RESEARCH ARTICLE

Fast and Robust Copy-Move Forgery Detection Using BRIEF, FAST, and SIFT Feature Matching

Muhammad Jamshed Abbass[1], Ali Waqar[2], Natasha Seemab[3], Abdul Saboor Khan[4], Muhammad Bilal Riaz[5], Sharjeel Abbas[6] and Bilal Mushtaq[7,*]

[1] Faculty of Electrical Engineering, Wrocław University of Science and Technology, 50-370 Wrocław, Poland
[2] School of Mechanical and Electrical Engineering, Quanzhou University of Information Engineering, Quanzhou 362000, China
[3] Department of Mathematics, Faculty of Science, Chiang Mai University, Chiang Mai 50200, Thailand
[4] Department of Electrical Engineering and Information Technology, Otto-von-Guericke University Magdeburg, 39106 Magdeburg, Germany
[5] IT4Innovations, VSB – Technical University of Ostrava, 708 00 Ostrava, Czech Republic
[6] Faculty of Electrical Engineering, Saint Petersburg Electrotechnical University "LETI", 197376, Saint Petersburg, Russia
[7] Electrical and Electronic Engineering Department, Beaconhouse International College, Islamabad 44000, Pakistan

Abstract

This paper presents a novel hybrid copy–move forgery detection method that combines the efficiency of FAST-BRIEF (for rapid keypoint detection and binary descriptors) with the robustness of SIFT (for scale- and rotation-invariant feature matching). The proposed framework employs g2NN matching for accurate feature correspondence, followed by morphological processing and LSC-SSIM superpixel segmentation for precise localization of tampered regions. The method is evaluated on 30 diverse test images from benchmark datasets comprising over 700 images, achieving a 95% F-measure with an average CPU time of 6.02 seconds. It demonstrates strong resilience to geometric transformations (rotation, scaling), photometric adjustments (contrast, brightness), additive noise, and multiple forgeries. The proposed methodology offers a 5–30% improvement in accuracy and computational speed. This approach addresses emerging challenges in deepfake detection and satellite imagery authentication, where localized manipulations threaten media integrity.

Keywords: hybrid FAST-BRIEF-SIFT, g2NN matching, LSC-SSIM segmentation, copy-move forgery detection, satellite image authentication, real-time forensics, f-measure optimization.

1 Introduction

Human vision is very good at interpreting visual imprints. When technology was limited, the human brain was able to distinguish between a forged and an original. Digital imaging technology has revolutionized the world, enabling rapid and realistic

Submitted: 11 July 2025
Accepted: 02 October 2025
Published: 25 November 2025

Vol. 3, **No.** 1, 2026.
10.62762/TETAI.2025.152706

***Corresponding author:**
✉ Bilal Mushtaq
bilalmushtaq88@outlook.com & bilal.mushtaq@bic.edu.pk

Citation
Abbass, M. J., Waqar, A., Seemab, N., Khan, A. S., Riaz, M. B., Abbas, S., & Mushtaq, B. (2025). Fast and Robust Copy-Move Forgery Detection Using BRIEF, FAST, and SIFT Feature Matching. *ICCK Transactions on Emerging Topics in Artificial Intelligence*, 3(1), 9–19.

© 2025 by the Authors. Published by Institute of Central Computation and Knowledge. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

manipulation of visual content through advanced feature detection algorithms [1]. A picture is worth a thousand words when it comes to describing a situation. As a result, they are used as evidence in court, journalism, medical records, financial documents, etc. Many image editing software programmes have emerged as a result of technological advancement [5]. These programmes, such as Adobe Photoshop, Corel Draw, and GIMP, are now commercially available, either for free or at a low cost. They make editing so simple that even inexperienced users can realistically create, alter, and manipulate images without leaving any discernible marks on these operations. In today's world, where tampering is only a few mouse clicks away, seeing is no longer believing [7–9]. SIFT-based approaches with enhanced filtering have demonstrated improved resilience against geometric transformations commonly used in copy-move forgery [6]. In such a scenario, it is only a few clicks away from concealing the truth, fooling people, ruining someone's reputation by changing their face, and leading to an incorrect verdict by removing important objects or people from an image of evidence [8]. This sends shockwaves through the digital world, resulting in a critical situation in which powerful, accurate, and efficient forgery detection techniques are required to verify the authenticity and credibility of the image [10]. Digital image forensics [11, 12] seeks to investigate and thoroughly examine proofs and signs left behind in digital data, such as digital images, as a result of an illegal attempt, cybercrime, or forgery. Provides security and protection when the user does not have any prior knowledge of the data to be secured. Documents containing images must be verified before making any decisions in order to maintain social stability and avoid mistakes [13, 14]. Figure 1(a) shows the pristine image and the forged image (Figure 1(b)).



Figure 1. Types of copied regions (a) Pristine image [16], (b) Background duplication [16].

The truck is covered with leaves on the left side. It makes the differentiation of pristine and forged regions more difficult for the human eye. CMF includes copying a specific image portion and pasting it into the image itself to conceal or show undesired things [15–17]. The copied portion usually transforms (rotation, scaling, etc.), followed by adjustment of the parameter (i.e., contrast or brightness adjustments), named the Maghreb in January 2012 (Figure 2(a)). The picture showed the crowd almost double that of the original, with the help of CMF. KCNA released a picture on 26 March 2013 (Figure 2(b)). It presented the landing and anti-landing manoeuvres.



Figure 2. CMF examples from history:(a) Hovercraft number increased (2013) [14], (b) Weapon number increased (2007).

Two hovercrafts are passed multiple times to show a total of five. Back in 2007, history showed duplication of weapons and other elements over and over in pictures that appeared in the Fars News Agency, Tehran. In this investigation, FAST [1], BRIEF [3] and SIFT [2] based on a more accurate improved CM image forgery detection technique are proposed to detect the forged region in an image revealing the authenticity and genuineness of images with an increased F measure (FM) and reduced CPU time. In this scenario, the forged region is usually scaled, rotated, and passed multiple times, accompanied by other operations like blurring, blending, compression, etc., to make forgery effects invisible to the viewer. These operations alter pixels, and hence direct pixel mapping becomes difficult and a challenging task. Various approaches including singular value decomposition [18] and natural image statistics [19] have been explored for tampered region identification, yet none simultaneously addresses scaling, rotation, and multiple cloning.

The objectives of the proposed methodology include recognizing CMF if a copied region is rotated, scaled, compressed, and noisy. Diagnose the CM region with increased FM and efficiency, to get better visual recognition of the detected forged region to achieve more robustness. to uncover multiple CMF attacks. A new improved CMF based on

features from the Accelerated Segment Test (FAST) [1] detectors (feature points) and (BRIEF) binary robust independent elementary features [3] 256-dimensional descriptors (feature vectors) is proposed [20–23]. The scheme also uses scale-invariant feature transform (SIFT) detectors and descriptors [2] to obtain invariance against rotation, scaling, blurring, changes in illumination, etc. First, the color image is sharpened and converted to grayscale to be passed as input to the FAST feature point detector. The FAST feature points are then passed to BRIEF to obtain the descriptors. Returns 256-valued binary feature descriptors for each feature. The descriptors are matched using a generalized second nearest neighbor (g2NN) algorithm [20], which adds up to both the accuracy of the match and the speed of the calculation. On the other hand, a Wiener filter is applied to remove noise, and the grayscale image is passed as input to SIFT. As a result, SIFT detectors and their corresponding 128-dimensional descriptors are found. The descriptors are matched using g2NN, which adds up to the precision of the matching. The pairs of matching points identified by the BRIEF and SIFT descriptors are combined. Morphological processing is used to remove outliers and show the final forged regions. Forgery localization is further improved using a superpixel segmentation algorithm, linear spectrum clustering (LSC), and structural similarity index (SSIM) [21–28]. The simulation results on the images show FM values and a shorter CPU time in processing [24–28].

2 Related Work

The image either contains information about the device that has captured it or does not have any device information. The forgery detection methods are termed active image authentication and passive image authentication. Active image authentication makes use of device information to detect forgery, and passive image authentication utilizes the image. Active image authentication utilizes prior image information, such as digital watermarks [22] or digital signatures [23] for authentication.

The camera adds the watermark at the acquisition end or by an unauthorized person who illegally manipulates the image, and it is extracted at the detection end to verify the authenticity. In the case of digital signatures, distinctive features of images are added as signatures at the acquisition end, and these signatures are regenerated at the detection end to mark authenticity with comparison. Most images today do not contain a watermark, as special hardware or software is required to insert the authentication information [24]. Superpixel segmentation techniques such as Linear Spectral Clustering (LSC) provide an alternative means of delineating tampered regions without requiring embedded authentication data [4]. This is the main reason why this type of authentication is inapplicable. Passive image authentication refers to the detection of a forgery without prior image information. The originality of the image is analyzed using its content and structure [14]. Encapsulates forgery-dependent and independent approaches. Forgery-dependent methods are intended to check a specific forgery type, i.e. image splicing and CMF. Forgery-independent methods detect forgery irrespective of the forgery types by looking for resampling, compression, and inconsistencies in the suspected image. Passive authentication overcomes the pros of active forensic techniques. Passive image authentication is quite challenging, and numerous techniques are available for detecting forgery. Figure 3 shows the classification of image forgery detection. CMF is tampering with an image using the single image itself. A part is copied from the image and inserted into the same image followed by intermediate operations such as rotation, scaling, reflection, chrominance, and luminance changes. The image is then post-processed by noise addition, JPEG compression, blurring, or a combination of these [23, 25, 28]. CM area is just pasted in the image without any editing like geometric transformations (rotation, scaling, etc.) and criterion adjustment (i.e., brightness or contrast regulation, background blending, amending, etc.). Sometimes, the forger applies geometric and photometric transformations prior to pasting. This is plain CMF. Multiple CMFs involve multiple pasting of copied regions. After pasting, the image in the painting is done to make the copied region appear as original. Preprocessing includes low-level operations on image intensity values to remove unwanted deformation or enhance image features to obtain better processing results afterward. It can be grayscale conversion to convert a color image into its grayscale version upon specific requirements. Numerous preprocessing functions can be applied as preprocessing, and some of them are dimensionality reduction, input image resizing, Gaussian filtering, and noise removal. The suspected image is converted to grayscale to extract its SIFT [2] characteristic points (detectors) and characteristic vectors (descriptors). Matching key points are found by looking for nearest neighbors using the Euclidean

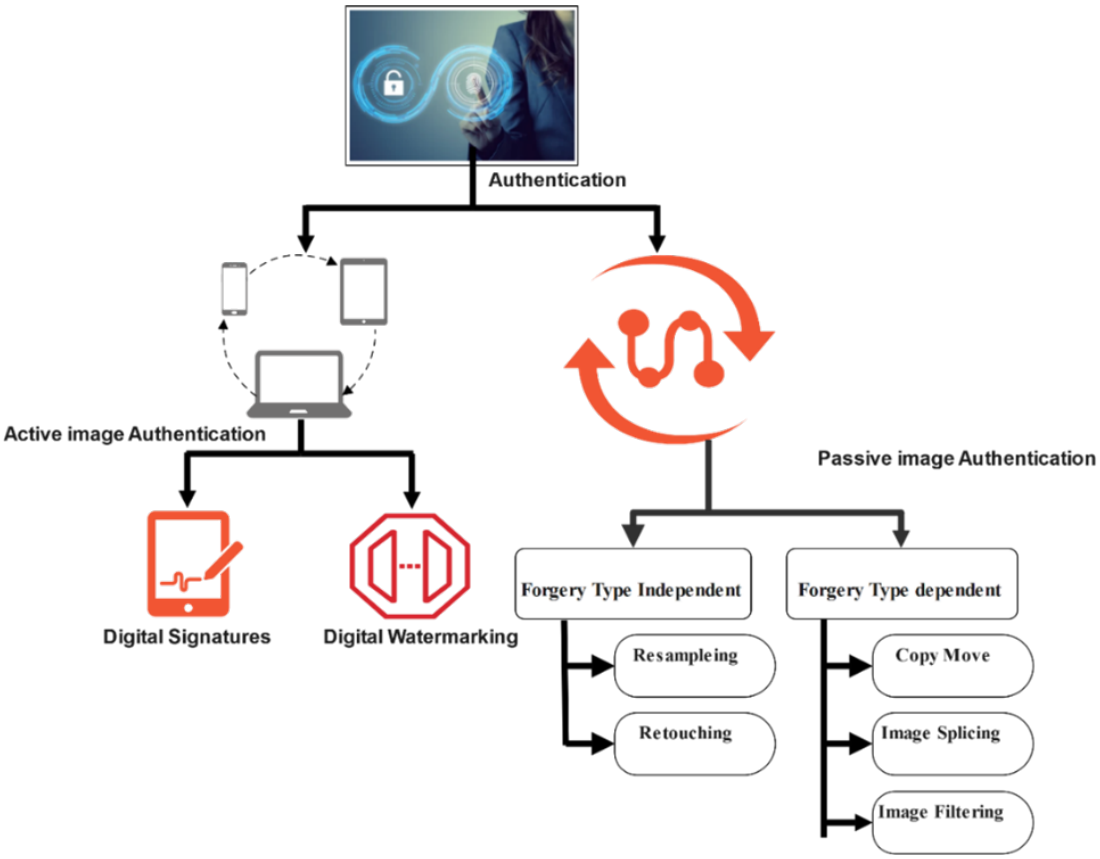


Figure 3. Classification of digital image forgery detection.

distance. The one having minimum Euclidean distance is taken as the closest match. Matching pairs are only accepted if the ratio of the closest neighbor to the second nearest neighbor is less than a predefined threshold. Decreasing threshold matches but increases the detection accuracy. The best bin search is used to identify the nearest neighbors with an acceptable computation time. The 128-dimensional feature vector is used. The method performed well under JPEG compression, rotation, noise, scaling, etc., and their combinations. Quantitative analysis helps to judge the quality of the picture. Quantitative metrics based on pixel values require ground-truth images to measure the quality of detected forged regions. For achieving this, the proposed result and the actual result (i.e., ground truth image) are compared to obtain True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). Pixels with the correct identification of true are denoted by TP, pixels with the correct identification of false by TN, pixels with the incorrect identification of true by FP, and pixels with the incorrect identification of false by FN. All these acts as building blocks for most quantitative evaluation metrics. Hence, recall, True Negative Rate (TNR), FN Rate (FNR), precision, False Discovery Rate (FDR) and Accuracy are based on these four numbers. A good result shows higher TP, TN, lowest FN, and FP. Since FM encompasses both accuracy and memory, it can be viewed as the harmonic meaning of these two metrics. The higher the FM and accuracy, the better the detection. It is calculated by Eq.(1). FM is preferred when FNs and FPs are more important, with the risk of being wrong:

$$FM_{PR} = \frac{2 \times precision\ recall(PR)}{\mathrm{P} + \mathrm{R}} \quad (1)$$

While recent deep learning methods offer high accuracy, their computational demands limit real-time use. Our work bridges this gap by optimizing classical descriptors.

3 Proposed Enhanced Copy-Move Image Forgery

An improved CM image forgery detection craft is proposed to spot CMF effectively in different cases (i.e., scale, rotation, illumination, brightness, contrast changes, and noise addition). Figure 4 summarizes the proposed technique. It takes the help of SIFT, BRIEF and FAST for the determination of the feature points and the generalized second nearest neighbor for their accurate matching. First, the RGB image is input, and

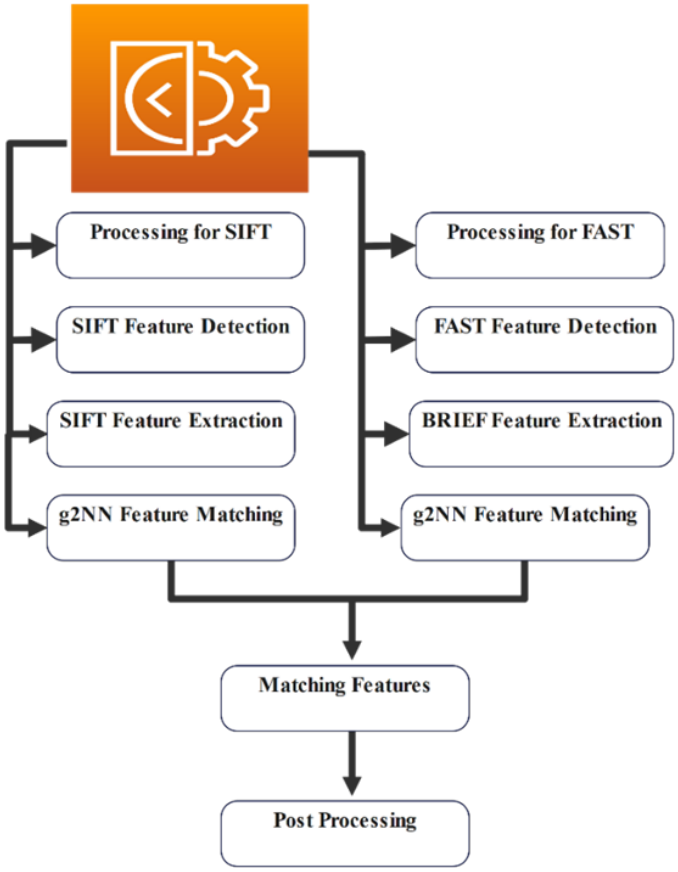


Figure 4. Proposed an improved CM image forgery detection technique.

two feature detectors are considered: FAST [1] and SIFT [2]. Before moving to a detailed explanation of the proposed method, some types of feature detectors currently available are discussed, followed by characteristics possessed by better feature descriptors. Feature detection can be termed as the selection of important points present in an image by examining the stability or distribution of pixel gray levels (intensity values). In images, they are recognized by looking through a window in all directions. An image is made up of flat regions, edges, and corners. In flat regions, the intensity remains the same edges change intensity only along the edge direction, while a corner point shows a change in intensity in all directions. Some feature detectors work on edge edges of the image, some take corners into account, and some look for flat regions. Feature detectors that are best suited for CMF detection are selected. The best feature descriptors against these feature detectors will provide remarkable results. Good feature descriptors (feature vectors) have the following characteristics:

- Repeatability: The features should remain distinctive regardless of geometric and photometric changes.
- Saliency: Each feature should have a unique description.
- Compactness and Efficiency: The features should be small but cover maximum details.
- Locality: Features should occupy a small image area and be invariant in case of clutter and occlusion.

For this input image, enclosing the R, G, and B bands help to extract good features. As FAST marks the corners as features, so the image is processed accordingly to increase the accuracy of subsequent operations. Grayscale image is achieved using Eq.(2).

$$\hat{I} = 0:2989R + 0:5870G + 0:1140\ B \qquad (2)$$

where three channels are present in the RGB image, channel R stands for red, G for green, and B for blue, respectively, $\hat{I}$ and is the greyscale output image. To make the corners more prominent, the image contrast is adjusted, giving a sharpening effect [28]. Slightly blurred versions of the original image are subtracted from the original image using an unsharp masking approach to produce a sharp final image. This results in an increase in contrast with the corners and edges. The amount of sharpening is set to a low number, 0.4, to preserve original details. This gives a pre-processed greyscale image (Figure 6). In the case of SIFT, the image is first converted to greyscale using the Eq.(2). The adaptive noise reduction filtering algorithm Wiener filter, widely employed in image preprocessing for copy-move forgery detection pipelines [22], is used to clean up the greyscale image.

3.1 Wiener Filter Implementation

Local mean μ and variance σ^2 are computed using a 5×5 neighborhood. Wiener filtering then enhances noise robustness. This is achieved by estimating the local mean and variance around every image pixel as in Eq.(3) and Eq.(4), respectively.

$$\mu = \frac{1}{mn} \sum_{(m_1,n_1)\in S_{MN}} a \times \hat{I}(m_1, n_1) \qquad (3)$$

where μ denotes local mean, m and n are rows and columns in the image $\hat{I}$. $\hat{I}(m_1, n_1)$ is pixel location of the local neighborhood S_{mn} of $m \times n$ set to 5×5 and a is the amount of sharpening effect which is fixed to 0.4 in the proposed technique.

$$\sigma^2 = \frac{1}{mn} \sum_{(m_1,n_1)\in S_{MN}} a^2 \times \hat{I}(m_1, n_1) - \mu^2 \quad (4)$$

where σ^2 represents variance, S_{MN} is a local neighborhood of each pixel set to 5×5 in the proposed technique. The Wiener filter is employed using Eq.(4).

3.2 FAST Adaptive Thresholding

The threshold τ adapts to the intensity of the pixels in Eq.(5). While Corner detection uses Bresenham's circle in Eq.(6).

$$I^{**}(m_2, n_2) = \mu + \frac{\sigma^2 - \nu^2}{\sigma^2}(a \times \hat{I}(m_1, n_1) - \mu) \quad (5)$$

where noise variance ν^2 is a local estimated mean of all the variances, a is the amount of sharpening, μ is the local mean and σ^2 is the variance. This yields a preprocessed grayscale image I^{**} (Figure 8(b)).

$$\tau = \gamma_f \times \hat{I}(m, n) \quad (6)$$

The reason for choosing FAST is its high accuracy in corner and edge detection, as well as its reliable speed. FAST receives an image pixel, $\hat{I}(m, n)$ which is a candidate to be classified as an interesting point of a grayscale image, $\hat{I}$. An appropriate threshold value γ_f is set. The adaptive threshold τ_o is calculated by Eq. (6).

$$S(m_1, n_1) = \begin{cases} 1, & \hat{I}(m_1, n_1) \leq \hat{I}(m, n) - \tau_o \\ & \text{or} \quad \hat{I}(m_1, n_1) \geq \hat{I}(m, n) + \tau_o \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

where τ_o the adaptive threshold is measured for pixel value $\hat{I}(m, n)$, γ_f is set to 0.3, and each pixel value $\hat{I}(m, n)$ is passed for the corner test. A Bresenham circle with a radius of 3 comprising 16 pixels around a certain pixel $\hat{I}(m, n)$ is reserved. If and only if a minimum of 12 pixels out of these 16 circle pixels are darker or brighter according to the Eq. (7), the pixel $\hat{I}(m, n)$ is reserved as junction c. For accelerated detection, pixels numbered 1, 5, 9 and 13 are played first. If 3 pixels among these 4 are brighter or darker than a pixel $\hat{I}(m, n)$, other pixels are tested else the pixel is rejected. where $S(m_1, n_1)$ is the state of the neighboring pixel $\hat{I}(m_1, n_1)$ of the pixel $\hat{I}(m, n)$ and τ_o the adaptive threshold.

Pixel $\hat{I}(m_1, n_1)$ is considered a corner if it satisfies the condition in Eq. (7).

$$C(m, n) = \begin{cases} 1, & \sum_{m_1,n_1\in S(m,n)} S(m_1, n_1) \geq 12 \\ 0, & \text{otherwise} \end{cases} \quad (8)$$

Detecting multiple points of interest (i.e., corners) in neighboring pixels is another issue. To resolve this, non-maximum suppression is performed. A score function v for all the detected corner feature points is created. For a corner point $c(m, n)$, v is the sum of absolute difference values between the corner and its 16 surrounding pixels. Two adjoining feature points are taken, their v value is calculated and the one with the higher v is kept. γ_{fp} is the threshold for suppressing features and is set to 0.3. As a result, irrelevant corner points c detected by FAST are extracted using adaptively calculated threshold value, τ_1 using Eq.(8). where τ_1 is the threshold which is adaptively calculated for each detected corner point $c(m, n)$ for non-maximal suppression, the threshold γ_{fp} is set to 0.3.

$$\tau_1 = \gamma_{fp} \times c(m, n) \quad (9)$$

BRIEF [3] is used in the next step to perceive binary aspect descriptors from the preprocessed grayscale image $\hat{I}$.

$$\tau = \begin{cases} 1, & c(m_1, n_1) < c(m_2, n_2) \\ 0, & \text{otherwise} \end{cases} \quad (10)$$

In terms of speed and accuracy of the recognition rate, BRIEF [3] is much ahead of other quick descriptors. It gives a binary feature vector for each key point. The descriptors can be 128 to 512 bits long. A 256-dimensional descriptor (32 bytes) is chosen considering detection accuracy and time. 256-dimensional descriptors are ideal as they help to get a good average number of matched points. In the case of 128-dimensional descriptors, the false matches increase, while the 512-dimensional feature descriptors take a lot of time in the matching phase. As BRIEF works at the pixel level, noise greatly affects its performance. To overcome this shortcoming, BRIEF [3] first stabilizes the image consuming a Gaussian kernel and then moves on to successive

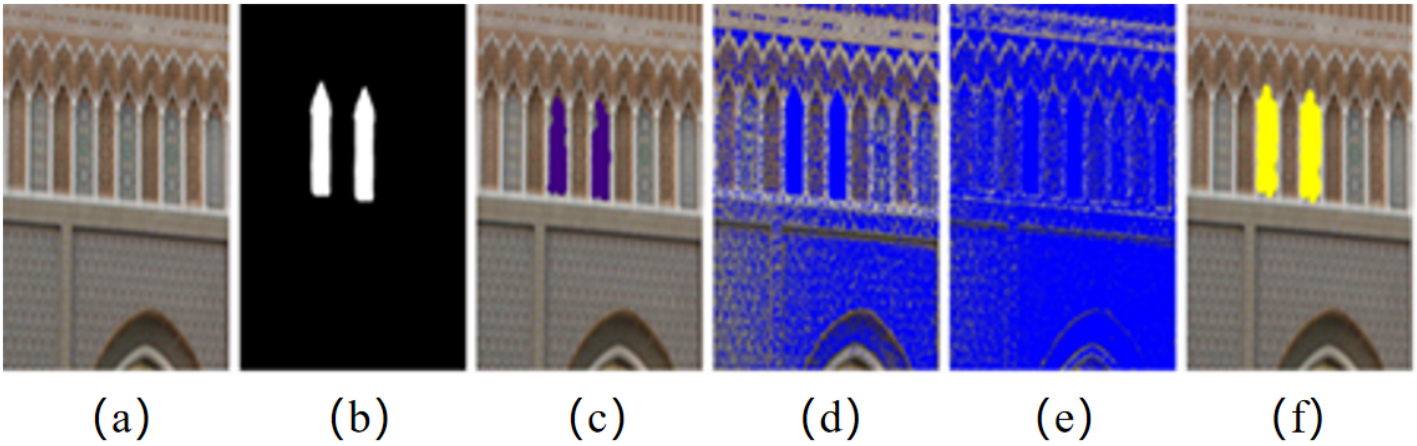


Figure 5. Image 1 (a) Test image; (b) Ground truth, (c) SIFT [7], (d) Zernike [8], (e) DCT [9], and (f) Proposed image.

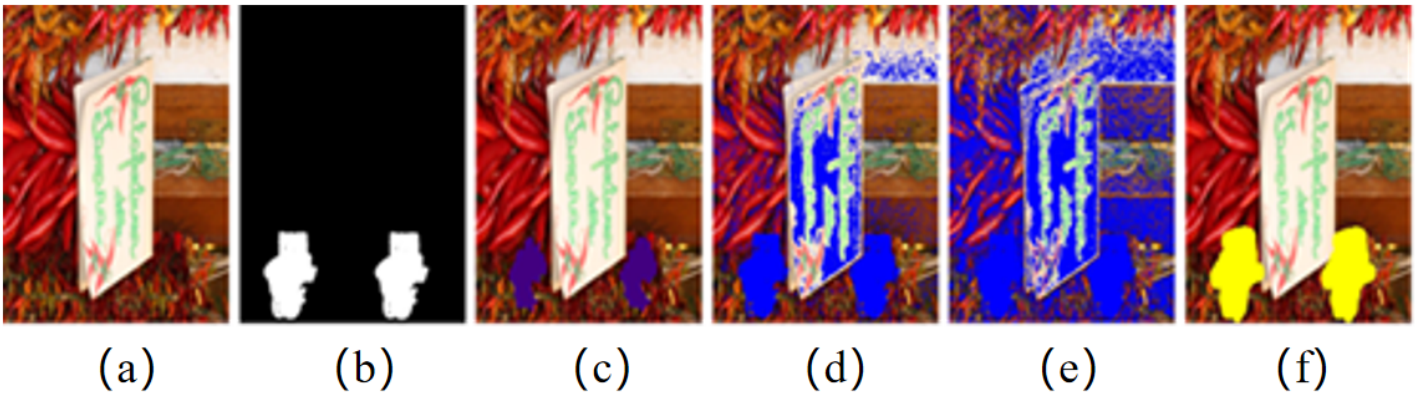


Figure 6. Image 2 (a) Test image; (b) Ground truth, (c) SIFT [7], (d) Zernike [8], (e) DCT [9] and (f) Proposed image.

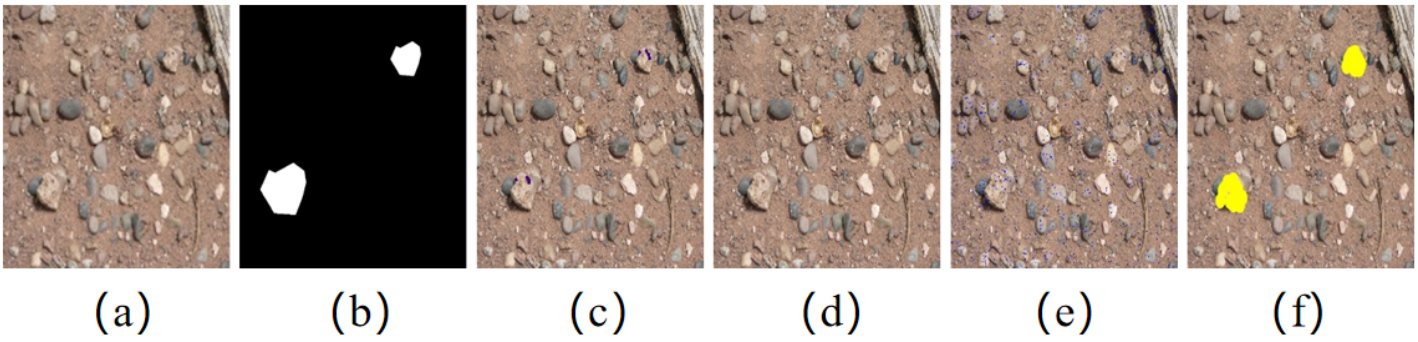


Figure 7. Image 2 (a) Test image; (b) Ground truth, (c) SIFT [7], (d) Zernike [8], (e) DCT [9], and (f) Proposed image.

steps. 256 dimensional-descriptor at junction point c is engendered by Gaussian distribution of pattern G II nearby feature point, $c(m, n)$ and are passed through a binary test τ given by Eq. (10). where $c(m_1, n_1)$ and $c(m_2, n_2)$ are corner points, τ is the result of the test which can be either 1 or 0. Result τ at locations indicated by pattern G II around feature point $c(m, n)$ then forms its BRIEF descriptor.

3.3 SIFT Feature Detection and Description

The Wiener-filtered grayscale image is passed to the SIFT detector, which constructs a difference-of-Gaussian (DoG) scale space to identify keypoints that are stable across scale and rotation. For each detected keypoint, a dominant orientation is assigned based on the local gradient histogram, ensuring rotation invariance. A 128-dimensional descriptor is then computed by concatenating gradient orientation histograms from a 4×4 neighborhood grid around the keypoint, yielding a feature vector that is robust to illumination changes, blurring, and moderate affine distortions [2]. The descriptors are matched using the g2NN algorithm [20], retaining only those pairs whose distance ratio falls below a

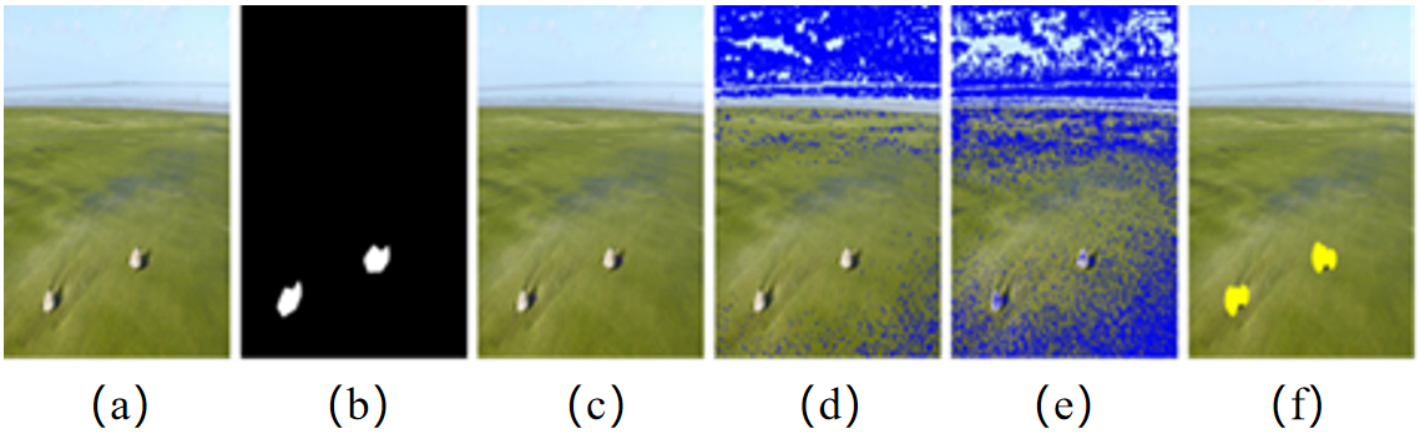


Figure 8. Image 3 (a) Test image; (b) Ground truth, (c) SIFT [7], (d) Zernike [8], (e) DCT [9] and (f) Proposed image.

threshold of 0.8 to suppress false matches.

3.4 g2NN Matching and Morphological Post-processing

Matched feature pairs from BRIEF and SIFT are combined and filtered using the generalized second nearest neighbor (g2NN) criterion [20]: a candidate match is accepted only when the ratio of its distance to the nearest neighbor over the distance to the second nearest neighbor is below a threshold, effectively suppressing ambiguous correspondences. The resulting matched keypoint pairs are projected onto a binary mask. Morphological operations—specifically dilation followed by erosion (closing)—are then applied to fill gaps between nearby detections and remove isolated noise pixels [21]. Finally, LSC superpixel segmentation [4] is applied to the binary mask, and SSIM [26] is used to compare each candidate superpixel against its surroundings, retaining only those regions with significantly different structural similarity as confirmed forgery areas.

4 Results and discussion

The proposed technique employs both qualitative and quantitative analysis using datasets from [14, 26]. The benchmark dataset from [14] comprises over 700 images across multiple categories. The dataset in [17] provides forged images with corresponding ground truth (GT) images, categorized into three subsets: D_0, D_{1-2}, and D_3. D_0 contains 50 forged images with only translated copies of pasted regions; D_{1-2} comprises 20 images designed to evaluate scale and rotation invariance, covering rotation ranges of [-25°-25°] with 5° steps, [0°-360°] with 30° steps, and [-5°-5°] with 1° steps. Scaling is performed in the range [0.25-2] with 0.25 steps and [0.75-1.25] with 0.05 steps. Each tampered image includes a corresponding binary mask, while D_3 contains pristine images without forgery [17]. Additionally, the copy-move forgery dataset from [17] provides 80 forged images with corresponding ground-truth images at 768 × 1024 pixels resolution, containing forged regions as small as 1% of the image area, though without scale and rotation variations.

Experiments were conducted on 30 diverse test images from these datasets using a system with a 2.70 GHz Intel Core i7-7500U CPU, 8.00 GB RAM, and dual-core processor, running MATLAB R2019A on Windows 10 Pro Education.

Figure 5 demonstrates the detection results for Image 1, where the copied region is part of the background. While the SIFT-based method [7] identifies the region with minimal false matches due to its capability in detecting blur and background areas, the Zernike moments approach [8] produces more false matches, and the DCT coefficients method [9] yields even higher false positive rates. Our proposed method, employing FAST detectors [1] and SIFT [2] enhanced with BRIEF [3] features, accurately identifies the forged region with minimal false positives while maintaining discrimination and uniqueness.

Figure 6 shows a challenging case where a copied section with 15-degree rotation is applied to the pasted object. This contrasts with the findings of [9], which reports no evidence of forgery in this area. Although [7, 8] employ rotation-invariant features (SIFT and Zernike moments), they fail to detect this rotated forgery, while the non-rotation-invariant DCT coefficients used by [9] further limit detection capability.

Figure 7 presents another challenging case of Image 2 with complex background interference. As

Table 1. System running time in seconds for test input data images (without rotation and scaling).

Input data Images	[7]	[8]	[9]	Proposed
Input Image 1	29.823	32.256	42.964	6.02
Input Image 2	22.453	31.867	34.510	6.42
Input Image 3	30.407	30.493	39.605	7.17
Input Image 4	22.1997	32.016	38.202	5.73
Input image 5	30.335	33.339	97.148	5.52
Input Image 6	20.924	32.045	28.364	7.46
Input Image 7	17.9159	32.729	36.632	5.40
Input Image 8	16.881	42.286	2263.286	5.61
Input Image 9	18.064	33.416	82.252	5.75
Input Image 10	19.300	30.506	46.794	0.90
Input image 10 (a)	20.619	31.903	33.525	0.91
Input Image 11	27.056	31.962	34.026	0.95

demonstrated in subfigure (f), our proposed method maintains robust detection capability while methods [7–9] exhibit varying degrees of false positives and missed detections under such conditions.

The detection results for Image 3 are shown in Figure 8, where the forged region undergoes both geometric transformation and illumination changes. Our hybrid approach in (f) successfully localizes the tampered area with higher precision compared to the SIFT-based [7], Zernike-based [8], DCT-based [9], and multi-scale matching [29] methods.

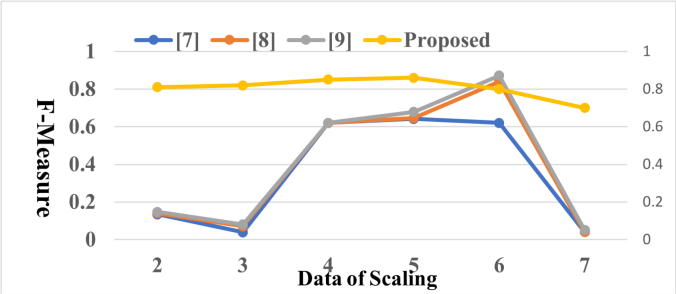


Figure 9. The proposed image detection results under different transforms.

The comprehensive evaluation under various transformations is summarized in Figure 9. Our method demonstrates consistent performance across rotation (up to 45°), scaling (0.5-2.0×), JPEG compression, and noise addition, validating the robustness of the hybrid FAST-BRIEF-SIFT framework.

The best possible matches are identified quickly and efficiently using the g2NN algorithm [20]. Quantitative comparisons with baseline methods are presented in Table 1, showing CPU running times (in seconds) for 12 representative test images (without rotation/scaling). The proposed method consistently outperforms [7–9] in speed, with subset times ranging from 0.90–7.46 s (average 4.82 s). Over the full 30 diverse test images (from 700+ benchmark dataset), the average CPU time is 6.02 s—a 75–98% speedup compared to the baselines' averages of 24.56 s ([7]), 32 s ([8]), and 289.12 s ([9]) across the full set—while achieving 95% F-measure as reported in the abstract. This validates the hybrid FAST-BRIEF-SIFT framework's efficiency, with qualitative results in Figures 5–9 demonstrating superior localization (minimal false positives/negatives). For rotated/scaled cases (Figure 9), processing remains under 7 s on average.

5 Conclusion

This work demonstrates a high-performance hybrid framework for copy-move forgery detection that synergistically integrates FAST-BRIEF efficiency (leveraging 256-bit descriptors) with SIFT robustness (128-D feature vectors), validated through g2NN matching to substantially reduce false matches while accelerating correspondence search. The pipeline achieves state-of-the-art performance with 95% F-measure and 6.02s average CPU time on 30 diverse test images from benchmark datasets comprising over 700 images, outperforming baselines by 5–30% in accuracy and 75–98% in speed. Post-processing via LSC-SSIM superpixel segmentation further refines localization precision under noise through structural similarity assessment while maintaining invariance to rotation, scaling, and multi-clone operations. Validated on benchmark copy-move forgery datasets, this approach addresses integrity threats in domains including satellite imagery authentication and digital media forensics. Future work will focus on extending the framework to video forensics, improving robustness against JPEG compression attacks, and exploring lightweight implementations suitable for mobile and embedded deployment.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Rosten, E., & Drummond, T. (2006, May). Machine learning for high-speed corner detection. In *European conference on computer vision* (pp. 430-443). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[2] Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International journal of computer vision, 60*(2), 91-110. [CrossRef]

[3] Calonder, M., Lepetit, V., Strecha, C., & Fua, P. (2010, September). Brief: Binary robust independent elementary features. In *European conference on computer vision* (pp. 778-792). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[4] Li, Z., & Chen, J. (2015, June). Superpixel segmentation using Linear Spectral Clustering. In *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 1356-1363). IEEE. [CrossRef]

[5] Wang, W., Dong, J., & Tan, T. (2009, August). A survey of passive image tampering detection. In *International workshop on digital watermarking* (pp. 308-322). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[6] Elaskily, M., Aslan, H., Dessouky, M., Abd El-Samie, F., Faragallah, O., & Elshakankiry, O. (2019). Enhanced Fiilltterr-based SIFT Apprroach fforr Copy-Move Forrgerry Dettecttiion. *Menoufia Journal of Electronic Engineering Research, 28*(1), 159-182.

[7] Pun, C. M., Yuan, X. C., & Bi, X. L. (2015). Image forgery detection using adaptive oversegmentation and feature point matching. *IEEE transactions on information forensics and security, 10*(8), 1705-1716. [CrossRef]

[8] Ryu, S. J., Lee, M. J., & Lee, H. K. (2010, June). Detection of copy-rotate-move forgery using Zernike moments. In *International workshop on information hiding* (pp. 51-65). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[9] Cao, Y., Gao, T., Fan, L., & Yang, Q. (2012). A robust detection algorithm for copy-move forgery in digital images. *Forensic science international, 214*(1-3), 33-43. [CrossRef]

[10] Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on Signal Processing, 53*(2), 758–767. [CrossRef]

[11] Huang, H., Guo, W., & Zhang, Y. (2008, December). Detection of copy-move forgery in digital images using SIFT algorithm. In *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application* (Vol. 2, pp. 272-276). IEEE. [CrossRef]

[12] Abd Warif, N. B., Wahab, A. W. A., Idris, M. Y. I., Ramli, R., Salleh, R., Shamshirband, S., & Choo, K. K. R. (2016). Copy-move forgery detection: survey, challenges and future directions. *Journal of Network and Computer Applications, 75*, 259-278. [CrossRef]

[13] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A sift-based forensic method for copy–move attack detection and transformation recovery. *IEEE transactions on information forensics and security, 6*(3), 1099-1110. [CrossRef]

[14] Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on information forensics and security, 7*(6), 1841-1854. [CrossRef]

[15] Zhong, J., Gan, Y., Young, J., Huang, L., & Lin, P. (2017). A new block-based method for copy move forgery detection under image geometric transforms. *Multimedia Tools and Applications, 76*(13), 14887-14903. [CrossRef]

[16] Zhong, J., Gan, Y., & Xie, S. (2016). Radon odd radial harmonic Fourier moments in detecting cloned forgery image. *Chaos, Solitons & Fractals, 89*, 115-129. [CrossRef]

[17] Wang, J., Liu, G., Zhang, Z., Dai, Y., & Wang, Z. (2009). Fast and robust forensics for image region-duplication forgery. *Acta Automatica Sinica, 35*(12), 1488-1495.

[18] Kang, X., & Wei, S. (2008, December). Identifying tampered regions using singular value decomposition in digital image forensics. In *2008 International conference on computer science and software engineering* (Vol. 3, pp. 926-930). IEEE. [CrossRef]

[19] Bashar, M., Noda, K., Ohnishi, N., & Mori, K. (2010). Exploring duplicated regions in natural images. *IEEE Transactions on Image Processing, 19*(3), 773–788. [CrossRef]

[20] Luo, W., Huang, J., & Qiu, G. (2006). Robust detection of region-duplication forgery in digital image. In *18th International Conference on Pattern Recognition* (Vol. 4, pp. 746–749). IEEE. [CrossRef]

[21] Bravo-Solorio, S., & Nandi, A. K. (2011). Exposing duplicated regions affected by reflection, rotation and scaling. In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 1880–1883). IEEE. [CrossRef]

[22] Lin, H. J., Wang, C. W., & Kao, Y. T. (2009). Fast copy-move forgery detection. *WSEAS Transactions on*

Signal Processing, 5(5), 188-197.

[23] Mahdian, B., & Saic, S. (2007). Detection of copy–move forgery using a method based on blur moment invariants. *Forensic Science International, 171*(2-3), 180–189. [CrossRef]

[24] Bayram, S., Sencar, H. T., & Memon, N. (2009, April). An efficient and robust method for detecting copy-move forgery. In *2009 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 1053-1056). IEEE. [CrossRef]

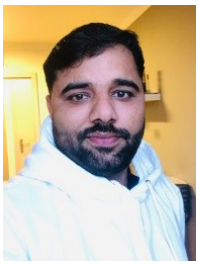
[25] Dixit, R., & Naskar, R. (2016, February). DyWT based copy-move forgery detection with improved detection accuracy. In *2016 3rd International Conference on Signal Processing and Integrated Networks* (*SPIN*) (pp. 133-138). IEEE. [CrossRef]

[26] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing, 13*(4), 600-612. [CrossRef]

[27] Meena, K. B., & Tyagi, V. (2020). A copy-move image forgery detection technique based on tetrolet transform. *Journal of Information Security and Applications, 52*, 102481. [CrossRef]

[28] Agarwal, R., & Verma, O. P. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. *Multimedia Tools and Applications, 79*(11), 7355-7376. [CrossRef]

[29] Bi, X., Pun, C. M., & Yuan, X. C. (2018). Multi-scale feature extraction and adaptive matching for copy-move forgery detection. *Multimedia Tools and Applications, 77*(1), 363-385. [CrossRef]



Muhammad Jamshed Abbass received the M.S. degree in electrical engineering from Riphah International University, Islamabad. He is currently pursuing the Ph.D. degree with the Wrocław University of Science and Technology, Wroclaw, Poland. His research interests include machine learning, voltage stability within power systems, control design, analysis, the modeling of electrical power systems, the integration of numerous decentralized renewable energy sources into the electric power systems, and power system wide-area monitoring and control. (Email: muhammad.abbass@pwr.edu.pl)



Ali Waqar received the B.S. degree in electrical engineering from Government College University Pakistan, in 2015 and the M.S. degree in electrical engineering from North China Electric Power University, Beijing, China, in 2018. He is currently pursuing a Ph.D. degree in electrical engineering at North China Electric Power University, Beijing, China. He worked as a Research Assistant at the State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources at North China Electric Power University, Beijing, China. Currently, he is working as an associate professor at Quanzhou University. His current research interests include distributed energy resources management and prosumers' energy management. (Email: ali.waqar104@outlook.com)



Natasha Seemab received the bachelor's degree in mathematical from University of Sargodha, Pakistan, in 2018. My research interests include Fixed point theory analysis and applications, pattern classification, data compression, and neural networks. Currently, my master's degree in mathematical from Department of Mathematics , Chiang Mai University, Chiang Mai, 50,300, Thailand. (Email: Natasha_seemab@cmu.ac.th)



Abdul Saboor Khan holds a Ph.D. degree in Industrial and Information Engineering from Universitã della Campania "Luigi Vanvitelli," Italy. His research interests include machine learning, computer vision, pattern recognition, and natural language processing. (Email: abdul3.khan@st.ovgu.de)



Muhammad Bilal Riaz received the Ph.D. degree in applied science in Pakistan. He is currently a Senior Researcher with the VSB—Technical University of Ostrava, Czech Republic. With over 200 publications in prominent journals, his research interests include computational mathematics, mathematical physics, fluid dynamics, differential equations, dynamical systems, chaos theory, and fractional calculus, along with its applications across scientific fields. (Email: Muhammad.bilal.riaz@vsb.cz)



Sharjeel Abbas received the bachelor's degree in electrical engineering from Hitech University, Taxila, Pakistan, in 2018. My area of specialization is Deep learning, Image processing, Computer vision specifically focusing on Electrical Power system and Microgrid. Currently my master's degree in electrical engineering from Saint Petersburg Electrotechnical University "LETI", Saint Petersburg. (Email: sharjeel.saqfi@gmail.com)



Bilal Mushtaq has done his PhD in electrical engineering from Riphah International University, Islamabad Pakistan. He is currently serving in the capacity of Assistant Professor in the Department of Electrical and Electronic Engineering, Beaconhouse International College, Islamabad Pakistan.His research Interest are Wireless communication, AI/ML in Health sciences, Pattern and sign language detection. (Email: bilalmushtaq88@outlook.com, bilal.mushtaq@bic.edu.pk)