

[2] P.-J. Chiang, N. Khanna, A. K. Mikkilineni, M. V. O. Segovia, J. P. Allebach, G. T. C. Chiu, and E. J. Delp, *Printer and Scanner Forensics: Models and Methods*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 145–187. [Online]. Available: https://doi.org/10.1007/978-3-642-11756-5_7

[3] L. M. Manevitz and M. Yousef, "One-class SVMs for document classification," *J. Mach. Learn. Res.*, vol. 2, pp. 139–154, Mar. 2002. [Online]. Available: http://dl.acm.org/citation.cfm?id=944790.944808

[4] A. K. Mikkilineni, P.-J. Chiang, G. N. Ali, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Printer identification based on texture features," *NIP Digital Fabrication Conference*, vol. 2004, no. 1, pp. 306–311, 2004. [Online]. Available: https://www.ingentaconnect.com/content/ist/nipdf/2004/00002004/00000001/art00069

[5] A. K. Mikkilineni, P.-J. Chiang, G. N. Ali, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, "Printer identification based on graylevel co-occurrence features for security and forensic applications," *Proc.SPIE*, vol. 5681, pp. 5681 – 5681 – 11, 2005. [Online]. Available: https://doi.org/10.1117/12.593796

[6] M. Egmont-Petersen, D. de Ridder, and H. Handels, "Image processing with neural networksa review," *Pattern Recognition*, vol. 35, no. 10, pp. 2279 – 2301, 2002. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320301001789

[7] G. N. Ali, A. K. Mikkilineni, E. J. Delp, J. P. Allebach, P.-J. Chiang, and G. T. Chiu, "Application of principal components analysis and gaussian mixture models to printer identification," *NIP Digital Fabrication Conference*, vol. 2004, pp. 301–305, 2004.

[8] O. Arslan, R. Kumontoy, A. K. Mikkilineni, J. P. Allebach, E. J. Delp, P.-J. Chiang, and G. T. Chiu, "Identification of inkjet printers for forensic application," *NIP Digital Fabrication Conference*, vol. 2005, no. 1, pp. 235–238, 2005. [Online]. Available: https://www.ingentaconnect.com/content/ist/nipdf/2005/00002005/00000001/art00067

[9] H. Abdi and L. J. Williams, "Principal component analysis," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, no. 4, pp. 433–459, 2010. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/wics.101

[10] N. M. Nasrabadi, "Pattern recognition and machine learning," *Journal of Electronic Imaging*, vol. 16, 2007. [Online]. Available: https://doi.org/10.1117/1.2819119

[11] M. Li and B. Yuan, "2d-lda: A statistical linear discriminant analysis for image matrix," *Pattern Recognition Letters*, vol. 26, no. 5, pp. 527 – 532, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865504002272

[12] C. Liu and H. Wechsler, "Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition," *IEEE Transactions on Image Processing*, vol. 11, no. 4, pp. 467–476, April 2002.

[13] C. J. Burges, "A tutorial on support vector machines for pattern recognition," *Data Mining and Knowledge Discovery*, vol. 2, no. 2, pp. 121–167, Jun 1998. [Online]. Available: https://doi.org/10.1023/A:1009715923555

[14] G. G. Hazel, "Multivariate Gaussian MRF for multispectral scene segmentation and anomaly detection," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 38, no. 3, pp. 1199–1211, May 2000.

Author Biography

Karthick Shankar is a undergraduate junior at Purdue University studying Computer Engineering. His focus is primarily in the side of machine learning in image processing applications and has worked on numerous projects related to this. He has also worked with a startup called YourMechanic in Mountain View, CA as a Software Engineering Intern and will be working at Hulu in Seattle, WA for Summer 2019. Besides academics, he is a part of the Student Orientation Committee at Purdue and the Eta Kappa Nu honor society.

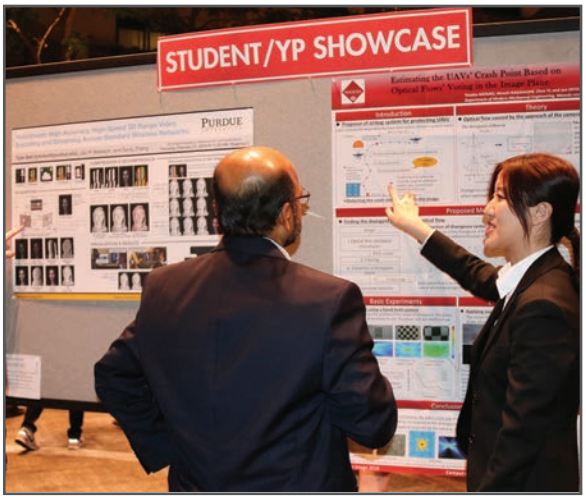
JOIN US AT THE NEXT EI!

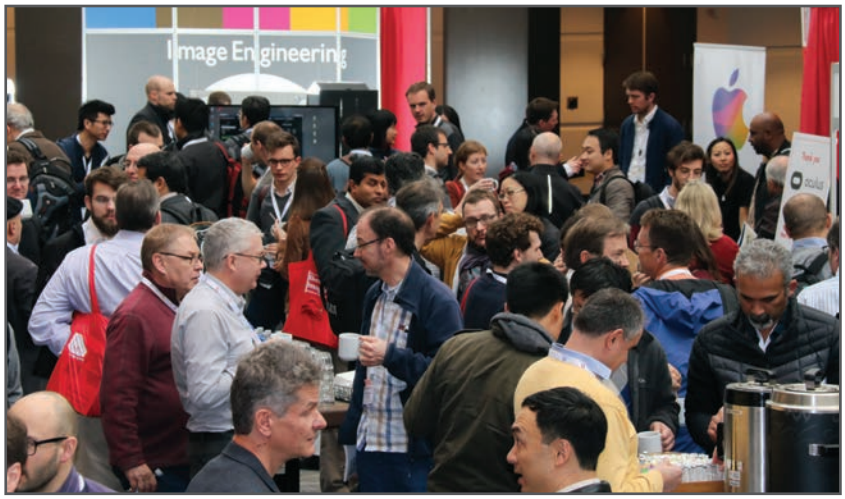
IS&T International Symposium on

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

IS&T
imaging.org