Jurnal Sisfotek Global
ISSN (Online): 2721 - 3161, ISSN (Print): 2088 – 1762
DOI: http://dx.doi.org/10.38101/sisfotek.v15i2.15998
Vol. 15, No. 2, September 2025, pp. 57-63

# EXIF Metadata Feature Extraction to Improve Source Device Identification Accuracy in Digital Images within a Digital Forensics Approach

**Muhammad Naufal Bahreisy[1], Adi Rizky Pratama[2], Gugy Guztaman Munzi[3] & Yusuf Eka Wicaksana[4]**

[1,2,3,4] Universitas Buana Perjuangan Karawang, Karawang, Indonesia, 41361
E-mail: [1]muhammad.bahreisy@ubpkarawang.ac.id, [2]adi.rizky@ubpkarawang.ac.id, [3]gugy.guztaman@ubpkarawang.ac.id, [4]yusuf.eka@ubpkarawang.ac.id

## ARTICLE HISTORY

*Received : August 22, 2025*
*Revised : September 11, 2025*
*Accepted : September 27, 2025*

## KEYWORDS

*Digital Forensics*
*Convolutional Neural Network*
*PRNU*
*Image Forensics*
*EXIF Metadata*

## ABSTRACT

This study aims to develop and evaluate methods for digital image source device identification through three main approaches, namely EXIF metadata feature extraction, visual analysis using Convolutional Neural Networks (CNN), and Photo Response Non-Uniformity (PRNU). The dataset consists of 500 original images captured from five different devices, with 100 images per device containing intact metadata. The EXIF-only model was built using the Random Forest algorithm, the CNN model employed a ResNet18 architecture, while PRNU utilized high-pass filtering to construct sensor noise templates for each device. Evaluation was carried out using accuracy, precision, recall, and f1-score metrics. The results show that EXIF-only achieved perfect accuracy (100%) on the dataset with complete metadata, CNN reached 21% accuracy with imbalanced recall across classes, and PRNU demonstrated low performance due to the limited number of templates and image quality. These findings indicate that EXIF-only excels under intact metadata conditions but is vulnerable to manipulation, CNN can be applied when metadata is unavailable but requires optimization, while PRNU has potential resilience against metadata manipulation but demands higher-quality data. The novelty of this study lies in its comparative multi-method approach that integrates metadata-based, visual-based, and sensor fingerprint-based analyses, along with the proposal of a multimodal integration framework to enhance the reliability of device identification systems in digital forensic practice.

## 1. Introduction

The extraction of Exchangeable Image File Format (EXIF) metadata is an essential step in identifying the source device of digital images in digital forensics, with methods evolving from traditional techniques based on metadata analysis software and camera fingerprints [1] to procedures that strengthen the validity of evidence in court [2]. Advances in machine learning and deep learning have enabled the combination of pseudonoise residuals and noiseprints to improve identification accuracy [3]. while automated and semi-automated systems accelerate the extraction process [4], [5]. Statistical analyses such as Photo-Response Non-Uniformity (PRNU) and the use of convolutional neural networks further enhance source device authentication [6], [7].

In reality, the integration of Exchangeable Image File Format (EXIF) metadata feature extraction with advanced forensic identification algorithms is still rarely implemented optimally. Although the combination of metadata with machine learning and deep learning has shown potential for improving accuracy [8], [9]. the challenge of metadata manipulation that reduces the reliability of authentication has not yet been fully addressed [6], [10]. There is no standardized approach capable of maintaining high performance when metadata is incomplete or has been altered, thereby necessitating more robust and adaptive methods [2], [11].

Conventional digital forensic techniques that utilize Exchangeable Image File Format (EXIF) metadata have the advantage of leveraging standardized metadata structures, such as brand information, camera model, and image capture parameters, as well as source device recognition through stable Photo-Response Non-Uniformity (PRNU) patterns [1], [3]. However, the effectiveness of this method is limited by the potential manipulation or deletion of metadata, which can reduce the reliability of image authentication [12]. The complexity of imaging technology also hinders the generalization of noise patterns across devices [6], along with the challenges faced by passive techniques

when dealing with advanced editing or cross-platform migration that modifies EXIF data [13].

In reality, digital forensic methods are still not effective in handling Exchangeable Image File Format (EXIF) metadata that is incomplete, manipulated, or inconsistent. Integrative approaches that combine metadata with intrinsic image features have indeed shown potential [10], [14], but conventional algorithms remain vulnerable to manipulation [15] and there is no established standard to ensure the reliability of results when metadata is compromised [16], [17].

The utilization of Exchangeable Image File Format (EXIF) metadata has been proven to improve the accuracy of digital image source device identification through the integration of traditional techniques and deep learning. Methods such as CNN-based Noiseprint are capable of combining metadata with intrinsic image features for more reliable authentication [1], while the combination of Photo-Response Non-Uniformity (PRNU) with machine learning enhances resilience against manipulation [3], [12]. Although effective, the challenge of metadata manipulation has encouraged the use of image noise patterns as a safer alternative [6].

In reality, empirical evidence regarding the improvement of device identification accuracy when combining Exchangeable Image File Format (EXIF) metadata with other forensic features on real-world datasets is still rarely reported comprehensively. Although holistic approaches that integrate metadata analysis, Error Level Analysis (ELA), and deep learning algorithms have been proven to enhance the accuracy of manipulation detection and source identification [18], and CNN-based systems combined with similarity networks have shown performance improvements on real-world datasets [8], most studies have not yet tested the effectiveness of these methods under diverse and uncontrolled forensic conditions. There is no established evaluation standard to consistently assess the synergy between metadata and intrinsic image features, leaving a wide open opportunity for the optimization of such integrative methods in digital forensic practice [16], [17].

This study aims to develop and evaluate methods for digital image source device identification through three main approaches, namely EXIF metadata feature extraction, visual analysis using Convolutional Neural Networks (CNN), and Photo Response Non-Uniformity (PRNU). The novelty of this research lies in its comparative multi-method approach that simultaneously examines three device identification pathways (EXIF-only, CNN, and PRNU) on a multi-device image dataset with complete metadata, something that is rarely conducted in an integrated manner within digital forensic studies.

## 2. Research methods

### 2.1 Research Design

This study employs a quantitative experimental approach with a comparative evaluation design to examine the effectiveness of Exchangeable Image File Format (EXIF) metadata feature extraction in improving the accuracy of digital image source device identification within a forensic context. The proposed method is validated by comparing its performance against existing device identification techniques, namely Photo Response Non-Uniformity (PRNU) and CNN (Convolutional Neural Network)-based visual feature extraction, with reference to best practices outlined in previous studies [1], [3], [12], [19]. The research flow is presented in Figure 1.

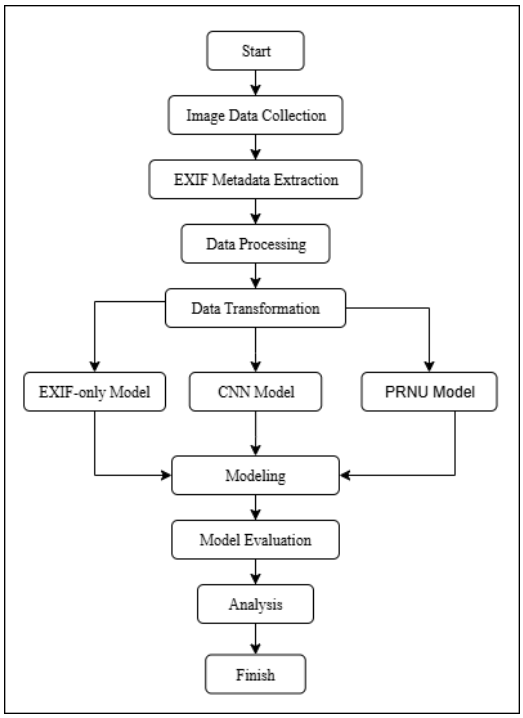


Figure 1. Research flow diagram

The figure illustrates the research methodology flow carried out systematically to examine the identification of digital image source devices. The study begins with the data collection stage, where images are obtained from five different devices used as the dataset source. Subsequently, EXIF metadata extraction is performed using ExifTool to obtain technical information related to the images, such as Model, Make, ISO, ExposureTime, and other parameters. At the data processing stage, the extracted metadata is examined for its validity and completeness to ensure that no corrupted or manipulated data is included.

The next stage is data transformation, in which the dataset is divided into three modeling pathways: the EXIF-only model, the CNN model, and the PRNU model. The EXIF-only model converts metadata into numerical and categorical representations through encoding and normalization processes. The CNN model utilizes raw images that have been normalized and converted into tensors for training using the

ResNet18 architecture. Meanwhile, the PRNU model constructs sensor fingerprint templates from image residual noise obtained through high-pass filtering.

These three pathways then proceed to the modeling stage, where each model is trained and tested according to its respective approach. Subsequently, model evaluation is conducted using accuracy, precision, recall, and f1-score metrics, along with further analyses. The evaluation results are then comprehensively analyzed in the analysis stage by comparing the strengths and limitations of each method. The study concludes with the conclusion stage, which presents the interpretation of findings and their implications within the context of digital forensics.

### 2.2 Data Dataset and Data Collection

The dataset consists of original JPEG images captured from five devices: OnePlus_8T, Poco_F5_Pro_5G, Samsung_Galaxy_S20FE, iPhone_11, and iPhone_15. Each device contributed 100 images with complete EXIF metadata. For PRNU testing, 15 images per device were used as reference templates, while the remaining images were employed as test data.

### 2.3 Data Preprocessing and Transformation

The validated EXIF data were converted into numerical format through feature encoding for attributes such as ISO, ExposureTime, FNumber, and FocalLength, while categorical attributes such as Make, Model, and Software were processed using one-hot encoding. All features were then normalized to ensure a uniform scale.

For the CNN approach, the images were pixel-normalized, converted into tensors, and split into 80% training data and 20% validation data.

In the PRNU approach, images were EXIF-transposed to preserve their original orientation, resized and center-cropped to 256×256 pixels, and then subjected to high-pass filtering to extract sensor residual noise. These PRNU features, or alternatively Noiseprint [1], can be integrated with EXIF features to form a richer combined representation, which is expected to improve the accuracy and robustness of device identification in the context of digital forensics.

### 2.4 Modeling

Modeling in this study was carried out through three main approaches that can be integrated to build a more robust source device identification system. First, the EXIF-only approach employed the Random Forest algorithm to classify devices based on metadata that had undergone feature encoding and normalization. Second, the image-based CNN approach utilized the ResNet18 architecture trained from scratch on raw images to recognize differences in visual patterns produced by the imaging process of each device. Third, the Photo Response Non-Uniformity (PRNU) approach constructed sensor noise fingerprint templates for each device by applying high-pass filtering and computing correlation scores against test images. These approaches can further be developed into a multimodal architecture that combines raw image inputs and EXIF metadata within a CNN-based model, as proposed by Wang et al. (2021)[7], which demonstrated that multi-source data integration can improve the accuracy and robustness of device identification systems in complex environments.

### 2.5 Model Evaluation

Evaluation was conducted using the k-fold cross-validation technique to test the consistency of model performance across different data subsets, with the main metrics including accuracy, precision, recall, and f1-score, as commonly applied in digital forensic studies based on machine learning [12]. Additional analyses included generating Receiver Operating Characteristic (ROC) curves per class (one-vs-rest) for the EXIF-only and CNN models, as well as boxplots of PRNU correlation score distributions per device to observe the spread and overlap of sensor fingerprint patterns across device classes.

## 3. Results and Discussion

### 3.1 EXIF- only performance

The results of the EXIF-only model demonstrate perfect performance in classifying the source devices of digital images. The EXIF-only model achieved maximum accuracy across all metrics (precision, recall, f1-score = 1.00). This perfect performance is consistent with the findings on the Receiver Operating Characteristic (ROC) curves per class, where all ROC lines are located at the ideal point with a True Positive Rate (TPR) = 1.0 and a False Positive Rate (FPR) approaching 0 for all classes. The Area Under the Curve (AUC) values, which reached 1.00 for all devices, indicate maximum discriminative capability between positive and negative classes. The ROC results of the EXIF-only model are shown in Figure 2.

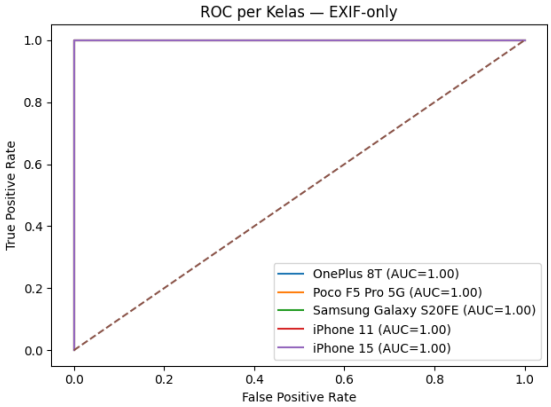


Figure 2. EXIF-only Model ROC visualization

Figure 2 presents the Receiver Operating Characteristic (ROC) curves per class for the EXIF-only model in classifying five types of devices, namely OnePlus 8T, Poco F5 Pro 5G, Samsung Galaxy S20FE, iPhone 11, and iPhone 15. It can be observed that all ROC curves for each class follow the ideal path at the top-left corner of the graph, indicating a True Positive Rate (TPR) of 1.0 with a False Positive Rate (FPR) close to 0. The Area Under the Curve (AUC) values for all classes are 1.00, which indicates perfect performance in distinguishing each device. These results confirm that the EXIF metadata features used, particularly attributes such as Model and Software, possess very high discriminative power on datasets that are intact and not manipulated. Nevertheless, this perfect performance should be critically reviewed in a forensic context, as the heavy reliance on metadata makes this model vulnerable to metadata manipulation when EXIF attributes are deliberately deleted or altered.

## 3.2 Performance of CNN Methods

The CNN model achieved an accuracy of 21% with an average precision of 0.58 but a low recall of 0.24. There was a noticeable imbalance in detection across classes—for instance, iPhone_15 achieved a recall of 0.94, whereas iPhone_11 recorded a recall of 0.00. The learning curves indicated signs of overfitting, likely due to the limited dataset size, the absence of pretraining, and the minimal application of data augmentation.

These findings are consistent with the class-wise Receiver Operating Characteristic (ROC) results shown in Figure 3. The ROC results for the CNN model are presented in Figure 3.

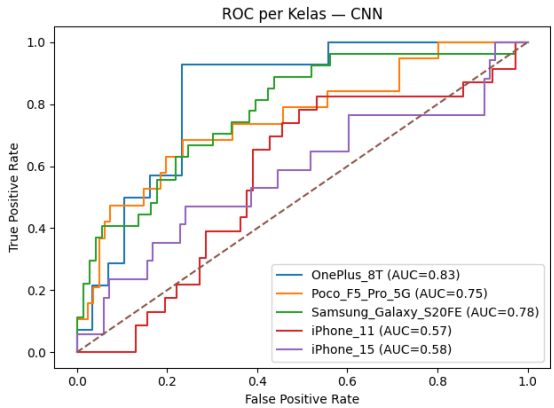


Figure 3. CNN Model ROC visualization

Based on Figure 3, the Area Under the Curve (AUC) values varied considerably across classes, with the highest being OnePlus_8T (AUC = 0.83) and the lowest being iPhone_11 (AUC = 0.57) and iPhone_15 (AUC = 0.58). This variation in AUC values indicates that the model's discriminative ability in distinguishing positive and negative classes was not consistent across all devices. Classes with AUC values above 0.75 (OnePlus_8T, Samsung_Galaxy_S20FE) tended to demonstrate more stable classification performance, whereas classes with AUC values approaching 0.5 exhibited performance nearly equivalent to random prediction. This reinforces the indication that the CNN architecture used was not yet able to capture sufficiently representative visual features for all devices, particularly in classes with similar visual characteristics or varying image quality.

## 3.3 Performance of the PRNU Method

To evaluate the performance of the Photo Response Non-Uniformity (PRNU) method, an analysis of the distribution of correlation scores across devices was carried out using a boxplot representation. This analysis aims to observe the spread of residual noise correlation values generated by each device, as well as to identify potential overlaps between classes. Accordingly, the PRNU score boxplot per device provides an initial overview of the stability of sensor fingerprints and the level of discrimination between devices. The visualization results are presented in Figure 4.

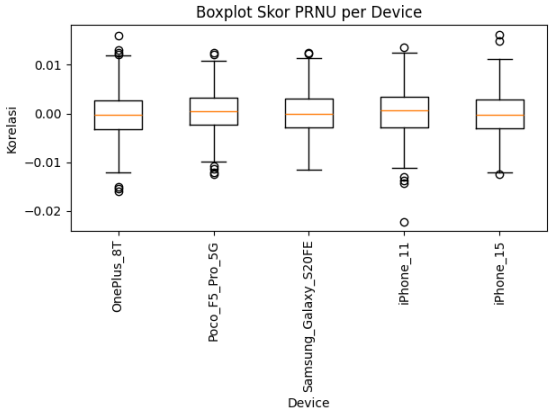


Figure 4. PRNU score visualization

Based on the testing results using the Photo Response Non-Uniformity (PRNU) method as shown in Figure 4, the per-device correlations indicate that the distribution of correlation values lies within a relatively narrow range, approximately −0.01 to 0.01. This range suggests that the extracted sensor noise signal has low strength, thereby limiting PRNU's discriminative capability in distinguishing devices. Furthermore, an overlap in the distributions across devices can be observed, which means that the residual sensor noise patterns between cameras cannot be clearly differentiated. This directly impacts the high rate of misidentification, where images from one device may potentially be misclassified as belonging to another device.

The occurrence of numerous outliers across almost all devices, particularly on the OnePlus 8T and iPhone 15, indicates instability in the construction of PRNU templates. This factor is most likely caused by the limited number of images used to build the templates (only 15 images per device), resulting in sensor noise

signals that are not sufficiently strong and consistent. In addition, the use of compressed image formats (JPEG) further weakens the PRNU patterns, as compression and post-processing can obscure or degrade the sensor noise signals that should be distinctive.

Thus, although PRNU is theoretically known as a robust method for identifying source devices because it is based on the physical fingerprint of the sensor, the experimental results indicate that its effectiveness is highly dependent on the quality and quantity of the data used. Under conditions of limited datasets and highly compressed images, PRNU performance cannot achieve optimal results. This underscores the necessity of increasing the number of template images per device, using high-quality images (with minimal compression), and applying more advanced noise extraction techniques in order for PRNU to function effectively in the context of digital forensics.

### 3.4 Method Performance Comparison

The radar chart illustrates that EXIF-only outperforms in all metrics, CNN shows moderate precision but low recall and f1-score, while PRNU lags behind in all metrics. In the forensic context, these comparative results are presented in Figure 5.

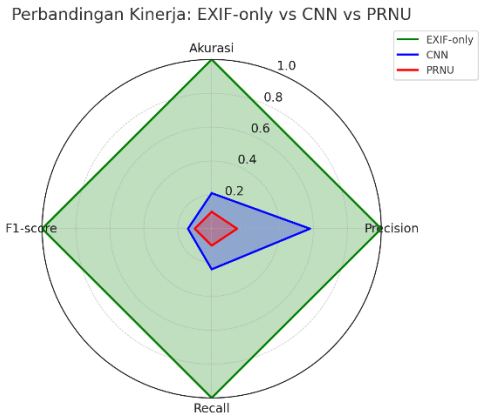


Figure 5. Comparison visualization of EXIF-Only vs CNN vs PRNU

The radar chart illustrates the relative performance of the three methods across four main metrics—accuracy, precision, recall, and f1-score—using a normalized scale of 0–1.

The EXIF-only method occupies the maximum area across all four metrics (value of 1.00 on every axis), indicating perfect performance on the test dataset. This condition is consistent with the results from the previous tables and bar charts, which showed that metadata-based identification in this dataset leveraged explicit attributes such as *Model* and *Software*, making class separation straightforward. Nevertheless, this ideal performance is highly dependent on the integrity of the metadata, meaning its robustness against manipulation cannot be guaranteed.

The CNN method occupies a much smaller area, with relatively better precision (0.58) compared to recall (0.24) and f1-score (0.14), and an overall low accuracy (0.21). This pattern illustrates that the model tends to make correct predictions when it assigns a class but fails to capture many positive examples that should have been correctly classified. This is consistent with the phenomenon of overfitting and the limitations of the training data that were previously identified.

The PRNU method occupies the smallest area in the diagram, with estimated values around 0.10–0.15 across all metrics. This profile reflects the low correlation scores obtained during testing, caused by the limited number of templates per device and the effects of image post-processing. The low and uniform distribution across all metrics demonstrates that, under the current testing configuration, this method is not yet capable of providing effective class separation.

Visually, the distinct radar shapes reflect the unique strengths and weaknesses of each method: EXIF-only excels but is forensically fragile, CNN has potential for adaptation based on visual content but requires enhanced data and architecture, while PRNU theoretically offers strong sensor-based validation but requires technical optimization to achieve significant performance. Integrating all three methods in a multimodal manner has the potential to produce a more balanced radar shape with broader coverage across all metrics, thereby strengthening the reliability of device identification in the context of digital forensics.

## 4. Conclusions and Suggestions

Based on the experimental results, it can be concluded that each method has its own strengths and limitations in the context of digital image source device identification. The EXIF-only approach demonstrated very high accuracy under conditions of intact metadata, but its performance is highly fragile when the metadata is manipulated or removed. The visual content-based CNN has the potential to serve as an alternative when metadata is unavailable, but it requires a larger dataset, pretraining, and data augmentation to achieve optimal performance. PRNU is theoretically resistant to metadata manipulation because it relies on the unique patterns of camera sensors; however, under the current experimental configuration, its performance was low due to the limited number of template images and data quality issues. Considering these characteristics, a multimodal approach that integrates EXIF, CNN, and PRNU is regarded as the most promising solution to produce a more robust and reliable device identification system in real-world digital forensic scenarios.

Based on the findings of this study, several development and improvement steps can be undertaken to enhance the effectiveness of the methods:

1. For EXIF-only: Develop metadata manipulation detection mechanisms, such as

cross-attribute consistency checks and anomaly pattern detection, so that the system does not rely solely on explicit information that is vulnerable to alteration.

2. For CNN: Apply transfer learning using pretrained models and employ diverse data augmentation techniques to improve generalization capability, particularly in distinguishing devices with similar visual patterns.
3. For PRNU: Increase the number and quality of template images per device and utilize uncompressed or minimally compressed images to minimize the degradation of sensor noise patterns.
4. For Integration: Implement decision-level fusion that combines the outputs of EXIF, CNN, and PRNU, accompanied by consistency checks between metadata and visual content, to strengthen the reliability of the system when dealing with various data conditions in digital forensic practice.

## References


[1] D. Cozzolino and L. Verdoliva, "Noiseprint: A CNN-Based Camera Model Fingerprint," *Ieee Trans. Inf. Forensics Secur.*, vol. 15, pp. 144–159, 2020, doi: 10.1109/tifs.2019.2916364.

[2] Z. Balkibayeva, "Methods of Extracting and Analyzing Metadata for Evidentiary Purposes," *Uzb. J. Law Digi. Policy*, vol. 2, no. 5, pp. 31–44, 2024, doi: 10.59022/ujldp.233.

[3] D. Cozzolino, F. Marra, D. Gragnaniello, G. Poggi, and L. Verdoliva, "Combining PRNU and Noiseprint for Robust and Efficient Device Source Identification," *Eurasip J. Inf. Secur.*, vol. 2020, no. 1, 2020, doi: 10.1186/s13635-020-0101-7.

[4] F. A. Musyaffa, K. Rapp, and H. Gohlke, "LISTER: Semiautomatic Metadata Extraction From Annotated Experiment Documentation in eLabFTW," *J. Chem. Inf. Model.*, vol. 63, no. 20, pp. 6224–6238, 2023, doi: 10.1021/acs.jcim.3c00744.

[5] M. Manisha, C. Li, and A. K. Karunakar, "Source Camera Identification With a Robust Device Fingerprint: Evolution From Image-Based to Video-Based Approaches," *Sensors*, vol. 23, no. 17, p. 7385, 2023, doi: 10.3390/s23177385.

[6] J. Zeng and X. Qiu, "Forensic Taken Time Authentication of Mobile Phone Photos," p. 17, 2024, doi: 10.1117/12.3048368.

[7] Y. Wang, Q. Sun, D. Rong, S. Li, and L. D. Xu, "Image Source Identification Using Convolutional Neural Networks in IoT Environment," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, 2021, doi: 10.1155/2021/5804665.

[8] O. Mayer and M. C. Stamm, "Forensic Similarity for Digital Images," *Ieee Trans. Inf. Forensics Secur.*, vol. 15, pp. 1331–1346, 2020, doi: 10.1109/tifs.2019.2924552.

[9] M. Iuliani, M. Fontani, and A. Piva, "A Leak in PRNU Based Source Identification—Questioning Fingerprint Uniqueness," *Ieee Access*, vol. 9, pp. 52455–52463, 2021, doi: 10.1109/access.2021.3070478.

[10] M. Manisha, C. Li, X. Lin, and A. K. Karunakar, "Beyond PRNU: Learning Robust Device-Specific Fingerprint for Source Camera Identification," *Sensors*, vol. 22, no. 20, p. 7871, 2022, doi: 10.3390/s22207871.

[11] T. Zhao, X. Xu, M. Xu, H. Ding, Y. Xiong, and W. Xia, "Learning Self-Consistency for Deepfake Detection," pp. 15003–15013, 2021, doi: 10.1109/iccv48922.2021.01475.

[12] I. C. Camacho and K. Wang, "A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics," *J. Imaging*, vol. 7, no. 4, p. 69, 2021, doi: 10.3390/jimaging7040069.

[13] X. Lin and C. Li, "PRNU-Based Content Forgery Localization Augmented With Image Segmentation," *Ieee Access*, vol. 8, pp. 222645–222659, 2020, doi: 10.1109/access.2020.3042780.

[14] C. Zeng, D. Zhu, Z. Wang, Z. Wang, N. Zhao, and L. He, "An End-to-End Deep Source Recording Device Identification System for Web Media Forensics," *Int. J. Web Inf. Syst.*, vol. 16, no. 4, pp. 413–425, 2020, doi: 10.1108/ijwis-06-2020-0038.

[15] Y. Liu, Z. Zou, Y. Yang, N.-F. Law, and A. A. Bharath, "Efficient Source Camera Identification With Diversity-Enhanced Patch Selection and Deep Residual Prediction," *Sensors*, vol. 21, no. 14, p. 4701, 2021, doi: 10.3390/s21144701.

[16] A. Stolbova, A. Malyshev, and O. Golovnin, "Two-Step Intelligent Approach for Photo Image Fragment Forgery Detection and Identification," p. 10, 2023, doi: 10.1117/12.2669232.

[17] S. Agrawal, P. Kumar, S. Seth, T. Parag, M. Singh, and V. Babu, "SISL:Self-Supervised Image Signature Learning for Splicing Detection and Localization," 2022, doi: 10.48550/arxiv.2203.07824.

[18] K. A. Nfor, T. P. T. Armand, and H. Kim, "A

Holistic Approach to Image Forensics: Integrating Image Metadata Analysis and ELA With CNN and MLP for Image Forgery.," 2024, doi: 10.21203/rs.3.rs-4667372/v1.

[19] S. Ferreira, M. Antunes, and M. E. Correia, "A Dataset of Photos and Videos for Digital Forensics Analysis Using Machine Learning Processing," *Data*, vol. 6, no. 8, p. 87, 2021, doi: 10.3390/data6080087.