I.J. Image, Graphics and Signal Processing, **2026, 3, 230-247**
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2026.03.12

Multi-channel Prediction Residue Modeling (MPRM) Using Second Order Residual Statistics for Enhanced CFA Artifact Based Forgery Detection

Somendra Kumar Soni*
JS Government Engineering College, Jagdalpur, India
E-mail: sksoni@gecjdp.ac.in
ORCID iD: https://orcid.org/0009-0005-5058-4416
*Corresponding author

Mohammad Rafique Khan
Government Engineering College, Raipur, India
Email: mrkhan@gecraipur.ac.in
ORCID iD: https://orcid.org/0000-0002-6117-5934

Vinay Kumar Singh
JS Government Engineering College, Jagdalpur, India
Email: vinay.rewa@gmail.com
ORCID iD: https://orcid.org/0000-0001-8642-2885

Received: January 26, 2026; Revised: March 1, 2026; Accepted: April 7, 2026; Published: June 8, 2026

Abstract: In recent years advanced image editing tools are easily available to tamper the images in visually undetectable form. This created an urgent need of reliable and robust technique to authenticate image integrity. Digital camera produces the full color image through interpolating remaining channels which creates periodic artifacts known as Color Filter Array Artifacts (CFAA). In forged image these artifact consistency is disturbed, which is often used to detect and localize the forgery in tampered images. Existing CFAA based splicing detection methods often rely on single channel, exhibit high computational complexity and show degraded performance under JPEG compression. Although some work have explored multi-channel CFA based approaches but their ability to effectively capture cross channel dependencies and maintain robustness under heavy JPEG compression remains limited. To address these gaps, we propose a splicing detection framework that performs second order statistical analysis on residuals extracted from all color channels. Unlike existing multichannel CFAA techniques, this work explicitly models inter-channel relationships through the Error Variance Ratio (EVR) and introduces a novel Inter Block Mean Square Error (IBMSE) metric. This formulation enhances the characterization of CFAA periodicity and improves discrimination between authentic and tampered regions. The proposed technique is evaluated on CUISDE, RTD and IMD datasets and compared with existing CFA based localization methods using ROC, precision-recall and AUC metric. Experimental results demonstrate that the proposed method improves localization performance and shows robustness against varying levels of JPEG compression.

Index Terms: Image Splicing, CFA Artifact, Image Tampering, Demosaicing, Bayer Pattern

1. Introduction

The rapid advancement of easily available image editing software and the development of artificial intelligence facilitate to create impeccable digital manipulated images. This growing technology pose serious challenge to the authenticity and credibility of the digital images. Also this can have serious implication on several domains such as journalism, social media, legal and scientific research [1, 2]. To address these challenges, digital image forensics has emerged as a crucial research area aimed to detect image tampering and restore trust in visual data. Based on literature

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

survey, existing forensic techniques can be broadly categorized into active and passive techniques. Active techniques require prior information of the image that has to be authenticated. One such example of active forensic technique is digital watermarking in which a hidden code is embedded in an image and during verification of tampered image this hidden signature is checked whether it is present or not. These dependency on prior information of image limits their applicability in real world scenarios [3]. Whereas the passive image forensics techniques do not require any prior information of manipulated image, instead these methods analyze intrinsic artifacts left during image manipulation [4-8]. Among various types of image manipulation, image splicing is one of the most common and challenging attacks. It involves combining regions from multiple images to create a composite image which is often producing visually convincing results, as illustrated in Figure 1. Some research utilized the inconsistencies in intrinsic image properties to detect and localize the image splicing forgery such as noise patterns[9-11], Color Filter Array (CFA) artifacts [12–24], JPEG compression marks [25], and blur inconsistency [26, 27]. This work address the CFA artifacts as forensics cues due to their hardware level origin and inherent reliability**.** In digital cameras, the CFA sensor captures only one color component per pixel and the missing channels are reconstructed through demosaicing which introduces structured interpolation artifacts. These artifacts remain consistent across authentic regions and are largely independent of specific manipulation operations. Consequently, any disruption in these in these patterns provides strong and reliable evidence for image tampering. However, effectively exploring these artifacts remains challenging due to post processing and modeling limitations.

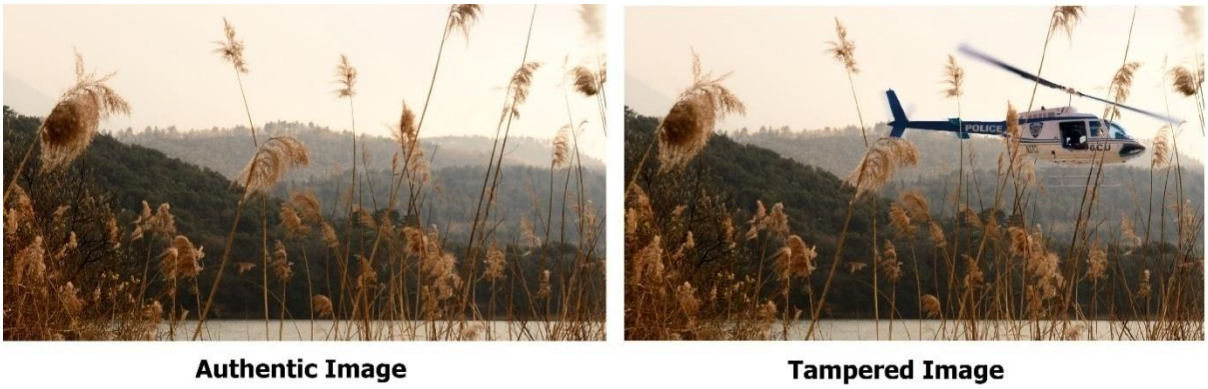


Fig. 1. Example of splicing forgery [30].

2. Related Work

Popescu and Farid [12] seminal work was among the first to use CFA inconsistencies in forgery detection. This study has introduced a framework based on periodic correlations induced by CFA interpolation and employs an expectation maximization (EM) algorithm to estimate interpolation coefficients. Thereby periodic peaks in Fourier domain analysis is utilized to verify the presence of CFA artifacts. Although this approach provides strong theoretical grounding but it is computationally expensive and shows coarser localization.

Gallagher and Chen in [13], proposed a frequency domain approach based on FFT analysis of CFA periodicity using large blocks size of 64×64. Although method is effective for detecting periodic patterns but it relies on large block sizes resulting in reduced effectiveness for small manipulations.

In [14], Dirik and Memon proposed a single feature based method that utilizes the low pass nature of interpolation, where a threshold is applied to the ratio of noise variance between interpolated and acquired pixels to distinguish authentic and tampered regions. The method is sensitive to JPEG compression and shows reduced effectiveness in identifying small tampered regions.

In [15], Ferrara et al. proposed a novel fine grained detection framework based on prediction error variance. The method operates on small blocks of size 2×2 in the green channel and models the statistical distribution using Gaussian Mixture Models (GMM). While this approach improves boundary localization but its performance degrades significantly under JPEG compression quality factor below 90 and in smooth regions.

In [16], Gonzalez Fernandez et al. proposed a technique that utilizes the Discrete Cosine Transform (DCT) on interpolation residuals. Subsequently DCT coefficients are analyzed to identify inconsistencies. The method achieves an accuracy of approximately 86% on benchmark datasets. However, the approach produces false positives in smooth regions and similar to prior work its performance degrades significantly under JPEG compression.

In [17], Amneet Singh et al. proposed a Markov Transition Probability Matrix (MTPM) based approach to capture spatial dependencies in CFA artifacts. This method effectively improves tampering localization by modeling the transition probabilities between neighbouring pixels. However, it requires a large feature set which significantly increases its computational complexity. Similarly, Gurinder Singh et al. [18] extended this work by incorporating DCT in MTPM approach and SVM (support vector machine) is used to localize the forged regions. Although this method

improves detection accuracy by leveraging higher order statistics but it still suffers from high computational complexity due to large feature dimensionality.

In [19], Le and Retraint proposed an improved CFA based forgery detection method by analyzing demosaicing artifacts in the noise residual domain. The method extracts feature statistics from the green channel and models them using a normal mixture model with penalized Expectation Maximization (EM) for tampering localization. This approach improves the detection accuracy. However, it introduces high computational overhead due to EM based modeling and remains sensitive to strong JPEG compression.

In [20], Wang et al. used bicubic interpolation on 16 neighbouring pixels to estimate prediction error and followed by GMM based statistical modeling employed over small blocks of 2×2 to 6×6. This improves localization precision but remains sensitive to noise and post processing.

In [21], Park et al. proposed a demosaicing based approach that utilizes Singular Value Decomposition (SVD) to calculate prediction residue and shown improved tampering localization accuracy. Similar to earlier approaches, this method still encounters difficulties when dealing with realistically manipulated images and those subjected to JPEG compression.

In [22], Liu et al. proposed a method by incorporating noise fingerprint with CFA configuration. In this method, noise residuals are extracted using a dual tree based wavelet de-noising approach and variance ratios are computed within a sliding window of size 42 to 48. While the use of large windows improves robustness against JPEG compression but it reduces localization accuracy for small tampered regions. In [23], Liu et al. proposed a CFA based forgery localization method that employs statistical analysis independent of linear interpolation assumptions. This method improves tampering detection performance by incorporating curvature based statistical analysis along with EM based modeling. Because of multiple statistical modeling stages increases its computational complexity.

To overcome the limitation of single channel analysis, Gonzalez Fernandez et al. [24] introduced a CFA based multi-channel correlation detection framework that utilizes 16×16 block size over all RGB channels. Although this approach improves robustness against compression but still suffers from block size limitations and shows degraded performance on lower compression quality factor.

The above related work is summarized in Table 1. It provides a comparative overview of existing CFA based forgery detection methods in terms of their features, models and limitations.

Table 1. Comparative overview of existing CFA based forgery detection methods.

Ref.	Method	Core Feature	Model Used	Strengths	Limitations
[12]	CFA correlation	Pixel correlation + Fourier analysis	EM	Strong theoretical foundation	High complexity, poor fine localization
[13]	FFT periodicity	Variance periodicity	FFT	Periodic pattern detection	Poor localization for small regions
[14]	Variance ratio	Noise variance ratio	Threshold	Simple, low cost	Fails under JPEG, small region detection
[15]	Variance imbalance	Prediction error variance	GMM	Fine grained localization	JPEG sensitive, unstable in smooth regions
[16]	DCT based CFA	DCT high frequency	Statistical	Detects small manipulations	False positives, post processing sensitive
[17]	MTPM	Transition probability	Statistical	Captures spatial dependencies	High feature dimension
[18]	DCT + MTPM	DCT + MTPM	SVM	High detection accuracy	High complexity
[19]	Noise domain CFA	Noise residual variance	EM	Improved detection accuracy	High computational cost, JPEG sensitive
[20]	Bi-cubic + GMM	Prediction error	GMM	High precision	Sensitive post processing
[21]	SVD based CFA	Prediction residue (SVD)	Statistical	No interpolation assumption, improved localization	Sensitive to compression, false positives in smooth regions
[22]	Noise + CFA hybrid	Noise variance ratio	Statistical	Robust to compression	Poor localization (large window)
[23]	Range based CFA	Probability + curvature	GMM + EM	No interpolation assumption	High complexity
[24]	Multi-channel CFA	Pattern correlation	Statistical	Uses RGB information	Block size limitation, JPEG sensitive

2.1. Key Limitations of Existing Methods

Based on the above discussion, several research gaps have been identified. Existing methods suffer from limitations such as single channel dependency, high computational complexity, larger block size and sensitivity to compression. However, some studies utilized multichannel information with larger block size. In the context of computational overhead the existing techniques shows higher computation cost because they rely on complex models such as GMM and EM. Similarly methods based on MTPM requires $(2T+1)^2$ features in which the number of features per block grows as the feature range [-T T] increases. Moreover, in existing studies show that the detection accuracy on JPEG compressed images drops sharply when compression ratio falls below 90.

2.2. Major Contributions of This Work

The key contributions to address the limitations of existing image forgery detection methods are outlined as follows:

1. Multichannel Prediction Residual Model (MPRM) Based Feature Design: The proposed method uses prediction residuals from all three color channels (red, green, and blue) instead of relying only on the green channel. This multichannel approach captures richer demosaicing artifact which shows consistent performance over diverse datasets.

2. Inter-Block Variance Ratio for Improved Detection Accuracy: The proposed method computes the inter-block mean square error (IBMSE) of the variance ratio between interpolated and acquired pixels. Further neighbor block correlation is analyzed to reduce false positive rate and improved the sensitivity to manipulations.

3. Robustness to JPEG Compression: As the proposed MPRM framework utilized the multichannel approach and IBMSE descriptor which increases the method sensitivity over manipulation. Thereby performances over multiple dataset have shown the strong robustness against JPEG compression.

4. Complexity Characterization in Terms of Simulation Time: Existing approaches used computationally intensive probabilistic models such as GMM and MTPM model which needs to simulate large feature set. Therefore this work introduces a simplified sigmoid of logarithmic features for Probability and binary map generation which reduces the computational overhead.

The rest of this paper is outlined as follows: In section 3 presents the proposed scheme in which design of the multi channel prediction residue model based features extraction and localization strategy is described in detail. Section 4 discusses the experimental settings used for simulation. Section 5 discusses the experimental results on benchmark datasets and demonstrated the effectiveness of the proposed method. Finally conclusion is provided in section 6.

3. Proposed Scheme

The overall workflow of the proposed method is illustrated in Figure 2. Given a suspected RGB image Z(x, y), the method detects forged regions by exploiting CFA inconsistencies through pixel level feature extraction followed by aggregation at the block level of size 8×8. The workflow is implemented through Algorithm 1 and it produces a probabilistic tampering map P (m, n) and a corresponding binary map using a threshold of 0.5.

Algorithm 1. Evaluation of the proposed probability and binary localization map

1. **Input:** Suspected or tampered RGB image Z(x, y)
2. **Output:** Probabilistic forgery map P (m, n) and binary localization map
3. Initialization: Block size B = 8, Gaussian window size M =4, and threshold τ=0.5
4. Boundary condition: Apply mirror padding to handle boundary pixels.
5. Decompose Z(x, y) into $A_r(x, y)$, $A_g(x, y)$, and $A_b(x, y)$ using Equation (1)
6. **for** each pixel (x, y) in the image **do**
7. Classify as Acquired or Interpolated using the Bayer pattern (as shown in Figure 3(a)).
8. **end for**
9. **for** each pixel (x, y) **do**
10. Compute re-interpolated pixel $Z_P(x, y)$ using Equation (3).
11. **end for**
12. **for** each pixel (x, y) **do**
13. Compute prediction error e(x, y) using Equation (4).
14. Store channel-specific errors $e_r(x, y)$, $e_g(x, y)$, $e_b(x, y)$.
15. **end for**
16. **for** each pixel (x, y) **do**
17. Normalize weights a_{ij} using Equations (8)-(9)
18. Compute local mean $\mu_e(x, y)$ using Equation (10).
19. Compute local weighted variance $\sigma^2_{e_c}(x, y)$ using Equation (7).
20. **end for**
21. Divide image into non-overlapping blocks B(m, n)
22. **for** each block **do**
23. Compute $\sigma^2_{\mathrm{IBMSE}}(x, y, c)$ using Equations (12-15)
24. **end for**
25. **for** each block B(m, n) **do**
26. Compute $S_A(m, n)$ using Equation (17)
27. Compute $S_I(m, n)$ using Equation (18)
28. Compute $M(m, n) = \frac{S_A(m,n)}{S_I(m,n)}$ ▷ Equation (16)

29. Compute F (m, n) = -log{M(m, n)} ▷ Equation (19)
30. **end for**
31. Apply 3 ×3 median filter to F(m, n)
32. Convert to probability map using P (m, n) = $\frac{e^{F(m,n)}}{1+e^{F(m,n)}}$ ▷ Equation (20)
33. Generate binary map:
34. If P (m, n) ≥ τ →Forged
35. Else → Authentic
36. **Return** P (m, n) and binary localization map

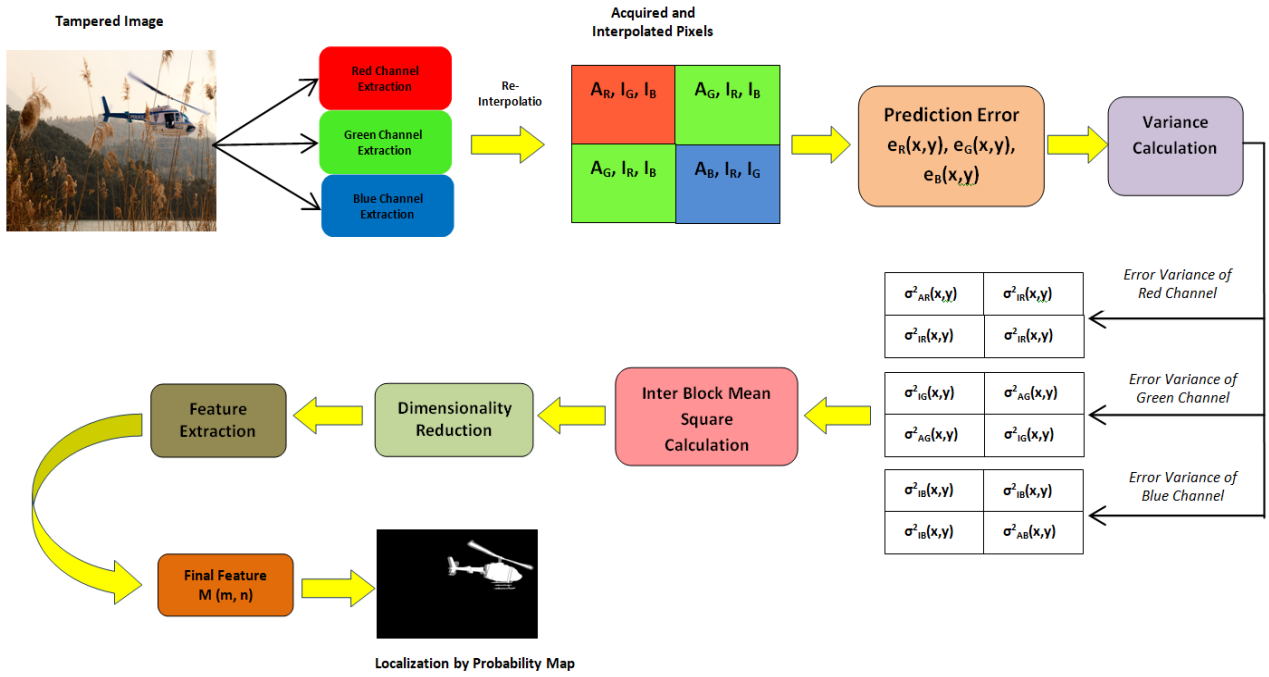


Fig. 2. Work flow of proposed method.

3.1. Channel Separation and Re-interpolation

The CFA is a critical component in digital imaging acquisition process because it governs how color information is captured at the sensor level. As most digital cameras utilizes Bayer pattern to capture the raw pixel values which is a specific arrangement of red, green, and blue channels. Within each Bayer pattern typically have two green pixels, one red and one blue pixel. Figure 3(a) illustrates the conventional Bayer pattern, where the red and green filters alternate along one row, and green and blue filters alternate along the subsequent row. Each pixel in the raw image sensor data is thus limited to a single-color channel, requiring demosaicing algorithms to interpolate the missing color components for transforming the raw sensor data into a complete color image. A crucial part of this analysis is re-interpolating missing values in each color channel, where the choice of interpolation method can greatly impact detection accuracy. As earlier studies have shown that the selecting an appropriate interpolation kernel plays a key role in effective forgery localization [21]. Hence, we adopted bilinear technique as the re-interpolation method for this work. As illustrated in Figure 3(b), the interpolated and acquired pixels are denoted by (I_r, I_g, I_b) and (A_r, A_g, A_b) corresponding to the red, green, and blue channels, respectively. For any 2×2 block in a Color Filter Array (CFA) image, the values of the acquired pixels $Z_A(x, y)$ at location (x, y) can be determined as follows:

$$Z_A(x,y) = \begin{cases} A_r(x,y) & if\ x mod 2 = 1\ and\ y\ mod 2 = 1, \\ A_g(x,y) & if\ (x+y) mod 2 = 1, \\ A_b(x,y) & if\ x\ mod 2 = 0\ and\ y\ mod 2 = 0, \\ 0 & otherwise. \end{cases} \quad (1)$$

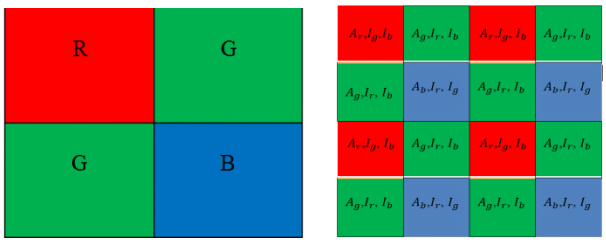
Where: $A_r(x, y)$, $A_g(x, y)$, $A_b(x, y)$ is the acquired value from the red, green and blue channel respectively. After demosaicing process the reconstructed pixel value $Z_R(x, y)$can be defined as:

$$Z_R(x,y) = \begin{cases} A_g(x,y) & if\ (x+y)\ mod2 = 1 \\ \sum_u h_u Z_A(x+u,y) & if\ (x+y) mod2 = 0 \\ A_r(x,y) & if\ x\ mod2 = 1\ and\ y\ mod2 = 1 \\ \sum_u h_u Z_A(x+u,y) & otherwise \\ A_b(x,y) & if\ x\ mod2 = 0\ and\ y\ mod2 = 0 \\ \sum_u h_u Z_A(x+u,y) & otherwise \end{cases} \quad (2)$$

Where: $Z_A(x,y)$ is the acquired pixel value and $Z_R(x,y)$ is the resultant signal after interpolation. h_u is the interpolation kernel and $\sum h_u$=1. For prediction of interpolated pixel value the re-interpolated kernel is assumed to be $k_u$then predicted pixel $Z_P(x,y)$at interpolated pixel position can be written as:

$$Z_P(x,y) = \sum_{u,v} k_{u,v} Z_R(x+u, y+v) \quad (3)$$

Where: $Z_R(x+u,y+v)$ is the reconstructed pixel value, $k_{u,v}$ is the re-interpolation kernel weight at offset u, v and the kernel satisfies the normalization condition $\sum k_{u,v}$= 1.



(a) (b)

Fig. 3. (a) Example of Bayer pattern. (b) Acquired and interpolated pixel.

3.2. Prediction Error

The prediction error is estimated from the difference of predicted value at the interpolated pixel position and acquired pixels thereby prediction error e (x, y) can be expressed as:

$$e(x,y) = \begin{cases} A_r(x,y) - \sum_{u,v} k_{u,v} Z_R(x+u,y+v) & if\ x mod2 = 1\ and\ y\ mod2 = 1 (Red\ Pixel\ acquired) \\ \sum_{u,v} (h_{u,v} - k_{u,v}) Z_R(x+u,y+v) & otherwise (Red\ Pixel\ interpolated) \\ A_g(x,y) - \sum_{u,v} k_{u,v} Z_R(x+u,y+v) & if\ (x+y) mod2 = 1 (Green\ Pixel\ acquired) \\ \sum_{u,v} (h_{u,v} - k_{u,v}) Z_R(x+u,y+v) & if\ (x+y) mod2 = 0 (Green\ Pixel\ interpolated) \\ A_b(x,y) - \sum_{u,v} k_{u,v} Z_R(x+u,y+v) & if\ x mod2 = 0\ and\ y\ mod2 = 0 (Blue\ Pixel\ acquired) \\ \sum_{u,v} (h_{u,v} - k_{u,v}) Z_R(x+u,y+v) & otherwise (Blue\ Pixel\ interpolated) \end{cases} \quad (4)$$

Where: $h_{u,v}$: Original interpolation kernel and $\sum h_{u,v}$ = 1

3.3. Variance of Prediction Error

Kirchner [28], discovered that the variance of e(x, y) shows a cyclical pattern with its period corresponding to the original sampling rate. In this scenario, e(x, y) signifies the prediction error of a resampled signal. Therefore, when an image is re-sampled, the variance ratio between the acquired and interpolated pixels also shows periodicity and consistently observable across all three color channels. Therefore the variance of the prediction error for each color channel can be expressed as Equations (5) & (6) for acquired and interpolated pixels respectively.

$$Var[e_C(x,y)] = \sigma_{A_C}^2 [(1 - \sum k_u h_{-u}) R(x,y) + \sum_{t \neq 0} (\sum k_u h_{t-u}) A_C(x+t, y+t)] \quad (5)$$

For interpolated pixels, the simplified variance based on kernel difference is:

$$\text{Var}[e_C(x,y)] = Var[\sum (h_u - k_u) \quad I_C(x+u, y+v)] = \sigma_{I_C}^2 \sum_u (h_u - k_u)^2 \quad (6)$$

Where: e, I *and* σ^2 A, C stands for prediction error, interpolated pixel, variance, acquired pixel and channels respectively. t: Offset index for neighboring pixels and u, v: Spatial offsets in the interpolation window.

Based on Equations (5) and (6), it can be inferred that the variance at acquired pixel location (σ_A^2) is typically higher than the variance at interpolated pixel location(σ_I^2). This is due to the inherent demosaicing artifacts introduced

during the image formation process. Thus in cases of image tampering this statistical relationship $\sigma_A^2 \geq \sigma_I^2$ may be disrupted. Therefore, the discrepancy in this prediction residue variance becomes a critical cue for identifying and localizing image forgeries. Furthermore, the local weighted variance of the prediction error $\sigma_{e_c}^2(x,y)$ can be formulated as:

$$\sigma_{e_c}^2(x,y) = \frac{1}{K}\left[\left(\sum_{i,j=-M}^{M} \alpha_{ij}\, e_c(x+i, y+j\right) - (\mu_{e_c}(x,y))^2\right] \tag{7}$$

Where c ϵ {red, green, blue} and α_{ij} are the weights which can be calculated as:

$$\alpha_{ij} = \frac{\alpha_{ij}'}{\sum_{i,j} \alpha_{ij}'} \tag{8}$$

And

$$\alpha_{ij}' = \begin{cases} W(i,j) & if\ e_c(x+i, y+j) \text{ Belongs to the } same\ class\ of\ e_c(x,y) \\ 0 & otherwise \end{cases} \tag{9}$$

Where $W(i,j)$ is a Gaussian window of size (2M+1) × (2M+1) with a standard deviation of M/2. The locally weighted mean of the prediction error μ_{e_c}(x, y) is calculated as:

$$\mu_{e_c}(x,y) = \left(\sum_{i,j=-M}^{M} \alpha_{ij}\, e_c(x+i, y+j) \right) \tag{10}$$

To ensure the error variance remains unbiased, the normalization constant K is given by:

$$\mathrm{K} = 1 - \left(\sum_{i,j=-M}^{M} {\alpha_{ij}}^2 \right) \tag{11}$$

3.4. Inter-block Mean Square Error

The proposed Inter Block Mean Square Error (IBMSE) metric is motivated by the observation that CFA interpolation artifacts are locally consistent in authentic image regions and tampering operations tend to disrupt these statistical dependencies. Therefore, this approach quantifies pairwise variance discrepancies between neighbouring blocks. This formulation provides a simplified and effective representation of local spatial dependencies that captures residual inconsistencies introduced by tampering. MRF based approaches require probabilistic modeling of neighborhood interactions which increases complexity. CNN based methods rely on large training data and learn statistical representations. In contrast IBMSE provides a direct deterministic measure of local inconsistency. Therefore the IBMSE can be formulated as:

$$IBMSE_c^{(d)}(u,v) = mean_square_error\left(\sigma_{e_c}^2(u,v), \sigma_{e_c}^2\left(u+t_x, v+t_y\right)\right) \tag{12}$$

Where t_x, t_y ϵ [-2, 0, 2], c ϵ {red, green, blue}, d ϵ { $\uparrow, \rightarrow, \downarrow, \leftarrow, \nearrow, \nwarrow, \swarrow, \searrow$}

3.5. Dimensionality Reduction

The IBMSE calculation performs differences in Error Variance Ratio (EVR) across eight directions and three color channels. This creates a detailed local feature set that captures inconsistencies between blocks. However, this detailed feature set also has some redundancy. Therefore the IBMSE values at each pixel location are aggregated into a single representative value using the following equation:

$$\sigma_{IBMSE}^2(x,y,c) = \frac{1}{N}\sum_{d} IBMSE_c^{(d)}(x,y,c) \tag{13}$$

Where: N, c and d denotes the number of directions, color channels and direction respectively.

The aggregation across directions is a statistical averaging process that reduces variance fluctuations induced by noise with minimal loss of discriminative information. This is because the averaging is done at any pixel location is belongs to either an acquired or interpolated class, thereby preserving class specific characteristics. In homogeneous regions, directional IBMSE values exhibit similar statistical behaviour which ensures that averaging maintains their

value range and similarly by using mirror padding preserves boundary variations. Furthermore, Due to the Bayer sampling pattern, the red and blue channels are sparsely acquired which results in multiple interpolated estimates at certain spatial locations. Therefore, the aggregation rules in Equations (14) and (15) are designed to ensure statistical consistency between acquired and interpolated variance estimates.

$$\sigma^2_{IBMSE}(\mathrm{x,y,r}) = \begin{cases} \sigma^2_{IBMSE}(x,y,r) & \text{if } x\bmod 2 = 1 \text{ and } y \bmod 2 = 1 \\ \mathrm{mean}\{\sigma^2_{IBMSE}(\mathrm{x,y,r}), \sigma^2_{IBMSE}(\mathrm{x,y-1,r}), \sigma^2_{IBMSE}(\mathrm{x-1,y,r})\} & \text{if } x\bmod 2 = 0 \text{ and } y \bmod 2 = 0 \\ 1 & \text{otherwise} \end{cases} \tag{14}$$

$$\sigma^2_{IBMSE}(\mathrm{x,y,b}) = \begin{cases} \sigma^2_{IBMSE}(x,y,b) & \text{if } x\bmod 2 = 0 \text{ and } y \bmod 2 = 0 \\ \mathrm{mean}\{\sigma^2_{IBMSE}(\mathrm{x,y,b}), \sigma^2_{IBMSE}(\mathrm{x+1,y,b}), \sigma^2_{IBMSE}(\mathrm{x,y+1,b})\} & \text{if } x\bmod 2 = 1 \text{ and } y \bmod 2 = 1 \\ 1 & \text{otherwise} \end{cases} \tag{15}$$

3.6. Feature Extraction

The proposed simplified feature extraction algorithm begins by computing the local variance for each pixel using Equation (7). Once these per pixel local variances are calculated, the tampered image of size X × Y is divided into non-overlapping blocks of B × B. Then block level feature M (m, n) can be calculated as:

$$\mathrm{M\ (m,\ n)} = \frac{S_A(m,n)}{S_I(m,n)} \tag{16}$$

$$S_A(m,n) = \prod_{c,(x,y)\in B_A(m,n))} \sigma^2_{IBMSE}(\mathrm{x,y,c}) \tag{17}$$

$$S_I(m,n) = \prod_{c,(x,y)\in B_I(m,n))} \sigma^2_{IBMSE}(\mathrm{x,y,c}) \tag{18}$$

Where $S_A(m,n)$, $S_I(m,n)$, $B_A(m,n)$, $B_I(m,n)$ represent the multiplicative aggregation of the features sets of acquired and interpolated pixels within the block and c refers to the color channel respectively.

In demosaiced images due to interpolation process its interpolated pixels become smoother which results in consistent variance compared to acquired pixels values. Therefore, the variance ratio M (m, n) between acquired and interpolated pixels M (m, n) is usually more than one in authentic region. Whereas in tampered region demosaicing effects get vanished, thereby the prediction error variances are evenly spread across both interpolated and original pixels which makes the M (m, n) ratio accumulates around one.

3.7. Localization

The proposed feature M (m, n) has a wide dynamic range which is transformed into a normalized probability map. This transformation facilitates intuitive interpretation by mapping raw feature values to likelihood scores that represent the probability of forgery at each block location. The localization process begins by applying a logarithmic transformation to stabilize the dynamic range:

$$F(m,n) = -\log\{M(m,n)\} \tag{19}$$

To suppress noise and enhance spatial consistency, a 3×3 median filter is applied to F (m, n). The filtered output is then converted into a probability score using the sigmoid function:

$$P(m,n) = \frac{e^{F\,(m,n)}}{1 + e^{F\,(m,n)}} \tag{20}$$

Here, P (m, n) ∈ (0, 1) denotes the likelihood that the corresponding block B (m, n) has been manipulated. Furthermore, a binary decision map is obtained by applying a threshold τ to the probability map P (m, n), where blocks satisfying P (m, n) ≥ τ are labelled as forged.

4. Experimental Settings

4.1. Dataset details

In order to demonstrate the reliability of the proposed tampering detection technique, comprehensive simulations were conducted using following benchmark datasets: the Columbia Uncompressed Image Splicing Detection Evaluation

Dataset [29], consists of 180 high quality images specifically designed to evaluate image splicing detection, the Realistic Tampering Dataset [30], contains 220 tampered images taken with four distinct camera models: Canon 60D, Nikon D90, Nikon D7000, and Sony A57 and the Image Manipulation Dataset [31], includes 160 manipulated images captured using cameras from Canon, Nikon, and Panasonic.

4.2. Performance Metrics

Tampering localization task has notable imbalance in class distribution as authentic pixels greatly outnumbering tampered ones. As a result, Receiver Operating Characteristics (ROC) and Precision -Recall are used as the evaluation metrics. These metrics are calculated from the standard components of a confusion matrix: True Positives (TP), False Positives (FP), True Negatives (TN) and False Negatives (FN). The evaluation metrics are defined as follows.

$$Recall\ (True\ Positive\ Rate,\ TPR) = \frac{TP}{TP + FN} \tag{21}$$

$$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} \tag{22}$$

$$Precision\ (P) = \frac{TP}{TP + FP} \tag{23}$$

Where:
TP – Number of tampered pixels correctly detected
TN – Number of authentic pixels correctly detected
FP – Number of authentic pixels incorrectly detected as tampered
FN – Number of tampered pixels missed by the detector

4.3. Implementation Details

All simulations were conducted using MATLAB R2022a on a system equipped with an Intel Core i7-8550U CPU running at 1.80 GHz, 8 GB of RAM and 64-bit Windows 10 operating system. Images were randomly selected from datasets to ensure unbiased performance evaluation. For feature extraction mirror padding is used and the block size B, Gaussian window size parameter M is taken 8×8 and 4 respectively. The complete experimental pipeline was executed entirely within the MATLAB's built-in Image Processing Toolbox environment without GPU acceleration**.**

5. Experimental Results

5.1. Variance Behaviour across Color Channels

To analyze the variance behaviour across color channels this work investigates the histogram distribution of features for red, green and blue channels. Each color component was processed individually to extract features for tampered and authentic region. Figure 4 shows the histograms distribution for each color channel which conclude that the features of tampered region is approximately equals to 1 whereas authentic regions has higher feature values. It also represents that each channel generates distinct feature pattern which means that CFA traces persist independently across color channels. Furthermore, quantitatively performances of the channels are analyzed by histograms overlapping of authentic and tampered region which is evaluated to 15%, 14%, and 16% for the R, G, and B channels respectively.

Moreover the proposed multichannel approach further reduced this histograms overlapping to 8% and by incorporating the IBMSE statistics further minimized this overlapping to 5%. This progressive improvement illustrates that the combination of multichannel analysis and IBMSE based modelling significantly strengthens the differentiability of CFA artifacts.

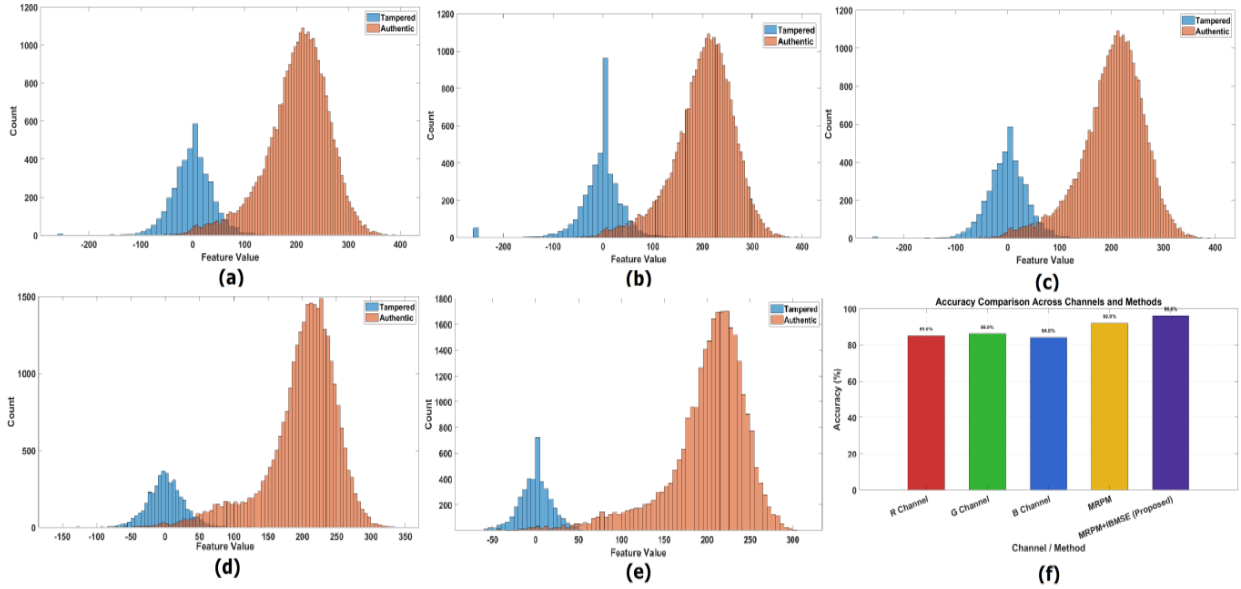


Fig. 4. Histograms of features for individual color channels and accuracy comparison between channels and the proposed method. (a) Red channel, (b) Green channel (c) Blue channel (d) Multichannel (e) Multichannel with IBMSE (proposed) (f) Accuracy comparison.

5.2. Ablation Study on Component Contributions

Table 2 presents the ablation study for individual color channels and provides an overview of their contribution when channels are combined. The study is carried out on CUISDE and RTD datasets and results demonstrate that use of a single channel yields moderate detection accuracy of around 84% to 86%. Furthermore, simulation results indicate that all three channels contain distinct and useful information and by limiting to only one channel restrict the model's potential to detect forgery artifacts. Moreover when using a multichannel fusion approach the detection accuracy is achieved about 92%. By incorporating IBMSE module with multichannel approach the detection accuracy is further increased to around 96%. The combined use of multichannel approach and the IBMSE module enables the proposed framework to effectively leverage inconsistencies introduced by forgery, thereby strengthening the overall detection capability.

Table 2. Quantitative Evaluation of Model Variants for Ablation Study.

Method	**CUISDE dataset**			**RTD dataset**		
	TPR	FPR	Accuracy (%)	TPR	FPR	Accuracy (%)
Only R Channel	0.82	0.21	85	0.78	0.25	84.6
Only G Channel	0.84	0.18	86	0.82	0.20	86.2
Only B Channel	0.83	0.19	84	0.83	0.22	84.5
Multichannel (RGB Fusion)	0.91	0.13	92	0.89	0.14	91.2
Multichannel + IBMSE (Proposed)	0.94	0.13	96	0.92	0.12	95.4

5.3. Quantitative Comparison

In Figure 5 the performance of the proposed method is quantitatively evaluated by Receiver Operating Characteristics (ROC) curves, precision-recall and the Area under the Curve (AUC) value against five state of the art tampering localization methods. Figure 5(a) illustrates the ROC curve and their corresponding AUC values for CUISDE dataset. ROC curve shown in figure 5(a) demonstrate that the proposed method have high true positive rate with minimal false positive rate which is outperformed the other localization methods. The proposed method also shows highest AUC values of 0.96 which is 2.12 % improvement over second ranked park's method. Similarly, Figure 5(b) and Figure 5(c) illustrate the ROC curve and their corresponding AUC values for RTD and IMD dataset respectively. In Figure 5(b) and Figure 5(c) shows the highest AUC value for the proposed method which is 0.91 and 0.92 respectively. Figure 5(c), Figure 5(d) and Figure 5(e) presents the precision-recall curve and their corresponding AUC values for CUISDE, RTD and IMD dataset respectively. As shown in these figures the proposed method shows better performance with respect to other localization methods. The AUC value of proposed method is 0.94, 0.86 and 0.92 for CUISDE, RTD and IMD dataset respectively which is higher than other forgery localization methods.

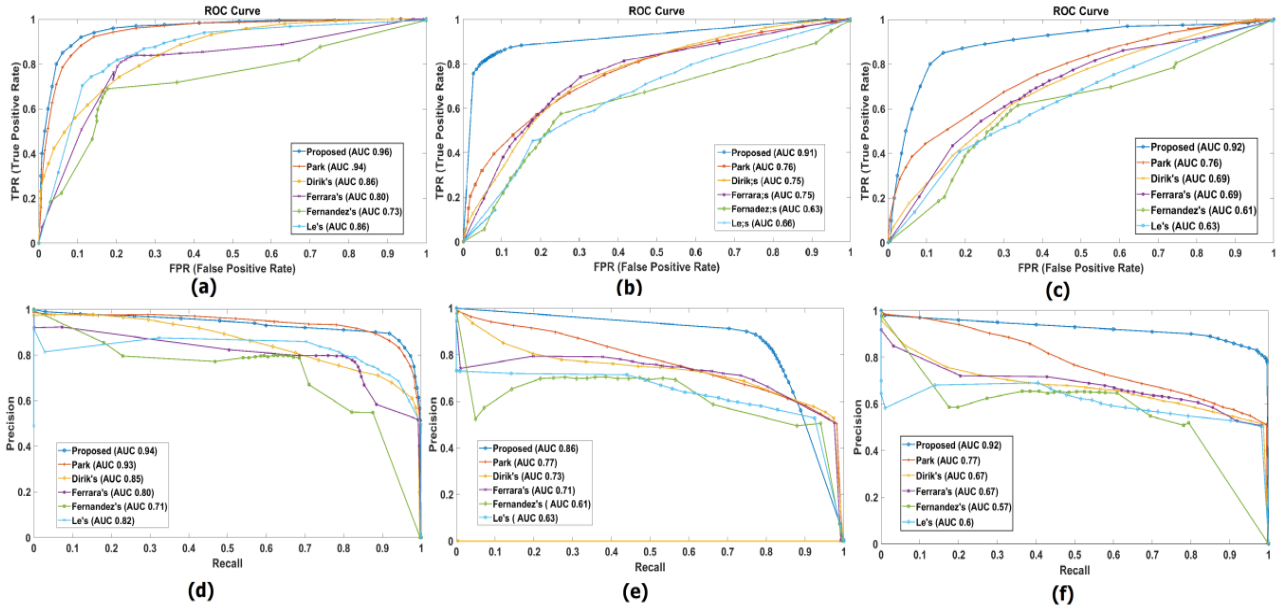


Fig. 5. Performance of the various methods across different datasets. ROC curve and AUC values for: (a) CUISDE dataset, (b) RTD dataset (c) IMD dataset (d) CUISDE dataset. Precision Recall curve and AUC values for: (e) RTD dataset (f) IMD dataset for Precision–Recall curves.

5.4. Qualitative Comparison

Figure 6 presents the forgery localization performance for CUISDE dataset. The approaches proposed by Dirik and Park shows only coarse localization of manipulated regions whereas the techniques developed by Ferrara and Fernandez frequently miss the tampered areas. Although Le's method detects boundary of manipulated regions but it has high rate of false positives.

Figure 7 illustrates the localization performance on the RTD dataset. Ferrara's and Le's localization performance is better than Dirik's and Fernandez's method. Park's method can detect manipulated areas but often misclassify genuine regions as tampered.

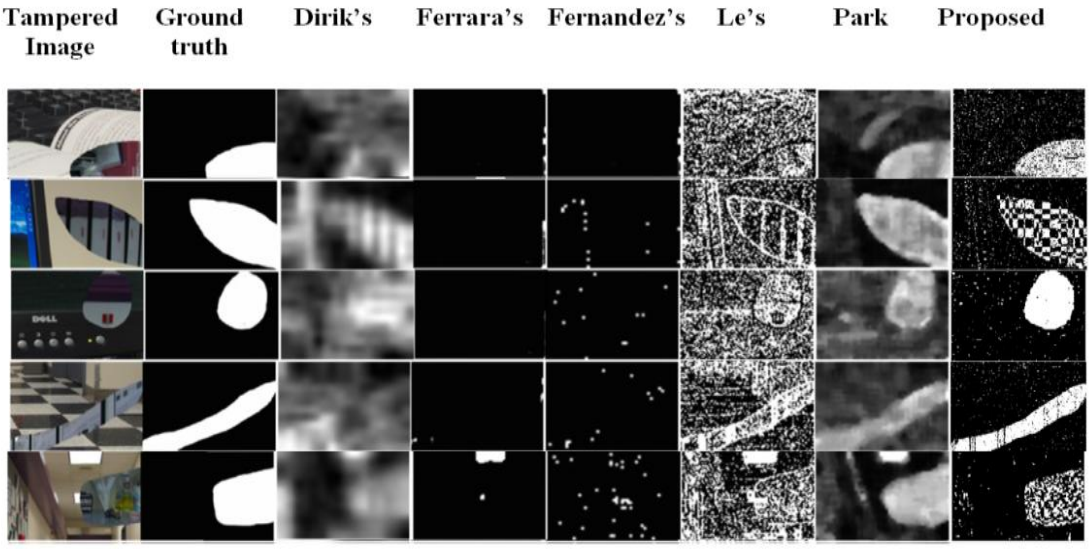


Fig. 6. A comparative analysis of tampering localization methods was conducted using the Columbia Uncompressed Image Splicing Detection Evaluation dataset.

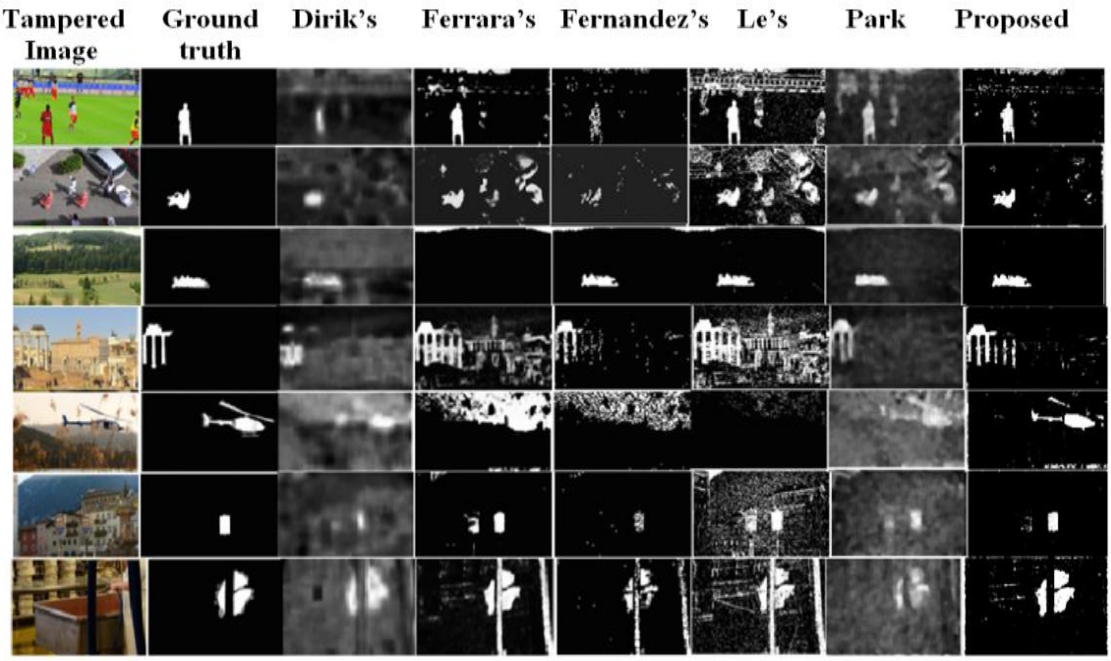


Fig. 7. A comparative analysis of tampering localization methods was carried out using the Realistic tampering dataset.

Figure 8 shows the localization results obtained using the IMD dataset. As shown in localization map the Dirik's method struggled to detect manipulated regions and able to highlight only the boundaries of the affected areas. Ferrara's approach generally fails to localize tampered region although it achieves partial success in specific instances. The methods proposed by Park, Fernandez, and Le demonstrated moderate performance but occasionally producing high false positive output. In contrast, the proposed method consistently achieved more accurate localization. As shown in Figure 6, Figure 7 and Figure 8 the proposed method localization performance is most consistent with the ground truth with minimal false positives which indicating its superior performance over other localization methods for all datasets.

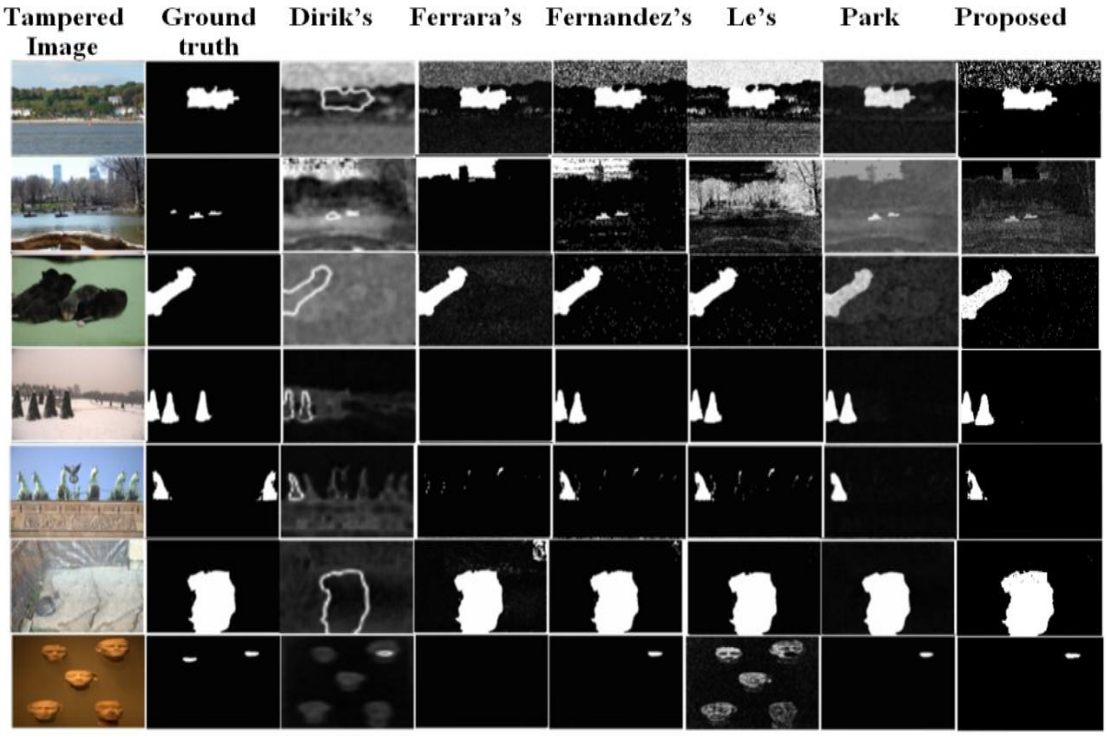


Fig. 8. Comparative analysis of tampering localization methods was conducted using the Image manipulation dataset.

5.5. Robustness Evaluation under JPEG Compression

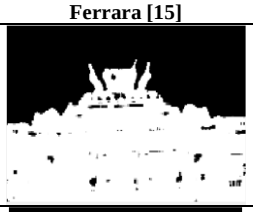
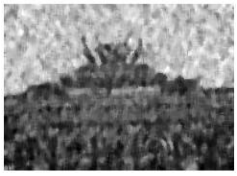
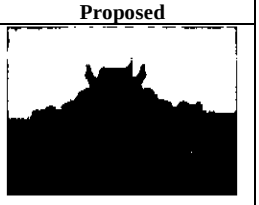
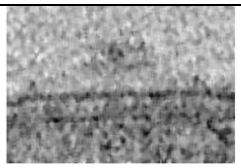
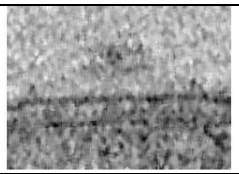
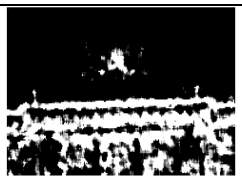
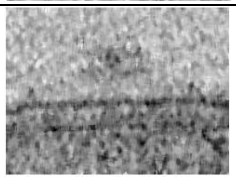
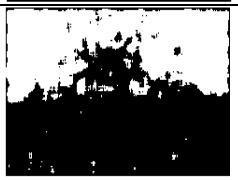
In earlier studies forgery localization methods generally fails to detect forgery on JPEG compressed images. Specifically, when the Jpeg compression quality factor falls below 90 the performance of forgery localization methods degrade gradually. Therefore to analyze the robustness of the proposed method this work evaluated forgery localization performance under various compression levels of JPEG100, JPEG 95, JPEG90 and JPEG 85.

Table 3 illustrate the overlapping of histogram (OH %) and binary localization of authentic and tampered region. As shown in Table 3(b), when the compression ratio decreased from 100 to 85, the Ferrara*'s* and Park's method shows a rapid rise in OH% from 6.8% to 64.3% and 7.9% to 40.6% respectively and that degraded performance is reflected by binary localization as shown in Table 3(a). Whereas, the proposed method provides considerably lower histogram overlap from, 6.15% to 19.1% which indicates superior robustness against JPEG compression.

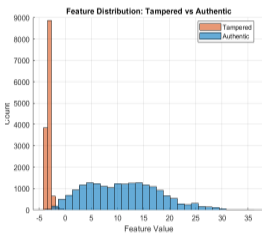
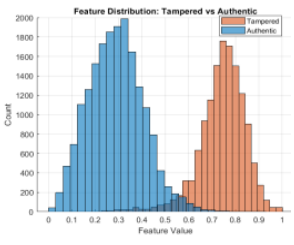
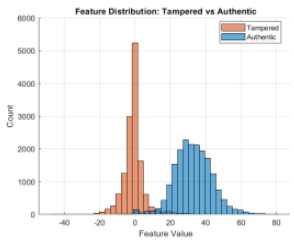
Table 3. Quantitative and Visual Comparison under JPEG Compression. (a) Forgery binary localization (b) Illustrates the corresponding histogram distributions and Overlapping of Histogram (OH %).

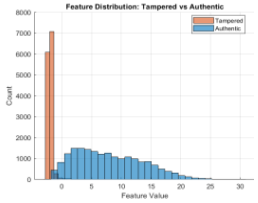
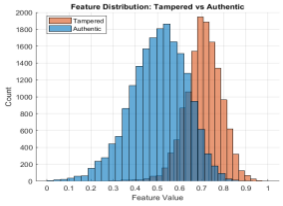
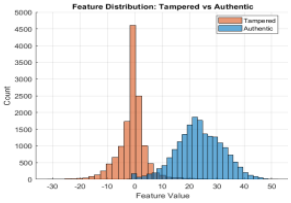
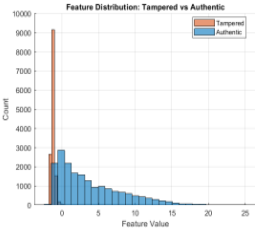
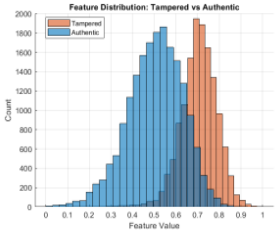
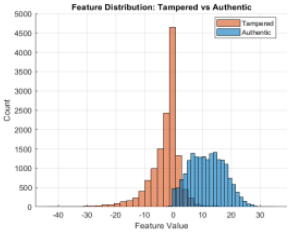
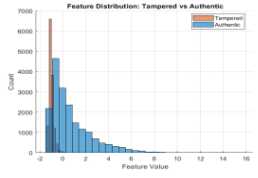
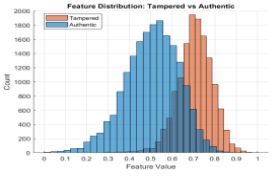
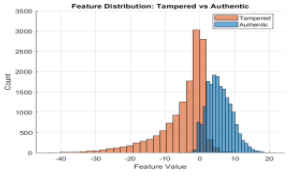


Tampered Image Ground Truth

Compression Level	Ferrara [15]	Park [21]	Proposed
JPEG 100			
JPEG 95			
JPEG 90			
JPEG 85			

(a)

Compr-ession Level	Ferrara [15]		Park [21]		Proposed	
	Histogram	OH (%)	Histogram	OH (%)	Histogram	OH (%)
JPEG 100		6.8		7.9		**6.1**

JPEG 95		16.1		35.4		**8.1**
JPEG 90		40.2		38.6		**15.4**
JPEG 85		64.3		40.6		**19.1**

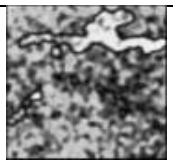
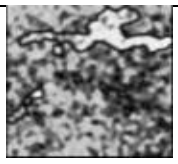
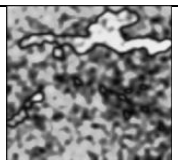
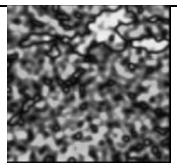
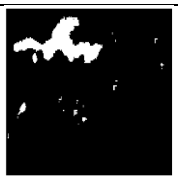
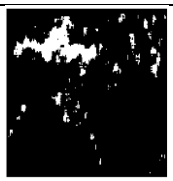
(b)

In Gonzalez Fernandez et al. [24] work utilized the multichannel feature to localize the forgery and shown robustness over JPEG compression. However, this method also shows similar degradation in localization performance below compression level 90. Thereby, In Table 4 presents a qualitative comparison of proposed method with Gonzalez Fernandez's method. The result highlights that the proposed method maintains clear, coherent and structurally accurate localization maps even when the compression ration decreased below 90 whereas the multichannel approach of Gonzalez Fernandez's shows a significant loss at higher compression levels and produces noisy, blurred and fragmented detection maps.

Table 4. Qualitative comparison of forgery localization under varying JPEG compression levels compared with existing multichannel approach.



Tampered Image **Ground Truth**

Method	**JPEG100**	**JPEG95**	**JPEG90**	**JPEG85**
Gonzalez Fernandez et al. [24]				
Proposed				

Furthermore, in Table 5 presents the robustness of the proposed method is quantitatively evaluated under varying JPEG compression levels for Quality factor (QF) 100 to 40 and compared with Ferrara et al. [15] and Park et al. [21] using precision and recall metrics. It is observed that as compression increases a significant degradation in precision occurs for existing methods while all methods maintain high recall across all compression levels. This sharp decline in precision and high recall beyond quality factor 85 indicates, increase in false positives. In contrast, the proposed method demonstrates comparatively stable performance while maintaining higher precision across all compression

levels. Overall, the proposed approach achieves a better balance between precision and recall which confirms its robustness and reliability under practical compression scenarios.

Table 5. Qualitative comparison of forgery localization under varying JPEG compression levels.

JPEG Quality Factor (QF)	Ferrara [15]		Park [21]		Proposed	
	Precision (%)	Recall (%)	Precision (%)	Recall (%)	Precision (%)	Recall (%)
100	94.23	95.60	93.61	95.18	96.82	95.81
95	93.44	96.91	88.97	96.31	94.83	94.30
90	77.46	97.27	60.47	96.48	91.30	95.91
85	60.61	98.55	55.65	97.96	86.31	96.22
70	56.59	98.74	52.36	98.22	83.45	96.83
60	47.53	98.47	51.58	98.73	81.10	97.14
50	42.98	99.05	48.67	98.83	71.25	97.83
40	36.44	99.42	42.45	98.99	67.20	98.20

5.6. Computational Efficiency Analysis

To analyze the computational efficiency and ensure fairness comparison against several demosaicing based forgery localization methods image and block size are taken 512×512 and 8×8 respectively. Table 6 shows the computational characteristics of the forgery localization methods. Ferrara's method achieves moderate performance whereas the SVD based method is more computationally intensive due to its reliance on matrix decomposition operations. The MTPM algorithm shows the highest runtime overhead due to large feature set. In contrast, the proposed Multichannel with IBMSE framework demonstrates the lowest processing time among all evaluated methods.

Table 6. Runtime comparison of various forgery localization methods.

Method	Processing Time (s)
Bilinear and GMM model [15]	6.32
SVD-based demosaicing [21]	10.68
MTPM-based model [17]	167.36
Multichannel + IBMSE (Proposed)	2.24

From a theoretical perspective, the proposed algorithm consists of three main stages: pixel level processing, local statistical estimation and block level aggregation. Let $N=X\times Y$ denote the total number of pixels in an image of size $X\times Y$. The pixel level operations which includes interpolation and prediction error computation, require a single pass over all pixels and thereby results in a complexity of O (N). The local statistical estimation computes mean and variance over a fixed window of size W leads to a complexity of O ($N\cdot W^2$).The block level processing divides the image into non-overlapping blocks of size $B\times B$, resulting in N/B^2 blocks. For each block, IBMSE features and decision metrics are computed across three color channels C, yielding a complexity of O ($N/B^2\cdot C$). Therefore, the overall computational complexity is given by:

$$Overall\ computational\ complexity = O\ (N+N.W^2 +N/B^2.\ C) \tag{24}$$

Since W, B, and C are constants, then complexity simplifies to O (N), this demonstrates that the proposed method scales linearly with image size.

6. Conclusion

This work focuses on improving digital image authentication in the presence of increasingly sophisticated image splicing techniques. Existing CFA based forensic methods often suffer from degraded performance under JPEG compression and show limited scalability on large datasets. To address these issues, a splicing detection framework based on second order statistical analysis of multichannel residuals is proposed. In particular, an IBMSE formulation of the EVR is introduced to better capture inconsistencies in CFA artifacts. The proposed method is qualitatively and quantitatively compared with existing state of the art conventional forgery localization techniques. Simulation results demonstrate that the proposed method consistently shows superior performance in terms of ROC, Precision-Recall and AUC metric. Moreover, the proposed method exhibits notable robustness against JPEG compression by maintaining high detection accuracy even under lower compression ratios. Experimental evaluations conducted on multiple benchmark datasets validate the effectiveness and generalization ability of the proposed approach. These findings suggest that the method offers a promising direction for advancing image forensics and improving the reliability of digital content verification.

All the Declarations and Statements

Author Contributions Statement
Somendra Kumar Soni – Conceptualization, Methodology, Formal Analysis, Constructed the overall framework, Data Curation and Software Implementation: Handled data acquisition, dataset pre-processing and implementing the research model. Validated results using standard metrics and benchmarked performance against existing methods. Writing: Drafted the initial manuscript.
Mohammad Rafique Khan – Conceptualization, Methodology, Supervision, Formal Analysis, Visualization, Performed in-depth analysis of experimental results and ensured the statistical robustness of the evaluation, Writing : Reviewed and edited the manuscript, ensured clarity and coherence.
Vinay Kumar Singh – Conceptualization, Methodology, Supervision, Formal Analysis, Visualization, Performed in-depth analysis of experimental results and ensured the statistical robustness of the evaluation, Writing : Review and Editing.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement
The authors declare no conflicts of interest.

Funding Declaration
None.

Data Availability Statement
This study analyzed publicly available datasets.

Ethical Declarations
Not applicable.

Acknowledgments
The authors gratefully acknowledge the Research Center of JSGEC Jagdalpur for the computing and Internet facilities provided for this work.

Declaration of Generative AI in Scholarly Writing
The authors declare that no generative AI tools were used in the preparation of this manuscript.

Abbreviations
The following abbreviations are used in this manuscript:

CFA – Color Filter Array
CFFA- Color Filter Array Artifact
EVR – Error Variance Ratio
IBMSE – Inter Block Mean Square Error
GMM- Gaussian Mixture Model
EM- Expectation Maximization
DCT – Discrete Cosine Transform
MTPM- Markov Transition Probability Matrix
SVD – Singular Value Decomposition
AUC – Area Under Curve
ROC- Receiver Operating Characteristics

Appendix
None.

References

[1] L. Verdoliva, “Media forensics and deepfakes: An overview,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910–932, 2020, doi:10.1109/JSTSP.2020.3002101.

[2] H. Farid, "Digital image forensics," *Scientific American*, vol. 300, no. 6, pp. 66–71, 2009.
[3] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 1st ed. San Francisco, CA: Morgan Kaufmann, 2002.
[4] P. Deb, S. Deb, A. Das, and N. Kar, "Image forgery detection techniques: Latest trends and key challenges," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3498340.
[5] V. K. Kadha, S. Bakshi, and S. K. Das, "Unravelling digital forgeries: A systematic survey on image manipulation detection and localization," ACM Computing Surveys, vol. 57, no. 12, Art. no. 323, pp. 1–36, 2025, doi: 10.1145/3731243.
[6] W. D. Ferreira, C. B. R. Ferreira, G. da Cruz Júnior, and F. Soares, "A review of digital image forensics," *Computers & Electrical Engineering*, vol. 85, p. 106685, 2020, doi: 10.1016/j.compeleceng.2020.106685.
[7] R. Thakur and R. Rohilla, "Recent advances in digital image manipulation detection techniques: A brief review," *Forensic Science International*, vol. 312, p. 110311, 2020, doi: 10.1016/j.forsciint.2020.110311.
[8] X. Lin, J. H. Li, S. L. Wang, A. W. C. Liew, F. Cheng, and X. S. Huang, "Recent advances in passive digital image security forensics: A brief review," *Engineering*, vol. 4, no. 1, pp. 29–39, 2018, doi:10.1016/j.eng.2018.02.008.
[9] S. Lyu, X. Pan, and X. Zhang, "Exposing region splicing forgeries with blind local noise estimation," *International Journal of Computer Vision*, vol. 110, no. 2, pp. 202–221, 2014, doi: 10.1007/s11263-013-0688-y.
[10] N. Zhu and Z. Li, "Blind image splicing detection via noise level function," *Signal Processing: Image Communication*, vol. 68, pp. 181–192, 2018, doi:10.1016/j.image.2018.07.012.
[11] B. Liu and C. M. Pun, "Locating splicing forgery by adaptive-SVD noise estimation and vicinity noise descriptor," *Neurocomputing*, vol. 387, pp. 172–187, 2020, doi:10.1016/j.neucom.2019.12.105.
[12] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948–3959, 2005, doi: 10.1109/TSP.2005.855406.
[13] A. C. Gallagher and T. Chen, "Image authentication by detecting traces of demosaicing," in Proc. IEEE Computer Society Conf. Computer Vision and Pattern Recognition Workshops (CVPRW), 2008, pp. 1–8, doi: 10.1109/CVPRW.2008.4562984.
[14] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, 2009, pp. 1497–1500, doi:10.1109/ICIP.2009.5414611.
[15] P. Ferrara, T. Bianchi, A. De Rosa, and A. Piva, "Image forgery localization via fine-grained analysis of CFA artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1566–1577, 2012, doi:. 10.1109/TIFS.2012.2202227.
[16] E. G. Fernández, A. S. Orozco, L. G. Villalba, and J. Hernandez-Castro, "Digital image tamper detection technique based on spectrum analysis of CFA artifacts," *Sensors*, vol. 18, no. 9, p. 2804, 2018, doi:10.3390/s18092804.
[17] A. Singh, G. Singh, and K. Singh, "A Markov based image forgery detection approach by analyzing CFA artifacts," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28949–28968, 2018, doi: 10.1007/s11042-018-6075.
[18] G. Singh and K. Singh, "Digital image forensic approach based on the second-order statistical analysis of CFA artifacts," *Forensic Science International: Digital Investigation*, vol. 32, p. 200899, 2020, doi:10.1016/j.fsidi.2019.200899.
[19] N. Le and F. Retraint, "An improved algorithm for digital image authentication and forgery localization using demosaicing artifacts," *IEEE Access*, vol. 7, pp. 125038–125053, 2019, doi: 10.1109/ACCESS.2019.2938467.
[20] X. Wang, S. Niu, and J. Zhang, "Digital image forensics based on CFA interpolation feature and Gaussian mixture model," *International Journal of Digital Crime and Forensics*, vol. 11, no. 2, pp. 1–14, 2019
[21] C. W. Park, Y. H. Moon, and I. K. Eom, "Image tampering localization using demosaicing patterns and singular value based prediction residue," *IEEE Access*, vol. 9, pp. 91921–91933, 2021, doi:10.1109/ACCESS.2021.3091161.
[22] L. Liu, P. Sun, Y. Lang, J. Li, and S. Shi, "Splicing forgery localization via noise fingerprint incorporated with CFA configuration," *Forensic Science International*, vol. 340, p. 111464, 2022, doi: 10.1016/j.forsciint.2022.111464.
[23] L. Liu, P. Sun, Y. Lang, and J. Li, "CFA-based splicing forgery localization method via statistical analysis," *IET Signal Processing*, vol. 18, 2024, Art. no. 9929900, doi: 10.1049/2024/9929900.
[24] E. G. Fernández, A. L. S. Orozco, and L. J. G. Villalba, "A multi-channel approach for detecting tampering in colour filter images," *Expert Systems with Applications*, vol. 230, p. 120498, 2023.
[25] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1003–1017, 2012, doi: 10.1109/TIFS.2012.2187516.
[26] K. Bahrami, A. C. Kot, L. Li, and H. Li, "Blurred image splicing localization by exposing blur type inconsistency," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 999–1009, 2015, doi:10.1109/TIFS.2015.2394231.
[27] D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, P. Shivakumara, and S. Sadeghi, "A novel forged blurred region detection system for image forensic applications," *Expert Systems with Applications*, vol. 64, pp. 1–10, 2016, doi:10.1016/j.eswa.2016.07.026.
[28] M. Kirchner, "Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue," in *Proc. 10th ACM Workshop Multimedia Security (MM & Sec '08)*, 2008, pp. 11–20, doi: 10.1145/1411328.1411333.
[29] T. T. Ng and S. F. Chang, "A dataset of authentic and spliced image blocks (Tech. Rep. 203-2004)," *Columbia University*, 2004. [Online]. Available: https://www.ee.columbia.edu/ln/dvmm/downloads/authsplcuncmp/
[30] P. Korus and J. Huang, "Multi-scale analysis strategies in PRNU-based tampering localization," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 809–824, 2016. [Online]. Available: https://pkorus.pl/downloads/dataset-realistic-tampering
[31] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, 2012. [Online]. Available: https://www5.cs.fau.de/research/data/image-manipulation/

Authors' Profiles



Somendra Kumar Soni is a PhD. Scholar in the Department of Electronics and Communication, JS Government Engineering College, Jagdalpur Chhattisgarh, India. He has B.E. degree in Electronics and Telecommunication Engineering from SSCET Bhilai, Chhattisgarh, in 2011, and his M.Tech. Degree from the IIT Roorkee in 2013. He has professional experience as a Site Engineer at Rail Vikas Nigam Limited and as an Executive Engineer at the Airport Authority of India, where he worked for 1.5 years. He is currently working as an Assistant Professor at JS Government Engineering College, Jagdalpur, Chhattisgarh, India. His research interests include computer vision, soft computing, machine learning, and image forgery detection.



Mohammad Rafique Khan received his Bachelor of Engineering degree in Electronics and Telecommunication Engineering from Engineering College, Jabalpur, India, in 1985. He obtained his M.Tech. Degree in Telecommunication Systems Engineering from IIT Kharagpur, India, in 2000. He received his Ph.D. degree in Electronics and Electrical communication Engineering from NIT Raipur, India, in 2008. He is currently working as Principal at Government Engineering College, Raipur, Chhattisgarh, India. He has three decades of academic and administrative experience and his research interests include telecommunication systems and signal processing.



Vinay Kumar Singh received his Bachelor of Engineering degree in Electronics and Communication Engineering from Government Engineering College, Rewa, India, in 1999. He obtained his M.Tech. Degree in Electronics and Communication Engineering from the Institute of technology, BHU, Varanasi, India, in 2002. He received his Ph.D. degree in Electrical Engineering from IIT Kanpur, India, in 2013. He is currently working as an Associate Professor in the Department of Electronics and Telecommunication at JS Government Engineering College, Jagdalpur, Chhattisgarh, India. His research interests include Signal processing, Soft Computing, Solid-State Devices, Device Fabrication and Modeling.

How to cite this paper:

Somendra Kumar Soni, Mohammad Rafique Khan, Vinay Kumar Singh, "Multi-channel Prediction Residue Modeling (MPRM) Using Second Order Residual Statistics for Enhanced CFA Artifact Based Forgery Detection", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.18, No.3, pp. 230-247, 2026. DOI:10.5815/ijigsp.2026.03.12