Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

A Content Independent Digital Image Forensics Framework for PRNU-Based Image Forgery Detection and Localization

Imran Maqsood*
Department of Computer Software Engineering, University of Engineering & Technology, Mardan, Pakistan, 23200 Email: imranmaqsood@uetmardan.edu.pk

Mareena Karim
Department of Telecommunication Engineering, University of Engineering & Technology, Mardan, Pakistan, 23200

Mazhar Ali
Department of Telecommunication Engineering, University of Engineering & Technology, Mardan, Pakistan, 23200

Uzair Shahzad
Department of Telecommunication Engineering, University of Engineering & Technology, Mardan, Pakistan, 23200

Kainat Bibi
Department of Telecommunication Engineering, University of Engineering & Technology, Mardan, Pakistan, 23200

ABSTRACT

The rapid proliferation of advanced image editing software has made digital image forgery increasingly prevalent, posing significant threats to the integrity of digital images used as evidence in forensic investigations, legal proceedings, journalism, and social media. This paper proposes a passive copy-move forgery detection technique, which relies on camera fingerprints called Photo Response Non-Uniformity (PRNU), without being dependent on the image content. A camera fingerprint is caused by manufacturing variations and other imperfections in the camera sensor, and is specific to each camera and will be present in every image taken by the camera. The method proposed in this paper is based on the fact that in the input image, the spatial domain averaged frames are extracted from the camera fingerprint and the Normalized Cross-Correlation (NCC) is calculated to determine if the image is tampered or not. Two practical situations are considered: (1) given both the original and forged images, and (2) given only the candidate image (which was captured from the same source camera) and the forged image. To localize the forgery, fingerprint subtraction, morphological dilation and thresholding is done to accurately identify the tampered area. Experiments are done on a set of 500 images where the proposed technique has been proved to be 100% successful in Scenario 1 and 97% successful in Scenario 2 when tested with several state of art CBIR techniques. The results prove the reliability and efficiency of

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

the camera fingerprint based approach in the passive image forensics.

Keywords: Image Forgery Detection; Camera Fingerprints; PRNU; Copy-Move Forgery; NCC; Passive Forensics; Forgery Localization; Digital Image Authentication

Introduction

Digital images are used as a source of information and as supportive evidence in forensic investigations, court cases, news reporting, insurance claims and social media today. Today, with the exploding drop in the price of digital cameras and smart phones, and the high resolution of modern sensors, digital photography is now ubiquitous. In parallel with these advances, powerful and user-friendly image editing tools such as Adobe Photoshop, GIMP, and Corel PaintShop Pro have made it simple for even non-technical users to manipulate images with minimal effort or expertise.

Although these technologies are valuable for creative and professional uses, they are being increasingly abused to produce fake images for malicious purposes such as misinformation, defaming prominent personalities, falsifying evidence and making false insurance claims. Pearson and Amsberry estimate that about 10% of all colour photographs published in the USA have been modified or retouched. [1,2]. This common manipulation has greatly cast doubt on the reliability of digital images as evidence. Forgery detection of images is a crucial area of research to ensure the authenticity and integrity of digital images, therefore. The methods for forgery detection can be generally divided into two categories: Active and Passive [3,4]. An active approach involves the embedding of watermark or digital signature at the moment of image capture, and necessitates the use of specialized hardware or software. Passive or blind methods, on the other hand, involve no knowledge of the image to be detected, and are based on the detection of statistical anomalies or intrinsic properties of the image resulting from the imaging process.

Passive methods are commonly divided into several categories, including copy-move forgery detection, image splicing detection, retouching detection, and resampling detection. Among these, copy-move forgery where a region of an image is duplicated and placed elsewhere within the same image is the most commonly used method. It is also particularly challenging to identify due to the high level of visual consistency between the copied and original regions. [5,6]. Most of the existing passive approaches are content-based, whose performance relies on the visual contents of the image. This reduces their usefulness in the real-world situations of a forensics investigation where content can differ markedly. In contrast, this paper introduces a so-called content-independent forgery detection method using camera fingerprints, namely the Photo Response Non-Uniformity (PRNU) noise that is intrinsic to digital camera sensors [7]. The camera fingerprint is a result of very small manufacturing defects in the camera sensor and is unique to each camera, thus providing a very reliable forensic tool for source identification and forgery detection.

The proposed technique will remove the camera fingerprint from the input image by using PRNU and Normalized Cross-Correlation (NCC) will be utilized to check the possibility of tampering. Two realistic forensic scenarios are considered: (1) the

Online ISSN 3007-3197
Print ISSN 3007-3189

original and forged image are the two images are available and (2) only a candidate image captured by the same source camera and the forged image are available. Moreover, a forgery localization pipeline is suggested, through fingerprint subtraction, thresholding and morphological dilation, to localize tampered regions. The main contributions of this paper are as follows:

(i) A passive, content-independent copy-move forgery detection technique using PRNU camera fingerprints.

(ii) Implementation and evaluation across two practical forensic scenarios with different levels of available reference information.

(iii) A localization pipeline to identify and highlight forged regions in tampered images.

(iv) Comprehensive comparison with state-of-the-art methods demonstrating superior or competitive performance.

The rest of the paper is structured as follows: Section 2 presents a review of existing research on image forgery detection, while Section 3 explains the proposed approach, including PRNU extraction, NCC calculation, and the process of identifying forged regions.Section 4 presents the experimental setup and results. Section 5 compares the proposed technique with existing methods. Section 6 concludes the paper and outlines future research directions.

Related Work

The problem of detecting forged digital images has been a subject of great interest for the last 20 years. The literature is divided into two categories: content based techniques (copy-move, splicing and resampling), and camera device based techniques (PRNU and GAN fingerprints). The most relevant work is reviewed in this section.

Camera Fingerprint and PRNU-Based Methods

To estimate the PRNU, a technique was proposed by Taspinar et al., which involved computing a geometric mean of still images and refers to it as Spatial Domain Averaged (SDA) frames. Then the extracted fingerprint is correlated with the PRNU of the test image to decide whether it is the source camera or it is a forged image. This approach does not depend on the image content and has been proved to be feasible in various camera models [8].

Khan and Bianchi proposed the Reduced Complexity Image Clustering (RCIC) algorithm, which is able to cluster images with the camera fingerprint without the knowledge of the source camera or the number of cameras involved. NCC is calculated between the reference fingerprint and all other fingerprints and forgery detection is done by using a probability based threshold. The algorithm can be further compressed, and a compressed version called Fast Image Clustering based on Compressed Camera Fingerprints was presented which further improved the computational efficiency [9].

Lin and Li put forward a PRNU-based forgery localization technique which constructs a sliding window over the image and calculates NCC for each pixel in the window. Forged areas are marked as regions where the PRNU does not exist. They also explored the possibility of using CNN-based correlation predictors to improve the performance of PRNU-based localization, and achieved higher performance on multi-scale datasets [10,11].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Copy-Move Forgery Detection Methods

To address this, Meena and Tyagi proposed a copy-move forgery detection technique based on Tetrolet transform that captures the geometric pattern in all direction as compared to Discrete Wavelet Transform (DWT) that captures the geometric pattern in two directions. The method is based on the division of image into overlapped 4 x 4 blocks, calculation of low and high pass coefficient, and the identification of forged region by comparing the similarity of the blocks [12].

Parveen and Khan suggested a block matching technique for detecting copy-move forgery in an image, in which the image is converted into the grayscale mode and then it is divided into overlapping blocks of size 8x8 and DCT coefficients are extracted from these blocks. The centroid groups are found by using k-means clustering and forged regions are detected by comparing the feature vectors [13].

Gani and Qadir proposed a hybrid method which comprises of DCT and Cellular Automata (CA) for copy-move forgery detection. Each block is represented with a five dimensional feature vector computed through DCT and CA inversion which makes it robust to be detected even in compressed images [14].

Deep Learning and CNN-Based Approaches

Chen et al. presented BusterNet which is comprised of two CNN modules: Simi-Det to detect similarity and Mani-Det to detect manipulation at the pixel level. The model has high detection and localization accuracy for the copy-move forgery, but requires high computational cost [15].

Yao and Xu introduced an algorithm to detect and localize forgery by utilizing a reliability fusion map, which is based on camera fingerprint discrimination among different camera models using CNN. The fixed high pass filter generates residual image patches which are fed into a CNN with content-texture module to identify tampered regions [16].

Chen and Zhao studied generative attacks on camera model identification using deep learning methods and showed that they could generate perturbations to fool CNN classifiers without being perceptible to the human eye. This underscores the need for strong forensic methods other than content analysis [17].

Image Splicing Detection

The image splicing detection using augmented Markov model in Block Discrete Cosine Transform (BDCT) and Discrete Meyer Wavelet Transform (DMWT) domain was proposed. Both domain feature vectors were combined and fed into an SVM classifier, which resulted in classification accuracy of more than 88% on the Columbia dataset [18].

Block-Based and Transform Domain Methods

For image splicing forgery detection and localization, Bi et al. proposed a framework called Reality Transform Adversarial Generator (RTAG). The approach is based on the idea of adversarial training to make the forgery detectors more generalizable to the various types of forgery. RTAG has been able to learn discriminative features in the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

transform domain, which resulted in better localization accuracy on different benchmark datasets, showcasing the usefulness of adversarial learning for forensic image analysis tasks [24].

Doan & Retraint presented a new statistical signal-dependent model for tamper detection of compressed JPEG images. They use a statistical model of the distribution of JPEG pixels in the discrete cosine transform (DCT) encoding and decoding pipeline. There are three factors at the pixel level for identifying fabricated regions and likelihood estimation is applied for detecting modifications. It was shown to be very sensitive to the very light manipulation added during JPEG re-compression, and it is therefore very useful in detecting forgeries in images that have been compressed multiple times [25].

In 2006, Gardella et al. put forth a multi-scale noise estimation method for the detection of forgery in JPEG-compressed images. The image is segmented in macro-blocks and global noise curves are created for each color channel. Each macro-blocks noise function is compared to the global noise curves and heat maps per channel are generated. Geometric mean of all the channel heat maps results in a single forgery map. This method is particularly useful in detecting the inconsistencies caused by JPEG compression artifacts and has been shown to work well on a variety of datasets [26].

Medical Image Forgery Detection and Specialized Applications

In the medical field, copy-move forgery detection is even more crucial since copy-move forgery of medical images can result in misdiagnosis and cause serious harm to patients. Suganya et al. presented a copy-move forgery detection method for medical images, which is based on Smooth Muscle Growth Medium (SMGM) approach and Minimum Eigenvalue Algorithm (MEVA) for keypoint extraction. MEVA can detect keypoint at both uniform and non-uniform region, which leads to more accurate detection in medical image textures, unlike SURF-based approach which detects keypoint only at non-uniform region. The feature matrices are obtained using SVD with 4×4 neighborhood and the Euclidean distance measure and thresholding are used for final decision making. Random Sample Consensus (RANSAC) is used to further refine falsely matched regions.

The technique was tested on 300 medical images and outperformed other keypoint-based methods [27]. Arun Anoop and Poonkuntran proposed Local Patterns of Gray Level (LPG) algorithm for medical image forgery detection, which is based on block-based approach and tested on breast cancer images. Noise removal is done by a Wiener filter and then Local Binary Pattern (LBP) features and Gray Level Co-Variance Matrix (GLCM) features are extracted to constitute a hybrid feature. The Extreme Learning Machine (ELM) is used as a classifier for further processing of features. A post-processing step is added to generate all odd/even/random feature pair combinations and AWGN and GB attacks are applied. Any pair of features that are not present indicate the image has been manipulated. The method showed better performance than previously proposed ones and emphasized on the need for strong forgery detection in healthcare image systems [28].

The review of existing literature indicates that most of content based approaches require both original and forged images to be present and are dependent on content

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

changes of images. In addition, there are specialized applications, such as medical imaging and JPEG compressed forensics, which need to be dealt with a specialized solution addressing domain-specific problems. In this paper, we propose to solve the aforementioned drawbacks by focusing on PRNU based camera fingerprints, which are content independent, and can be used in a more general and robust way in a wide range of forensic scenarios in real world.

Proposed Methodology

Just like the unique signature of marks made by the barrel of a gun on a bullet, every camera sensor has a unique and stable pattern of "noise" on each image it captures. This is a noise pattern referred to as Photo Response Non-Uniformity (PRNU), which is caused by an imperfection of the CCD or CMOS sensor which is inherent in the manufacture of the camera CCD or CMOS sensor. As described in 7, 19 and 20 PRNU is an ideal forensic feature for the detection of forgery since it is stable throughout the lifetime of the camera, is unique to each camera and does not rely on the image content.

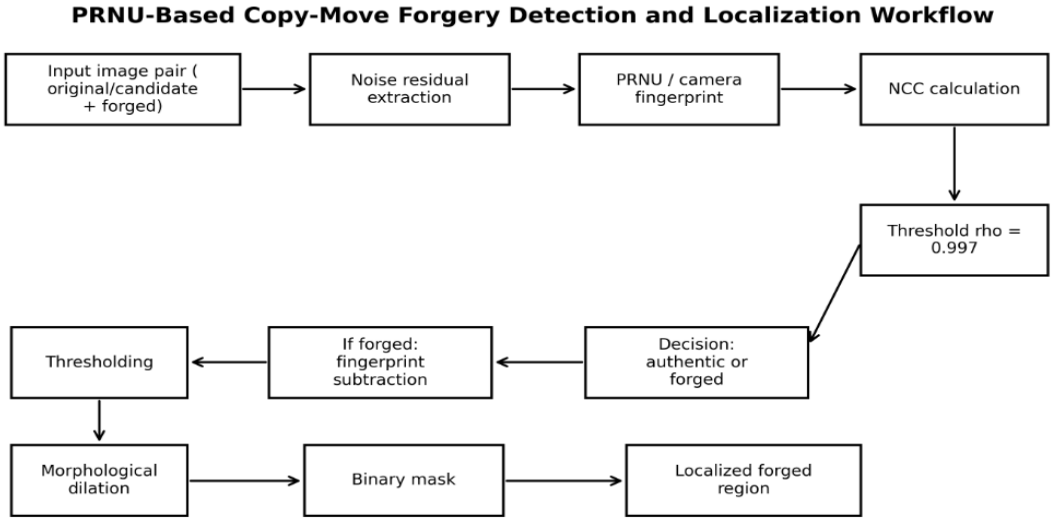

Figure 1. Proposed PRNU-based workflow for image forgery detection and localization.

Photo Response Non-Uniformity (PRNU)

PRNU is the dominant component of sensor pattern noise. It results from inhomogeneity in silicon wafers, imperfections during CCD/CMOS manufacturing, and pixel-to-pixel sensitivity variations. PRNU is a high-level multiplicative noise that remains consistent and camera-specific across all images captured by a given device.

The sensor noise n in an image is modeled as:

$$n = I - F \quad (1)$$

where I is the original captured image and F is the denoised version of the image obtained by applying a noise suppression filter.

The camera fingerprint (CF), which serves as the PRNU estimate, is extracted using the Spatial Domain Averaged (SDA) approach. For a set of images captured by the same camera, the average of their noise residuals is computed to obtain a reliable fingerprint estimate, suppressing high-level scene content and other distractors.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Normalized Cross-Correlation (NCC)

Once camera fingerprints are extracted from two images, the NCC is computed to measure the degree of similarity between the two fingerprints. The NCC is defined as:

$$NCC = \Sigma\, Rn[y] \cdot In[y] \;/\; Ps \qquad (2)$$

where Rn[y] is the reference fingerprint, In[y] is the test image fingerprint, and Ps is the total number of pixels. The NCC value ranges from 0 to 1. Ideally, if NCC equals 1, the two images are considered to have originated from the same source without any modification. In practice, a threshold of $\rho = 0.997$ is applied: if $NCC \geq 0.997$, the image is considered authentic; if $NCC < 0.997$, the image is flagged as forged or manipulated. The threshold is calculated using the formula:

$$Th = \sigma\rho \times \sqrt{(2\, erfc^{-1}(2 \times PFA))} \qquad (3)$$

where σρ is the standard deviation of the NCC and PFA is the desired probability of false alarm.

Scenario 1: Original and Forged Images Available

In the first case the original image is present, in the second case the forged image is present. The algorithm works as follows: PRNU fingerprinting is extracted from both original and forged images using camera. Then, NCC of both the fingerprint images is computed. If the value NCC is below 0.997, the image is classified as forged and if it is more than 0.997, it is considered as the original image. This scenario is the simplest forensic scenario and is likely to give the highest detection accuracy.

Scenario 2: Candidate Image and Forged Image Available

In real life forensic scenarios, the original image may not exist. For Scenario 2, the forged image and a candidate image are the only images provided. Any image made by the same camera as the original forged image is the candidate image. To get a good fingerprint estimate, the candidate image needs to be captured under same lighting condition and should not be saturated and also not too dark.

Fingerprint of both candidate and forged images is extracted using camera. Normalization of both the fingerprints and calculation of NCC. The threshold is fixed at the same value ($\rho = 0.997$) to determine whether the image is real or not. This situation also has some more uncertainty because of the different reference image used, but has more practical applications in real forensic investigations such as in figure 2.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

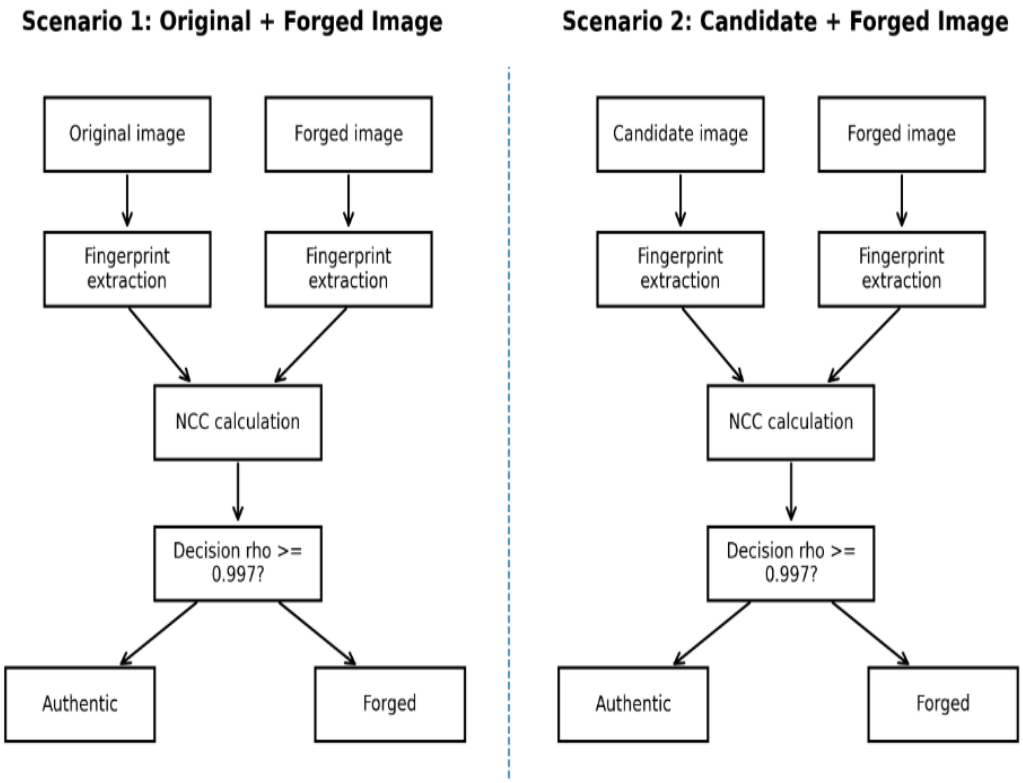

Figure 2. Scenario-wise PRNU comparison workflows for forgery detection.

Forgery Localization

After the classification of the image as a forged one, the forged region is localized by following the following steps as shown in figure 3.

Step1: **Fingerprint Subtraction:** The difference between the two camera fingerprints (original/candidate and forged) is calculated. When a region is forged, they create inconsistencies in the fingerprint which can be identified by subtraction.

Step 2: **Thresholding:** They threshold the difference image with a value of 200. If the pixel value is above 200, it is coded as 1 (forged region) and if it is below 200, it is coded as 0 (background). This helps to make less noise around the detected forged boundaries especially in the case that a forger smoothest the edges of the forged area.

Step 3: **Morphological Dilation:** Binary result is dilated to enlarge and join the forged areas to achieve better morphological quality and spatial consistency of localization output.

Step 4: **Masking:** The binary mask is then applied to the forged image. The forged regions are white, the original background is dark, and the final output is localized as desired.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

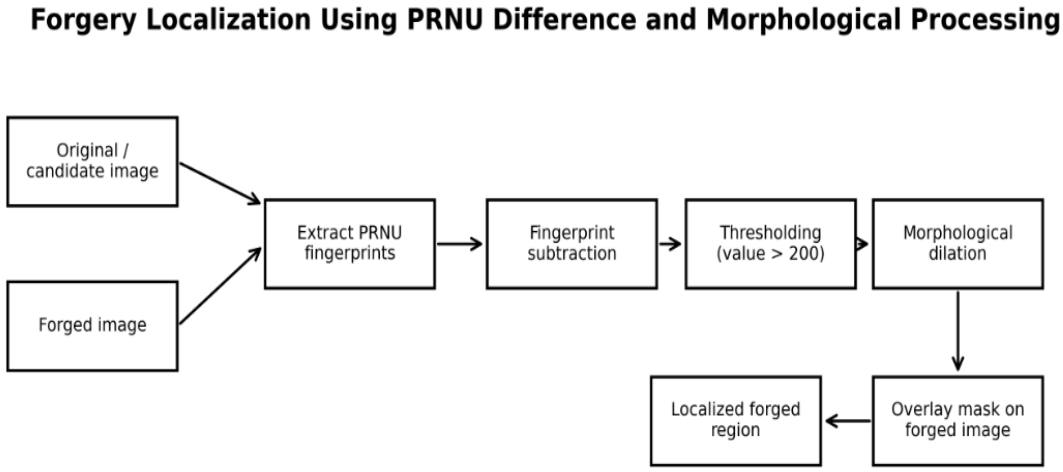

Figure 3. Localization pipeline used to highlight the tampered copy-move region.

Experimental Setup and Results

Dataset

500 original images were retrieved from publicly available image repositories to create a custom dataset. To create copy-move forgery images for the case of Scenario 1, copy-move forgery method was applied to each of the 500 images by simple copying and pasting parts of the same image using common image editing software and 500 such images were obtained. The original images used in the dataset were 500 and 500 forged images were used, making a total of 1000 images. The 500 images captured by source cameras under uniform lighting conditions were used as reference images instead of the original images for scenario 2.

All experiments have been carried out in MATLAB. Each of the images was then subjected to PRNU estimation using the SDA technique and then the NCC between a pair of PRNU fingerprints was calculated to classify whether the image is authentic or forged.

Evaluation Metrics

The performance of the proposed method is evaluated using standard binary classification metrics:

$$True\ Positive\ Rate\ (TPR) = TP / (TP + FN) \quad (4)$$

$$False\ Positive\ Rate\ (FPR) = FP / (TN + FP) \quad (5)$$

$$Precision\ (P) = TP / (TP + FP) \quad (6)$$

$$Recall\ (R) = TP / (TP + FN) \quad (7)$$

$$F\text{-}Measure = 2(P \times R) / (P + R) \quad (8)$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Results of Scenario 1

For Scenario 1, both original and forged images were fed to the algorithm. The original and forged images were captured with the camera and NCC values of these images were computed with the camera fingerprints in both cases. The NCC value for the forged image pair was equal to 0.9893, which is lower than the threshold value of 0.997, thus it was classified as forged. The original image and its unmodified copy had an NCC of 1, thus correctly classified as authentic.

The algorithm was tested on all 500 pairs in the dataset and it was found that the algorithm classifies all images perfectly. The performance metrics are detailed in the following Tables 1 and 2.

Table 1. Classification rates for Scenario 1.

Parameter	Result
True Positive Rate	1.00
False Positive Rate	0.00
True Negative Rate	1.00
False Negative Rate	0.00

Table 2. Performance metrics for Scenario 1.

Parameter	Result
Accuracy	1.00
Precision	1.00
Recall	1.00
F-Measure	1.00

The 100% accuracy in Scenario 1 confirms that when both the original and forged images are available, the PRNU-based camera fingerprint method provides a flawless forgery detection capability, with zero false positives and zero false negatives across all 500 test pairs.

Results of Scenario 2

The original image was swapped with a candidate image which was taken using the same camera in Scenario 2. 500 test pairs of images were used for extracting the camera fingerprints and calculating the NCC. Of the 500 tests performed, 480 images were correctly classified as forged (true positive) and 20 images as authentic (false negative). In a set of 500 genuine pairs, 490 pairs were correctly identified as genuine (true negatives) and 10 as falsely identified as forged (false positives). Table 3, Table 4 and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

figure 4 show the performance measurement for the Scenario 2.

Table 3. Classification rates for Scenario 2.

Parameter	Result
True Positive Rate	0.96
False Positive Rate	0.02
True Negative Rate	0.98
False Negative Rate	0.04

Table 4. Performance metrics for Scenario 2.

Parameter	Result
Accuracy	0.97
Precision	0.9796
Recall	0.96
F-Measure	0.9697

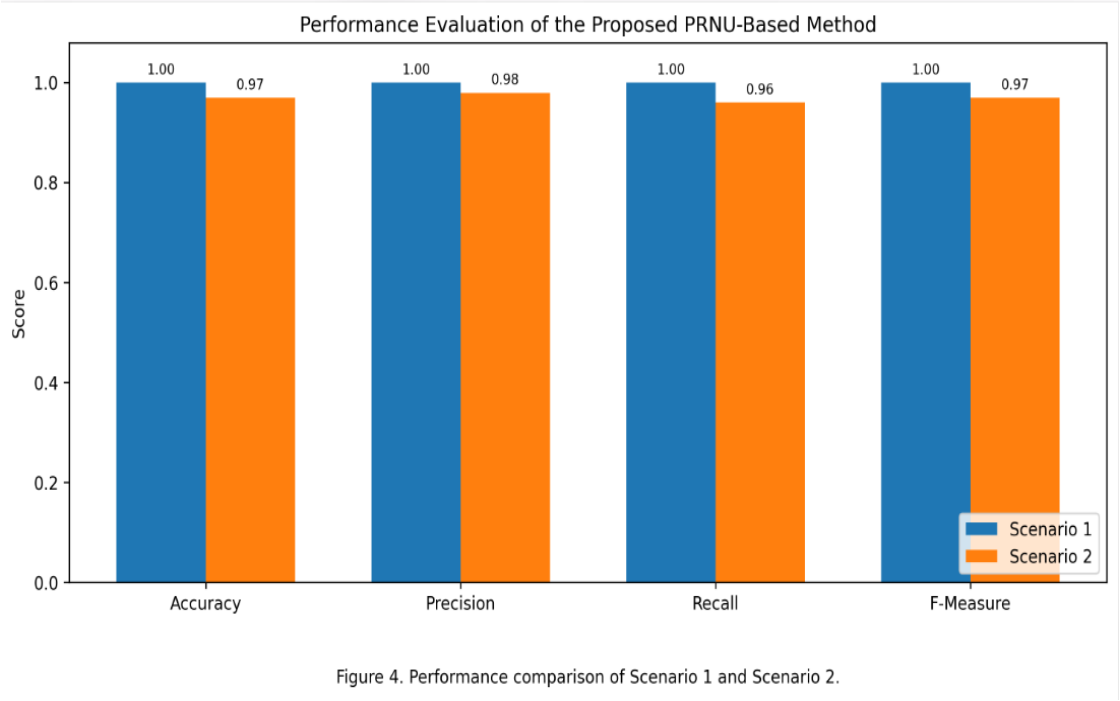

Figure 4. Performance comparison of Scenario 1 and Scenario 2.

Scenario 2 achieves an overall accuracy of 97%, with precision of 0.9796 and F-Measure of 0.9697. The slight reduction in performance compared to Scenario 1 is

Online ISSN 3007-3197
Print ISSN 3007-3189

expected, as the candidate image is not the original reference but a substitute captured under potentially slightly different conditions. Nonetheless, the results demonstrate that the proposed method maintains high reliability even when the original image is unavailable.

Forgery Localization Results

The localization pipeline was used for the images that were classified as forged. Camera fingerprints of the original/candidate images were subtracted and thresholding followed by morphological dilation was performed. This binary mask was then superimposed on the fabricated image to emphasize the manipulated area.

During the localization experiment, the NCC of a forged image was detected to be 0.9839, which is correct and then activated the localization pipeline. The difference of the camera fingerprints revealed the tampered region as a bright spot on a dark background. Following these steps of dilation and masking, the precisely forged region was successfully isolated, which proved that the proposed technique can not only detect copy-move forgery but also precisely localize the forged region.

The localization results on the different image sets evaluated showed the successful localization of forged regions both when the images contained scenes of varying complexity and when the size of the copied regions was varied.

Comparison with State-of-the-Art Methods

The performance of the proposed technique is compared with some of the most recent copy-move forgery detection techniques, in terms of accuracy and precision. The accuracy comparison is shown in the Table 5 and figure 5.

Table 5. Accuracy comparison with state-of-the-art methods.

Technique / Method	Max Accuracy (%)
CNN	99.02
Efficient DCT	98.60
DCT	98.05
SVD	98.90
PCA	97.78
BusterNet	93.01
DYWT	98.73
Improved DCT	98.56
PCA-DCT	98.96
Proposed Scenario 1 (Original + Forged)	100.00
Proposed Scenario 2 (Candidate + Forged)	97.00

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

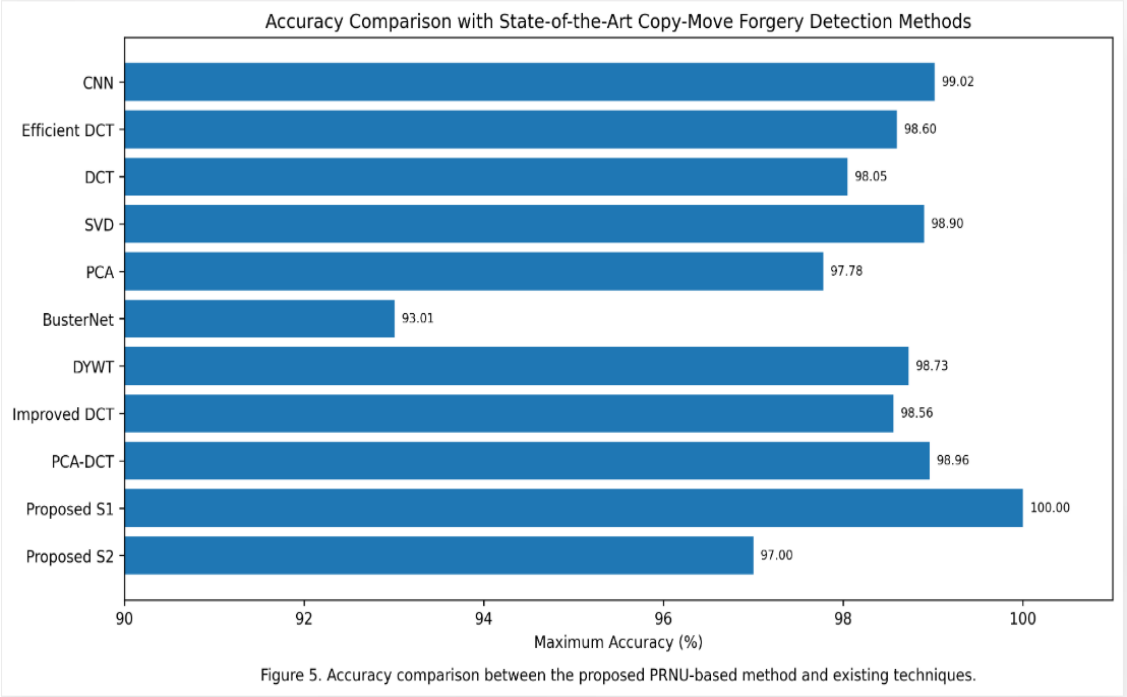

Figure 5. Accuracy comparison between the proposed PRNU-based method and existing techniques.

Table 5 and figure 6 shows that the proposed technique in Scenario 1 achieves the highest accuracy of 100% among all compared methods, outperforming even CNN-based approaches. In Scenario 2, the technique achieves 97% accuracy, competitive with PCA (97.78%) and outperforming BusterNet (93.01%) while remaining content-independent a distinct advantage in practical forensic applications.
Table 6 presents the precision and F-Measure comparison for selected methods.

Table 6. Precision and F-Measure comparison.

Method	Precision	F-Measure
Deep Learning Approach [21]	0.9537	0.9674
SURF and BRISK [22]	0.9402	
Mirror-SIFT [23]		0.894
Combined Features [23]	0.8183	0.8782
SURF [23]	0.9320	0.9020
Proposed Scenario 2	0.9796	0.9697

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

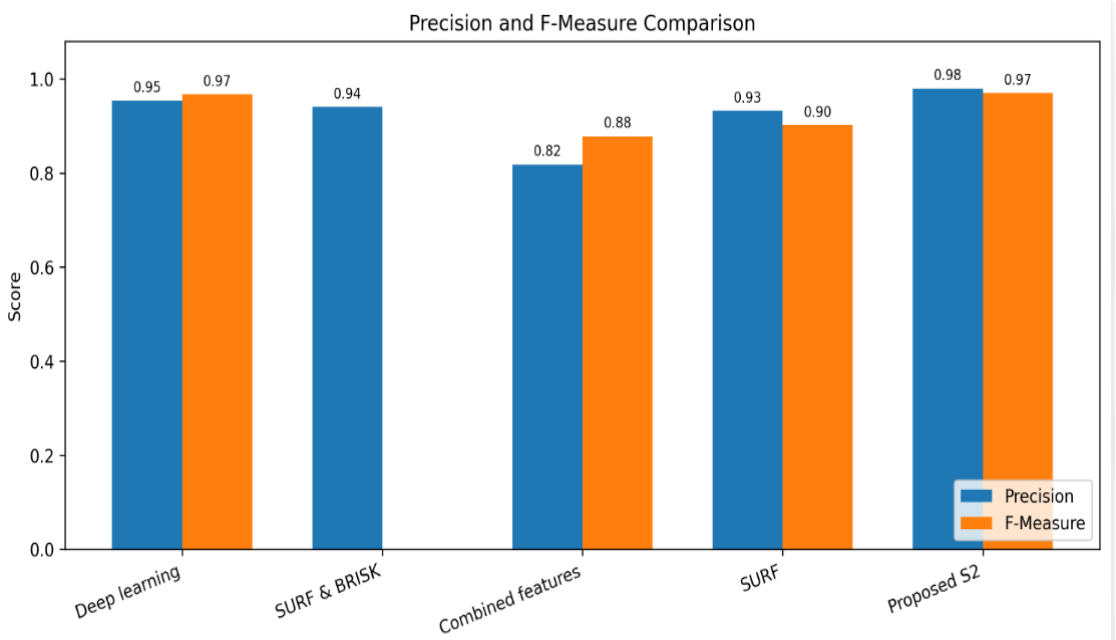

Figure 6. Precision and F-measure comparison of the proposed method against selected approaches.

The proposed technique shows a precision of 0.9796, which is higher than all compared techniques such as deep learning approach (0.9537) and SURF based approach (0.9402) in Scenario 2. This validates the PRNU-based camera fingerprinting method for its improved accuracy and demonstrates that it is independent of image content, which means it can be applied to a variety of real-world forensic applications.

Another merit of the proposed method is that it is independent of the original image in Scenario 2, which is different from the image content-based methods. Most of the content-based approaches are inherently constrained by the need of both original and forged images, which results in their low practicality. The proposed method (only a candidate image in Scenario 2) ensures comparable performance and significantly increases the spectrum of cases it can be applied to in forensic practice.

Conclusion

In this paper, the authors proposed a passive PRNU camera fingerprint based image forgery detection and localization technique. Unlike content-based methods, the proposed one uses the unique and stable patterns in the image noise generated by the source camera image sensor, and it does not consider the content of the images; it is useful for various forensic scenarios.

In the case of two practical scenarios, the results are as follows; for the scenario 1 with both original and forged images 100% accuracy, precision, recall and F-Measure is achieved on the data set of 500 image pairs. In the case of only having a candidate image from the same source camera, scenario 2 had the highest accuracy of 97 percent and precision of 0.9796 among several state-of-the-art methods. Forgery localization pipeline (fingerprint subtraction, thresholding and morphological dilation) was used to detect and mark tampered regions in forged images.

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

The experimental results prove that the proposed PRNU based method is reliable, efficient, and having very low complexity which is suited for real time deployment in forensic investigation tools in security agencies including FIA, police etc.
For the future, the proposed technique will be extended from image to video forgery detection. Given that a video is a collection of many image frames, the camera fingerprint method can be suitably modified for temporal analysis of video frames to help detect copy-move tampering in video evidence. Additional investigation will also be conducted to investigate the method's robustness against adversarial attack and JPEG re-compression.
Declaration

Author Contributions
Mareena Karim and Mazhar Ali, Uzair Shahzad and Kainat Bibi contributed to the concept and methodology of the paper, original draft preparation, data curation, formal analysis and validation, while Imran Maqsood contributed to investigation, resources, visualization and review and editing. All authors reviewed and approved the final version of the manuscript.

Data Availability
All relevant data and supporting material used in this study are in the manuscript.

Conflict of Interest
The authors declare that the research presented in this study was conducted independently and was not affected by any known financial conflicts of interest or personal relationships.

Ethics Approval
The study was conducted following standard ethical guidelines. Approval was obtained from the relevant institutional review board, and all participants provided informed consent.

References
[1] Pearson, H. Image manipulation: CSI: cell biology. Nature 2005, 434, 952–953.
[2] Amsberry, C. Alterations of photos raise host of legal, ethical issues. Wall Street J. 1989, 1, 26–89.
[3] Qureshi, M.A.; Deriche, M. A bibliography of pixel-based blind image forgery detection techniques. Signal Process. Image Commun. 2015, 39, 46–74.
[4] Asghar, K.; Habib, Z.; Hussain, M. Copy-move and splicing image forgery detection and localization techniques: a review. Aust. J. Forensic Sci. 2017, 49, 281–307.
[5] Mahmood, T.; Nawaz, T.; Ashraf, R.; Shah, M.; Khan, Z.; Irtaza, A.; Mehmood, Z. A survey on block based copy move image forgery detection techniques. In Proceedings of the 2015 International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 19–20 December 2015; pp. 1–6.
[6] Manu, V.T.; Mehtre, B.M. Detection of copy-move forgery in images using

Online ISSN 3007-3197
Print ISSN 3007-3189

segmentation and SURF. In Advances in Signal Processing and Intelligent Recognition Systems; Springer: Cham, Switzerland, 2016; Vol. 425, pp. 645–654.

[7] Lukas, J.; Fridrich, J.; Goljan, M. Digital camera identification from sensor pattern noise. IEEE Trans. Inf. Forensics Secur. 2006, 1, 205–214.

[8] Taspinar, S.; Mohanty, M.; Memon, N. Camera fingerprint extraction via spatial domain averaged frames. IEEE Trans. Inf. Forensics Secur. 2020, 15, 3270–3282.

[9] Khan, S.; Bianchi, T. Fast image clustering based on compressed camera fingerprints. Signal Process. Image Commun. 2021, 91, 116070.

[10] Lin, X.; Li, C.T. PRNU-based content forgery localization augmented with image segmentation. IEEE Access 2020, 8, 222645–222659.

[11] Lin, X.; Li, C.T. On constructing a better correlation predictor for PRNU-based image forgery localization. In Proceedings of the IEEE International Conference on Multimedia and Expo (ICME), Shenzhen, China, 5–9 July 2021; pp. 1–6.

[12] Meena, K.B.; Tyagi, V. A copy-move image forgery detection technique based on tetrolet transform. J. Inf. Secur. Appl. 2020, 52, 102481.

[13] Parveen, A.; Khan, Z.H.; Ahmad, S.N. Block-based copy-move image forgery detection using DCT. Iran J. Comput. Sci. 2019, 2, 89–99.

[14] Gani, G.; Qadir, F. A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata. J. Inf. Secur. Appl. 2020, 54, 102510.

[15] Chen, B.; Tan, W.; Coatrieux, G.; Zheng, Y.; Shi, Y.Q. A serial image copy-move forgery localization scheme with source/target distinguishment. IEEE Trans. Multimed. 2021, 23, 3506–3517.

[16] Yao, H.; Xu, M.; Qiao, T.; Wu, Y.; Zheng, N. Image forgery detection and localization via a reliability fusion map. Sensors 2020, 20, 6668.

[17] Chen, C.; Zhao, X.; Stamm, M.C. Generative adversarial attacks against deep-learning-based camera model identification. IEEE Trans. Inf. Forensics Secur. 2019, 15, 2169–2181.

[18] Kumar, M.; Srivastava, S. Image forgery detection based on physics and pixels: a study. Aust. J. Forensic Sci. 2019, 51, 119–134.

[19] Piva, A. An overview on image forensics. Int. Sch. Res. Not. 2013, 2013, 496701.

[20] Zhao, Y.; Zheng, N.; Qiao, T.; Xu, M. Source camera identification via low dimensional PRNU features. Multimed. Tools Appl. 2019, 78, 8247–8269.

[21] Thakur, R.; Rohilla, R. Recent advances in digital image manipulation detection techniques: a brief review. Forensic Sci. Int. 2020, 312, 110311.

[22] Warif, N.B.A.; Idris, M.Y.I.; Wahab, A.W.A.; Ismail, N.S.N.; Salleh, R. A comprehensive evaluation procedure for copy-move forgery detection methods. Multimed. Tools Appl. 2022, 81, 1–33.

[23] Lin, C.; Lu, W.; Huang, X.; Liu, K.; Sun, W.; Lin, H.; Tan, Z. Copy-move forgery detection using combined features and transitive matching. Multimed. Tools Appl. 2019, 78, 30081–30096.

[24] Bi, X.; Zhang, Z.; Xiao, B. Reality transform adversarial generators for image

Online ISSN 3007-3197
Print ISSN 3007-3189

splicing forgery detection and localization. In Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), Montreal, Canada, 11–17 October 2021; pp. 14294–14303.

[25] Doan, T.N.C.; Retraint, F.; Zitzmann, C. Image tampering detection based on a statistical model. Multimed. Tools Appl. 2021, 80, 32905–32924.

[26] Gardella, M.; Muse, P.; Morel, J.M.; Colom, M. Forgery detection in digital images by multi-scale noise estimation. J. Imaging 2021, 7, 119.

[27] Suganya, D.; Thirunadana Sikamani, K.; Sasikala, J. Copy-move forgery detection of medical images using golden ball optimization. Int. J. Comput. Appl. 2021, 43, 862–870.

[28] Arun Anoop, M.; Poonkuntran, S. LPG: a novel approach for medical forgery detection in image transmission. J. Ambient Intell. Humaniz. Comput. 2021, 12, 4925–4941.