

Machine identification codes of color laser printers: revisiting privacy and security

Shreya Arora¹, Rajendra Kumar Sarin², Pooja Puri¹

¹Amity Institute of Forensic Science, Amity University, Noida, India

²National Forensic Sciences University, Delhi Campus, India

Article Info

Article history:

Received Jan 17, 2025

Revised Apr 22, 2025

Accepted Jul 3, 2025

Keywords:

Greyscale imaging

Laser printers

Machine identification codes

Pattern recognition

Printer identification

Questioned documents

Yellow tracking dots

ABSTRACT

Forging legal documents has been easier and faster with the advancement of technology. Printer identification has become a critical field for tracing criminals and validating the authenticity of documents. The current study uses a non-destructive method to detect and identify covert embedded hidden information (machine identification codes (MIC)). Samples were collected from popular brands, including Xerox and HP color laser printers, to attain this aim. Their printouts were then scanned at 600 dpi using a Konica Minolta scanner. Scanned images were subjected to graphic editors for linear and non-linear adjustments. Following this, yellow-toner dots were observed as a base pattern. Grayscale imaging with a computational approach to analyze the yellow dot patterns was utilized for intensity-focused analysis, with edge detection algorithms applied using Python to enhance and highlight the converted patterns in printed documents. The printouts from Xerox printers exhibited repeating patterns. However, no such detailed information was observed in prints from HP printers, even when analyzed using binary code for deductions. A notable variation was detected in the yellow tracking dots among both brands, which can be instrumental in identifying the origin of printouts and scanned images for forensic investigations. This methodology provides conclusive and dependable accuracy.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Pooja Puri

Amity Institute of Forensic Science, Amity University

Noida, Uttar Pradesh, India

Email: pmalik1@amity.edu

1. INTRODUCTION

From the 1980s, document examiners have been working on various techniques for identifying the source of colored printed questioned documents. Forensic Document examination is a vast area that involves the identification of the source of color laser printers. The demand for improved quality printed materials, including high-quality images, has risen with the improvement in technologies and their widespread adoption worldwide [1]. The validity of printed documents frequently comes into question in various scenarios, with authentication typically linked to the signature's authenticity [2], [3]. The introduction of laser printing technology, including color laser printers and copiers, has even made it easier for unskilled individuals to indulge in high-quality forgeries related to documents [4], [5].

The identification of printed documents is broadly based on extrinsic and intrinsic features of the documents [6]. The extrinsic features are specifically added for security purposes like watermarks, and holograms while the intrinsic feature is added as a by-product of the normal document printing process [6]-[8]. The active techniques for identification include halftone analysis [9], noise analysis [10], toner

identification, and statistical analysis using discrete wavelength transform [11], [12]. These techniques are reliable but not entirely accurate [13].

The design of the machines introduces a specific tracking pattern known as machine identification codes (MIC) or counterfeit protection system (CPS) [14]. These codes are small yellow-colored dots created by the yellow toner, forming an invisible base pattern to the naked eye [8], [15]. These dots are a part of printer steganography, which is unique for the brand, irrespective of the content to be printed [16], [17]. Image processing techniques, including the use of convolutional neural networks (CNNs) [18] as demonstrated [19], offer robust methods for pattern detection [20] and visualization. In addition, greyscale conversion through various algorithms simplifies image data by focusing on intensity values [21], enhancing the identification and analysis of intricate patterns embedded within the visual data [22].

In the present study, ninety-six colored printout samples from Hewlett-Packard Company (HP®) brands and Xerox® were collected. The samples were analyzed using graphic editing software for better visibility of MIC [23]. In an attempt to locate these micro-sized yellow dots, as well as to compare the patterns observed among these brands [24], [25]. Also, a Python code was designed to detect yellow dots in an image, analyze their spatial distribution, and visualize the results with overlays and polynomial fitting [26].

2. METHOD

2.1. Sampling

A4-sized white sheets (75 GSM, JK Copier) were chosen for their widespread availability for use with color laser printers. The study involved a total of 96 samples, equally divided between Xerox and Hewlett-Packard (HP) printers. The Xerox samples consisted of four models: Xerox Docucolor 250, Xerox DC 252, Xerox Color C60, and Xerox Docucolor 242- 252- 260PS. Similarly, the HP samples were collected from four models: HP LaserJet Pro 400 colour M451dn, HP color LaserJet Pro MFP M180n, HP color LaserJet Pro MFP 33035dw, and HP color LaserJet managed MFP E77830. Samples were gathered using a convenience sampling approach from different locations across Delhi-NCR, India.

2.2. Sample collection

The printouts were scanned using a Konica Minolta Bizhub C280 scanner at a resolution of 600 dots per inch (dpi) in “.tif” format. While increasing the resolution could enhance the extraction and visibility of these nano-sized dots, the chosen value was utilized as it was the pre-set default resolution unless manually adjusted by the user.

2.3. Sample preparation

An indirect method was employed to extract samples for visualizing and identifying the yellow dots. Image processing was performed on the digital copies using GNU image manipulation program 2.10.34 (GIMP) as illustrated in Figure 1. The RGB mode was applied with a blue filter to enhance extraction and visibility, as the yellow dots appeared black in this mode, facilitating manipulation from the scanned images, as illustrated in Figures 2 and 3.

To process the scanned file in GIMP 2.10.34, follow these steps:

1. Open GIMP 2.10.34 and click on File, then select Open to display the scanned file.
2. Navigate to Colors and choose the non-linear adjustment option, Brightness and Contrast.
3. Set Brightness to -108 and Contrast to 127 to enhance the visibility of the dots.
4. In the right-hand panel, deactivate the red and green channels in RGB mode to view the results using the blue filter. This adjustment will improve the clarity of the yellow dots.

2.4. Identification of base patterns

The base patterns were identified and analyzed, with the yellow-colored nanodots appearing in black for comparison (Figure 3). To ensure accurate tracking of the security features, the observations were magnified to a zoom level of 200%-400% for enhanced visibility.

2.5. Automated detection of yellow dots using computer vision techniques

This involves employing Python-based computer vision techniques to identify yellow dots in images. The process begins with pre-processing steps to enhance image contrast and reduce noise. The image was then converted into an alternative color space (HSV) to isolate yellow regions based on predefined threshold values. A mask is then generated to detect yellow areas, enabling the extraction of spatial coordinates for further analysis.

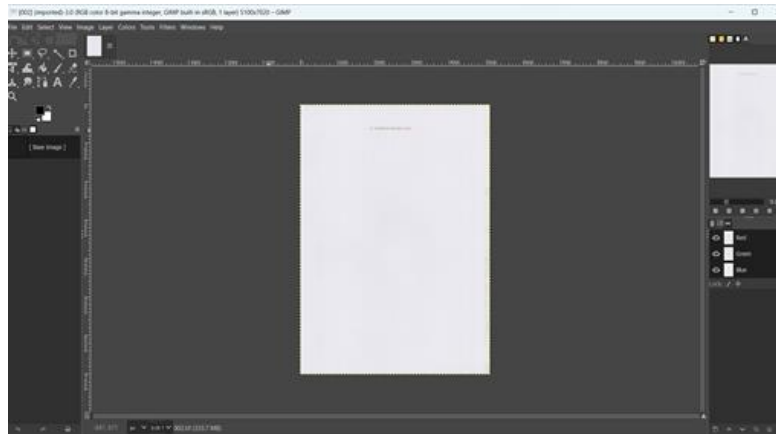


Figure 1. Sample preparation using GNU image manipulation program (GIMP 2.10.34)

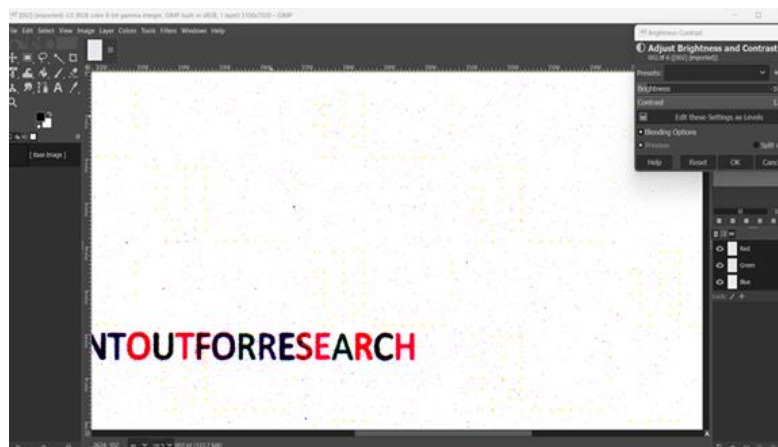


Figure 2. Sample preparation and processing using non-linear adjustments



Figure 3. Sample processing and extraction using blue filter

3. RESULTS AND DISCUSSION

The findings of the present study reveal that yellow tracking dots are embedded in the outputs of both Xerox and HP printers. These dots are distributed in a repetitive pattern, consistent across all 96 samples analyzed, regardless of the content (text or image). This data highlights the need for enhanced visibility techniques, including non-linear parameters and blue-filtering in a graphic editor like GIMP 2.10.34,

for accurate identification and analysis of these micro-patterns. This outcome confirms the hypothesis that yellow dot patterns are systematically embedded across printer brands and models and can be detected using a combination of manual enhancement and automated computer vision techniques. Figure 4 illustrates the yellow dots in a repeating pattern for Xerox printers. Enhanced visibility of the dots was achieved by shifting the mode to a blue filter, rendering the dots black for improved identification and comparison (Figure 5).

This study provides concrete evidence that printer manufacturers embed identifiable patterns for potential document traceability. This reinforces the idea that printed documents can be linked to specific devices, an important aspect for forensic investigations, intellectual property protection, and document authentication. The observation that newer printer models may incorporate modified base patterns challenges the prevailing assumption that legacy patterns persist across generations. This finding highlights the evolving nature of MIC and underscores the need for continuous research in this area. The results align with previous work [8], confirming that MICs can be used for printer identification. However, the findings also reveal deviations from earlier studies, suggesting that manufacturers may be modifying base patterns in newer models, potentially in response to security concerns or advances in printing technology. This underscores the necessity of regularly updating forensic databases and methodologies for printer identification. For instance, the patterns identified in this research differ from those observed in other models of Xerox printers [13] and HP printers [23], suggesting a shift in the base patterns used by manufacturers over time.

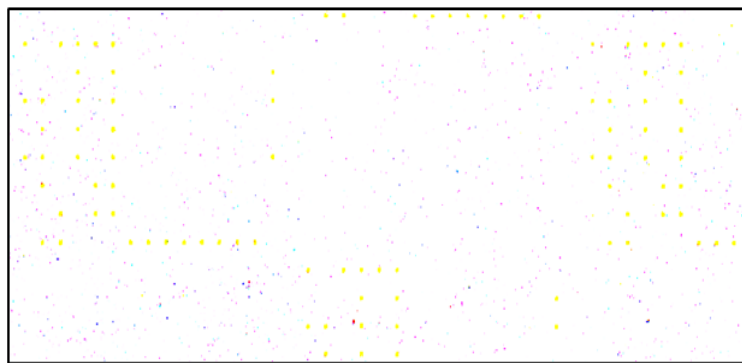


Figure 4. Tracking dots in the Xerox DC 252 sample are arranged in a regular grid pattern, illustrating their repetitive structure

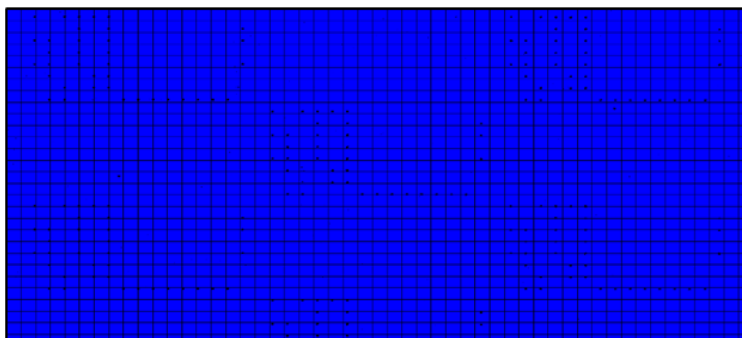


Figure 5. Tracking dots in the Xerox DC 252 sample are arranged in a regular 1 mm×1 mm grid pattern, visualized using an RGB filter

In the case of Xerox printers, the repetitive structure followed a 15×8 grid, where the 2nd and 4th columns in binary format corresponded to time-of-printing metadata. This structured arrangement supports the idea of manufacturer-embedded tracking for document verification (Figure 6). The grid formation observed in these printers allowed for systematic deciphering of the patterns, with specific columns in the binary coding (2nd and 4th) used to extract information related to the time of printing [25]. The parities for each row and column are represented by the first row and column when the data is displayed in a grid. In a geometric progression of 2, the rows are successively numbered as follows: 1, 2, 4, 8, 16, 32, and 64.

The values of the rows containing the dots are then added for each column. For example, the dots in the second column (the first column being the parity) are located in rows 32, 16, 4, and 2, for a total of 54. This process is repeated for all columns. This structured arrangement indicates a deliberate design in Xerox printers to encode metadata for tracking purposes. Subsequent comparison and analysis reveal that the second and fifth columns, respectively, indicate the depiction of time in minutes and hours. For HP printers, while the yellow dots also formed repetitive patterns, their spatial arrangement differed slightly from Xerox, suggesting brand-specific encoding strategies. Among the probable explanations for this variation are differences in firmware design or updated steganographic schemes implemented in newer models over the period of time (Figure 7). Yet, the core concept of embedding tracking dots remains shared across both brands.

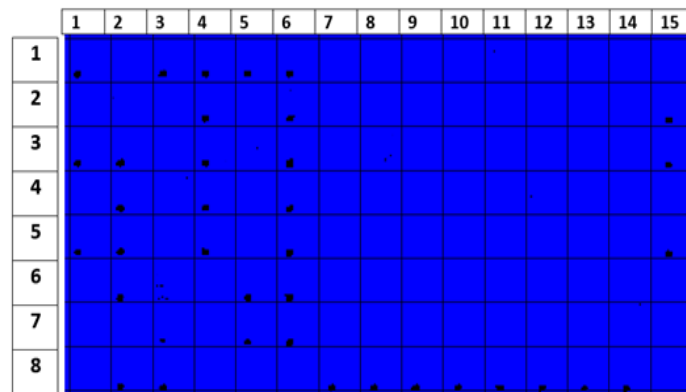


Figure 6. Repetitive patterns in Xerox printers are structured into a 15×8 grid



Figure 7. Tracking dots in the HP LaserJet Pro 400 sample are spaced apart but exhibit a repetitive pattern consistent across all samples

To automate the process, a mask was generated to detect yellow dots, and their contours were analyzed to extract spatial coordinates. The patterns were visualized and further examined using scatter plots and polynomial curve fitting to uncover underlying structures. The approach effectively demonstrated its capability in analyzing micro-patterns. A repetitive pattern was consistently observed in both Xerox and HP printers, as shown in Figure 8 and Figure 9, suggesting a standardized approach in embedding tracking dots among printer manufacturers. Figure 8(a), the yellow mask illustrates the repetitive pattern of yellow dots after preprocessing, displaying the distribution of these dots over a relatively large area. Figure 8(b) provides a magnified view that highlights the structured arrangement of the detected yellow dots, offering a clear representation of the pattern and regularity of the dots at a closer scale. Figure 9(a) displays the yellow mask illustrating the repetitive pattern of yellow dots after preprocessing, while Figure 9(b) is a magnified view highlighting the structured arrangement of these dots, clarifying the pattern and regularity of the detected yellow dots' distribution.

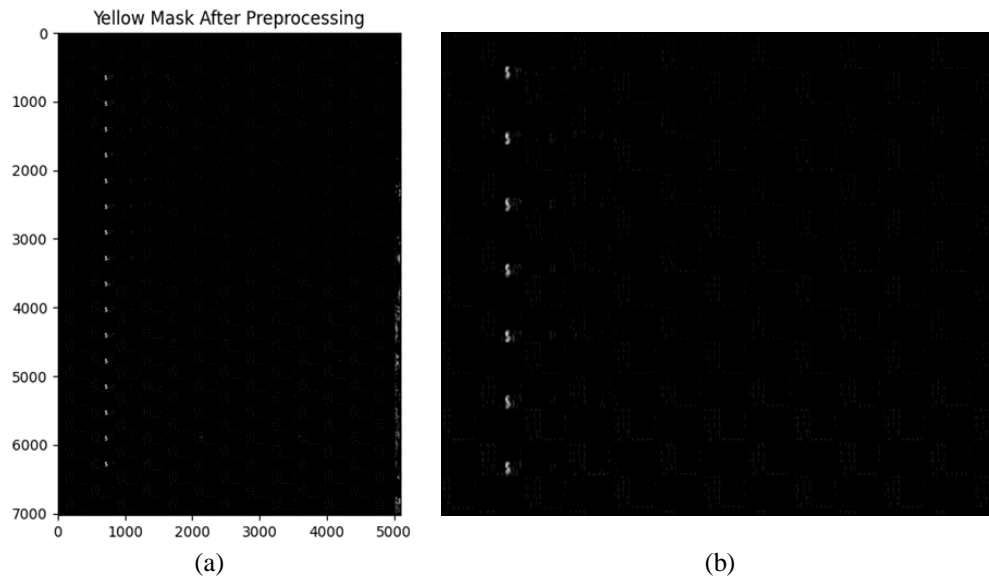


Figure 8. Visualization of yellow tracking dots in Xerox printers: (a) yellow mask showing the repetitive pattern of yellow dots after pre-processing and (b) magnified view highlighting the structured arrangement of the detected yellow dots

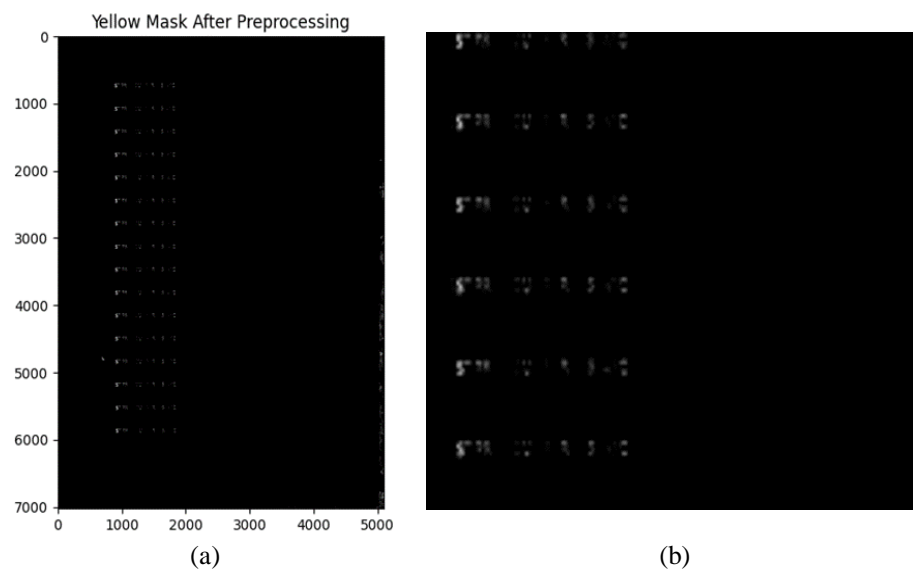


Figure 9. Visualization of yellow tracking dots in HP printers: (a) yellow mask showing the repetitive pattern of yellow dots after pre-processing and (b) magnified view highlighting the structured arrangement of the detected yellow dots

The results support the primary hypothesis that modern color laser printers embed detectable yellow dot patterns. However, some findings contradict earlier assumptions, particularly the expectation that printed content (image vs. text) might influence pattern appearance. Contrary to this assumption, the study demonstrates that content type has minimal to no effect on the base pattern, although it may impact dot visibility. This unexpected result could be attributed to internal printer firmware prioritizing consistent encoding over page content. Alternatively, newer printer models may have been designed to maintain uniformity across all outputs—a deviation from findings in older studies, such as [13] and [23].

A key strength of the study is the reliable detection of embedded patterns using standardized methodologies. The results contribute to the growing body of knowledge on document forensics and provide a foundation for future investigations into printer identification techniques.

However, the use of a single scanning resolution (600 dpi) may limit the visibility of finer patterns, though this choice aligns with standard forensic practice. Additionally, the study's geographic scope was restricted to Delhi-NCR, which may affect generalizability. Finally, the research focused exclusively on Xerox and HP printers; incorporating a broader range of brands in future research will enhance the applicability of our findings.

4. CONCLUSION

The primary aim of this study was to investigate the presence, structure, and consistency of yellow tracking dot patterns in printed outputs from modern Xerox and HP laser printers. The analysis confirmed that both brands embed repetitive and structured yellow dot patterns, which remain consistent across different content types. These findings reinforce the hypothesis that such patterns are intentionally embedded for traceability and are not influenced by the nature of the printed material. This research has demonstrated the effectiveness of combining manual pre-processing using GIMP with automated computer vision techniques in detecting and analyzing steganographic dot patterns.

A distinct base pattern was observed among both brands. Notably, the yellow dots are reproducible both within and across printers of the same brand. The observed variations in patterns were attributed to differences in serial numbers, date, and time. The findings of this study enhance the current understanding of how modern printers implement tracking technologies, contributing to ongoing research in document forensics, counter-forensics, and digital privacy. The results offer new perspectives on the covert nature of printer identifiers and underscore the importance of visibility-enhancing techniques within detection workflows. This research broadens the scope of inquiry by highlighting not only technical detection methods but also the ethical and regulatory implications of hidden tracking features. The study raises important considerations regarding user awareness, consent, and the potential misuse of such technologies.

Future studies are encouraged to expand the sample set to include a broader range of printer brands and models, including those from diverse geographic markets. Investigating the impact of firmware variations on pattern generation may reveal additional nuances in how these identifiers are embedded and maintained. Furthermore, exploring factors such as printing resolution, paper type, and toner composition could help determine environmental influences on pattern visibility.

Additional research may also focus on implementing multi-resolution scanning techniques and developing advanced feature extraction methods using both spatial and frequency-domain analyses. Machine learning models could be trained not only for printer brand classification but also for anomaly detection, aiding in the identification of tampered or counterfeit documents. By framing the issue within a broader socio-technical context, this study lays the groundwork for interdisciplinary research that considers the transparency, accountability, and potential regulation of covert security features in modern printing systems. This work serves as both a methodological contribution and a call to further explore and regulate embedded printer identifiers, striking a critical balance between their utility in forensic analysis and their implications for personal privacy.

FUNDING INFORMATION

The authors state no funding is involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Shreya Arora	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
Rajendra Kumar Sarin		✓	✓	✓		✓		✓		✓	✓	✓		
Pooja Puri	✓		✓	✓			✓	✓	✓	✓	✓	✓	✓	

C : Conceptualization	I : Investigation	Vi : Visualization
M : Methodology	R : Resources	Su : Supervision
So : Software	D : Data Curation	P : Project administration
Va : Validation	O : Writing - Original Draft	Fu : Funding acquisition
Fo : Formal analysis	E : Writing - Review & Editing	

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [PP], upon reasonable request.




REFERENCES

- [1] J. Mace, "COMPUTING printer identification techniques and their privacy implications," *School of Computing Science, Newcastle University, UK*, no. July, 2010.
- [2] 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," *International Conference on Digital Printing Technologies*, pp. 301–305, 2004, doi: 10.2352/issn.2169-4451.2004.20.1.art00068_1.
- [3] I. Amidror, "A new print-based security strategy for the protection of valuable documents and products using more intensity profiles," in *Optical Security and Counterfeit Deterrence Techniques IV*, Apr. 2002, vol. 4677, no. 57, pp. 89–100, doi: 10.1117/12.462738.
- [4] A. K. Mikkilineni, N. Khanna, and E. J. Delp, "Texture based attacks on intrinsic signature based printer identification," *Media Forensics and Security II*, vol. 7541, p. 75410T, 2010, doi: 10.1117/12.845377.
- [5] M. J. Tsai, C. L. Hsu, J. S. Yin, and I. Yuadi, "Digital forensics for printed character source identification," *Proceedings - IEEE International Conference on Multimedia and Expo*, vol. 2016-August, pp. 2347–2350, 2016, doi: 10.1109/ICME.2016.7552892.
- [6] H. Jain, S. Joshi, G. Gupta, and N. Khanna, "Passive classification of source printer using text-line-level geometric distortion signatures from scanned images of printed documents," *Multimedia Tools and Applications*, vol. 79, no. 11–12, pp. 7377–7400, Mar. 2020, doi: 10.1007/s11042-019-08508-x.
- [7] M. U. Devi, "Statistical measures for differentiation of photocopy from print technology forensic perspective," *International Journal of Computer Applications*, vol. 105, no. 15, pp. 1–7, 2014.
- [8] J. van Beusekom, F. Shafait, and T. M. Breuel, "Automatic authentication of color laser print-outs using machine identification codes," *Pattern Analysis and Applications*, vol. 16, no. 4, pp. 663–678, 2013, doi: 10.1007/s10044-012-0287-5.
- [9] D. G. Kim and H. K. Lee, "Color laser printer identification using photographed halftone images," in *European Signal Processing Conference*, 2014, pp. 795–799.
- [10] J. H. Choi, H. K. Lee, H. Y. Lee, and Y. H. Suh, "Color laser printer forensics with noise texture analysis," *MM and Sec'10 - Proceedings of the 2010 ACM SIGMM Multimedia and Security Workshop*, pp. 19–24, 2010, doi: 10.1145/1854229.1854235.
- [11] J. Sauvola and M. Pietikäinen, "Adaptive document image binarization," *Pattern Recognition*, vol. 33, no. 2, pp. 225–236, 2000, doi: 10.1016/S0031-3203(99)00055-2.
- [12] A. K. Mikkilineni, P.-J. Chiang, G. N. Ali, G. T. C. Chiu, J. P. Allebach, and E. J. Delp III, "Printer identification based on graylevel co-occurrence features for security and forensic applications," *Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, no. 0219893, p. 430, 2005, doi: 10.1117/12.593796.
- [13] A. S. Salim and A. A. M. Abdalla, "Application of Adobe® Photoshop® CC 2018 for identifying color laser printer source of Xerox® brand," *Egyptian Journal of Forensic Sciences*, vol. 8, no. 1, 2018, doi: 10.1186/s41935-018-0076-4.
- [14] C. Ma, X. Chen, Q. Zhang, and X. Yang, "Technical note: analyzing the effect of repeated fusing on toner to examine printing alterations made by the same laser printer," *Science and Justice*, vol. 61, no. 4, pp. 435–442, 2021, doi: 10.1016/j.scjus.2021.05.003.
- [15] S. Chen and S. Srihari, "A new off-line signature verification method based on graph matching," in *Proceedings - International Conference on Pattern Recognition*, 2006, vol. 2, pp. 869–872, doi: 10.1109/ICPR.2006.125.
- [16] G. N. Ali, A. K. Mikkilineni, J. P. Allebach, E. J. Delp, P. J. Chiang, and G. T. Chiu, "Intrinsic and extrinsic signatures for information hiding and secure printing with electrophotographic devices," in *International Conference on Digital Printing Technologies*, 2003, pp. 511–515, doi: 10.2352/issn.2169-4451.2003.19.1.art00015_2.
- [17] M. J. Tsai, J. S. Yin, I. Yuadi, and J. Liu, "Digital forensics of printed source identification for Chinese characters," *Multimedia Tools and Applications*, vol. 73, no. 3, pp. 2129–2155, 2014, doi: 10.1007/s11042-013-1642-2.
- [18] N. F. El Abady, H. H. Zayed, and M. Taha, "An efficient source printer identification model using convolution neural network (SPI-CNN)," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 3, pp. 745–753, 2023, doi: 10.14569/IJACSA.2023.0140386.
- [19] K. Sukvichai, P. Uthaisang, P. Chuengsutthiwong, and P. Maolanon, "Hidden Dot Patterns Recognition using CNNs on Raspberry Pi Zero W," *2018 International Conference on Embedded Systems and Intelligent Technology and International Conference on Information and Communication Technology for Embedded Systems, ICESIT-ICICTES 2018*, vol. 20, pp. 1–5, 2018, doi: 10.1109/ICESIT-ICICTES.2018.8442050.
- [20] Z. Guo *et al.*, "Digital forensics of scanned qr code images for printer source identification using bottleneck residual block," *Sensors (Switzerland)*, vol. 20, no. 21, pp. 1–13, 2020, doi: 10.3390/s20216305.
- [21] J. C. Li, B. Li, X. Z. Han, W. Han, and F. Fang, "Study of color laser printer and photocopier class using a pattern location measurement method," *Journal of Forensic Sciences*, vol. 64, no. 2, pp. 475–485, Mar. 2019, doi: 10.1111/1556-4029.13900.
- [22] G. Verhoeven, W. Karel, S. Štuhel, M. Doneus, I. Trinks, and N. Pfeifer, "Mind your grey tones-examining the influence of decolourization methods on interest point extraction and matching for architectural image-based modelling," *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, vol. 40, no. 5W4, pp. 307–314, 2015, doi: 10.5194/isprsarchives-XL-5-W4-307-2015.
- [23] A. S. Salim and A. A. Abdalla, "Application of Adobe® Photoshop® CC 2018 for Identifying the Source of HP® Color Laser Printouts," *Arab Journal of Forensic Sciences and Forensic Medicine*, vol. 1, no. 9, pp. 1158–1164, 2019, doi: 10.26735/16586794.2019.002.
- [24] N. F. E. Abady, M. Taha, and H. H. Zayed, "Text-independent algorithm for source printer identification based on ensemble learning," *Computers, Materials and Continua*, vol. 73, no. 1, pp. 1417–1436, 2022, doi: 10.32604/cmc.2022.028044.




- [25] J. S. Tweedy, "Class characteristics of counterfeit protection system codes of color laser copiers," *Journal of the American Society of Questioned Document Examiners*, vol. 4, no. 2, pp. 53–66, 2001, doi: 10.69525/jasqde.62.
- [26] A. Singh, N. Jindal, and K. Singh, "A review on digital image forensics," in *International Conference on Signal Processing (ICSP 2016)*, 2018, pp. 12 (6 .)-12 (6 .), doi: 10.1049/cp.2016.1451.

BIOGRAPHIES OF AUTHORS






Shreya Arora    is a research scholar at the Amity Institute of Forensic Science, Amity University, Noida, Uttar Pradesh, India. She holds a Bachelor's degree in Life Sciences from Delhi University and a master's degree in Forensic Science from LNJN-NICFS (now NFSU, Delhi). Currently pursuing her Ph.D. at Amity University, Noida, Shreya has nearly five years of experience in teaching and research in Forensic Science and has supervised multiple M.Sc. students in their research projects. Her research interests include forensic documentation and machine learning. She can be contacted at email: arorashreya1996@gmail.com.



Dr. Rajendra Kumar Sarin    is a professor at the National Forensic Science University, Delhi, is a distinguished forensic expert with extensive academic, research, and administrative experience. He holds a Ph.D. in Chemistry with a specialization in Coordination Compounds and has contributed significantly to forensic science through his leadership roles, research publications, and as a mentor to numerous scholars. His expertise spans forensic chemistry, toxicology, laboratory accreditation, and advanced analytical techniques, earning him accolades, including the Union Home Minister's Award and the Lifetime Achievement Award. Dr. Sarin's impactful career exemplifies dedication to advancing forensic science in India and globally. He can be contacted at email: sarinrk2000@yahoo.com



Dr. Pooja Puri    serves as an assistant professor (Senior Grade) at Amity University, India, bringing over 16 years of teaching experience to her role. She has guided more than 100 undergraduate and postgraduate research projects and successfully supervised four Ph.D. scholars. Dr. Puri boasts a robust academic and research background, having co-authored several book chapters and research papers. She is an active member of prestigious national and international forensic organizations, including the Indian Science Congress, the Indo-Pacific Academy of Forensic Odontology, and IAMLE. Her expertise and dedication have established her as a respected figure in the forensic science community, both in India and internationally. She can be contacted at email: pmalik1@amity.edu.