RESEARCH ARTICLE

Passive Image Forgery Detection Using Multiscale Weber Local Descriptor and SVM Classification

Aamir Ali[1], **Aamir Raza**[2], **Khaleelullah Syed**[3], **Swetank Mohan**[4], **Nikhat Fatima**[5], **Muhammad Umar**[6] **and Misbah Ali**[1,*]

[1] Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Sahiwal 57000, Pakistan
[2] Department of Information Technology and Management, Illinois Institute of Technology, Chicago, IL 60616, United States
[3] Hellenic American University, Nashua, NH 03063, United States
[4] The University of Texas Rio Grande Valley, Edinburg, TX 78539, United States
[5] Concordia University, Mequon, WI 53097, United States
[6] University of Management and Technology, Lahore 54770, Pakistan

Abstract

Digital image manipulation has become increasingly prevalent with the widespread availability of editing tools, raising concerns regarding image authenticity in critical applications. This study presents a passive image forgery detection framework based on multiscale Weber Local Descriptor features extracted from chrominance components and classified using a Support Vector Machine. The proposed method operates without embedded authentication information and focuses on detecting both copy-move and splicing forgeries through texture-based analysis. Experiments were conducted on two benchmark datasets, CASIA v2.0 and MICC F2000, using ten-fold cross-validation. On the CASIA v2.0 dataset, the framework achieved an overall classification accuracy of 97.0%, with a true positive rate of 98.4% for spliced images and an area under the ROC curve of 0.98. On the MICC F2000 dataset, the framework achieved an overall accuracy of 97.4%, with a true positive rate of 99.7% for copy-move forgery detection and an AUC value of 0.98. The results indicate consistent classification performance across different manipulation types and dataset characteristics. The use of chrominance channels enables the preservation of subtle manipulation artifacts, while multiscale texture representation enhances feature discrimination. The proposed framework demonstrates competitive performance compared to existing methods while maintaining moderate computational complexity, making it suitable for practical image authentication tasks.

Keywords: digital image forgery detection, passive image authentication, copy-move forgery, image splicing, weber local descriptor, multiscale texture analysis, chroma analysis, support vector machine.

Submitted: 25 March 2026
Accepted: 21 April 2026
Published: 28 April 2026

Vol. 3, **No.** 2, 2026.
10.62762/JIAP.2026.490874

***Corresponding author:**
✉ Misbah Ali
Talktomisbah.ali@gmail.com

Citation
Ali, A., Raza, A., Syed, K., Mohan, S., Fatima, N., Umar, M. & Ali, M. (2026). Passive Image Forgery Detection Using Multiscale Weber Local Descriptor and SVM Classification. *ICCK Journal of Image Analysis and Processing*, 3(2), 69–91.

1 Introduction

Digital images are widely used across communication, journalism, surveillance, and scientific documentation. Their credibility is increasingly questioned. The rapid availability of image editing tools has made manipulation accessible, and visual authenticity can no longer be assumed in many practical scenarios [1]. Image forgery has become a significant concern. It affects legal investigations, media integrity, and public trust [2]. Among various manipulation types, copy-move and splicing are frequently encountered. In copy-move forgery, a region is duplicated within the same image to conceal or replicate objects. In splicing, content from different images is combined to produce a composite scene [3]. Historical records indicate that photographic forgeries were created using manual editing techniques long before the advent of digital tools. These early manipulations demonstrate that concerns regarding image authenticity have existed for decades. With the transition to digital platforms, the complexity and accessibility of such manipulations have significantly increased.

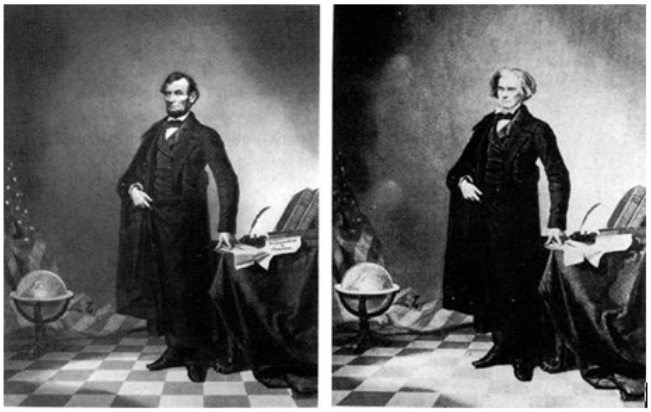

Figure 1. Early example of photographic forgery.

Figure 1 illustrates one of the earliest known instances of image manipulation in photography, where visual content was altered to modify appearance and context. This example illustrates that image manipulation predates digital editing tools. It highlights that visual content can be altered without obvious perceptual artifacts. This motivates the need for intrinsic forensic analysis.

Two main categories of image authentication approaches have been studied. Active methods rely on embedding information such as watermarks or digital signatures at the time of image acquisition. These methods provide controlled verification but require prior modification of the image and specialized acquisition systems. In contrast, passive methods operate without embedded information. They analyze intrinsic image characteristics and attempt to identify inconsistencies introduced during manipulation. Passive techniques are more applicable in real-world scenarios where prior information is unavailable.

Existing passive detection methods have explored different strategies. Block-based approaches analyze overlapping regions to identify duplicated content. These methods are sensitive to geometric transformations and post-processing operations. Key point-based techniques improve resilience to rotation and scaling by detecting salient features, yet their performance is reduced in smooth or low-texture regions. Deep learning-based approaches have also been introduced. They learn hierarchical representations from data but require large annotated datasets and considerable computational resources. Texture descriptors have received attention in passive image forensics. Local patterns are affected during manipulation, even when visual perception remains unchanged. Descriptors such as Local Binary Patterns and Weber Local Descriptor capture these variations. The Weber Local Descriptor model's relative intensity changes and gradient orientation within a local neighborhood. Its sensitivity to local contrast makes it suitable for detecting subtle artifacts. In addition, chrominance components have been shown to preserve manipulation traces that are less visible in luminance. This observation supports the use of color space transformations in forgery detection frameworks [4].

Despite these advances, certain limitations remain. Some methods exhibit reduced performance under compression or geometric transformations. Others require extensive training data or complex architectures. This motivates the development of methods that balance detection performance with computational efficiency across different manipulation types. Digital image editing has become a routine practice in many applications, ranging from photography to media production. Not all modifications affect the integrity of visual content. Certain adjustments, such as brightness correction and cropping, preserve the original semantics of the image [5, 6]. In contrast, some manipulations alter the meaning of the scene and may mislead interpretation. This distinction highlights the importance of differentiating between acceptable editing operations and malicious image alterations.

Digital image manipulation can be understood through a structured classification of forgery techniques. These categories differ based on the type and extent of modifications applied to the image content. Some manipulations involve minor visual adjustments, while others significantly alter the semantic meaning of the scene [7]. A clear categorization helps in distinguishing between different forms of forgery and supports the development of targeted detection strategies. This conceptual grouping provides a foundation for analyzing manipulation techniques in digital image forensics. Figure 2 illustrates major categories of image forgery, including image retouching, image splicing, and copy-move forgery. It also highlights common transformations such as rotation, scaling, and reflection that are frequently applied to copied regions, increasing the complexity of detection. This visual representation distinguishes major categories of manipulation based on structural modification. This categorization supports the selection of detection strategies tailored to specific forgery types.

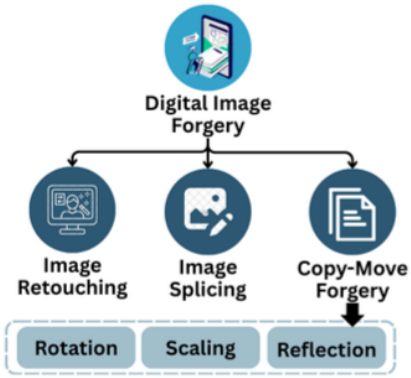

Figure 2. Categorization of digital image forgery techniques.

The illustration of common image processing operations that preserve visual content is provided in Figure 3 [8]. These operations include brightness adjustment and color correction, in contrast with manipulations that alter image semantics, including object insertion, removal, copy-move forgery, and image splicing. This distinction highlights the need for reliable methods to detect malicious modifications. The distinction emphasizes that not all image modifications indicate forgery. Only operations that alter semantic content are relevant to forensic detection.

Common forms of image forgery involve modifying visual content in a manner that alters scene interpretation [9]. Among these, copy-move

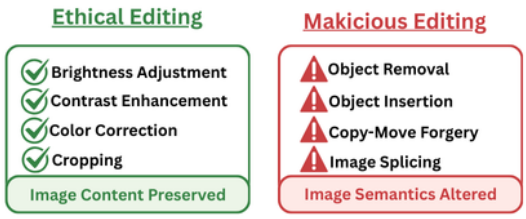

Figure 3. Distinction between ethical image editing and malicious image manipulation.

and splicing manipulations are frequently observed in real world scenarios. Copy-move forgery duplicates a region within the same image, often to conceal or replicate objects without introducing external content. In contrast, splicing combines elements from different images to create a composite scene with altered semantics [10]. Manipulated images can be used to mislead viewers, distort evidence, or alter contextual understanding. Such alterations may have consequences in domains such as journalism, legal investigations, and social media communication [11]. The process typically involves intentional modification followed by distribution to an unaware audience. This scenario highlights the broader impact of image forgery beyond visual inconsistencies. Figure 4 presents the typical workflow of image forgery, including image acquisition, manipulation through editing operations, and subsequent dissemination. It highlights the potential impact of forged images on interpretation, decision-making, and information reliability, emphasizing the need for effective detection mechanisms. The workflow specifies the stages where manipulation artifacts may be introduced. These stages guide the design of feature extraction methods used in this study.

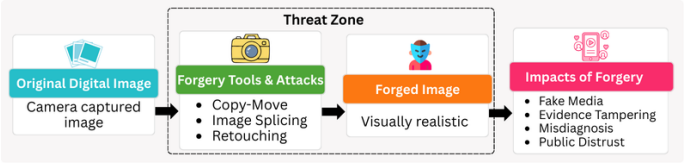

Figure 4. Threat model illustrating the creation and impact of digital image forgery.

Figure 5 presents representative examples of commonly encountered image manipulation techniques. Copy-move forgery involves duplication of a region within the same image to conceal or replicate content. In contrast, splicing combines regions from different images to generate a composite scene. The examples introduce subtle inconsistencies in texture and color distribution that are not always

perceptible to the human eye. These inconsistencies form the basis for the proposed feature representation.

In this study, a passive image authentication framework is presented based on multiscale texture analysis and supervised classification. The proposed method utilizes Weber Local Descriptor features extracted from chrominance channels to capture manipulation artifacts at multiple spatial resolutions. Figure 6 illustrates the overall framework of the proposed passive image forgery detection system. Existing studies have applied Weber Local Descriptor for forgery detection, including multiscale variants and SVM-based classification [1, 12]. However, prior approaches often rely on single color space representations or do not explicitly integrate chrominance-based analysis with multiscale texture modeling [13, 14]. In addition, the interaction between scale variation and color component selection has not been systematically examined [15].

The proposed method addresses these limitations by combining chrominance-focused preprocessing with a structured multiscale WLD configuration. This integration enables the descriptor to capture manipulation artifacts that vary across both spatial resolution and color components. The approach also maintains a consistent classification framework, allowing stable performance across datasets with different manipulation characteristics.

The main contributions of this study are summarized as follows.

1. A chrominance-based preprocessing strategy is employed to preserve manipulation-sensitive information that is less visible in luminance components.
2. A multiscale configuration of the Weber Local Descriptor is used to capture texture variations across different spatial resolutions, which improves discrimination between authentic and forged images.
3. A consistent integration of feature extraction and Support Vector Machine classification is developed and evaluated across datasets with different manipulation characteristics.

2 Literature Review

Digital image forgery detection has evolved into a distinct research domain within multimedia forensics. The rapid growth of editing software has intensified concerns regarding the authenticity and integrity of digital imagery. As a result, both active and passive detection paradigms have been widely investigated.

2.1 Active Authentication Approaches

Active authentication techniques rely on embedding verification information within the image at the time of acquisition or distribution. Unlike passive approaches, these methods require prior modification of the image [16]. Authentication is later performed by extracting or verifying the embedded information. A typical watermark embedding framework is illustrated in Figure 7. Authentication information is first computed from the original image and then embedded through a reversible data embedding mechanism. The output is a watermarked image that carries verification data within its structure.

The original image is processed to compute authentication information, which is then embedded using reversible data embedding to generate a watermarked image. At the verification stage, the received watermarked image undergoes watermark verification, as shown in Figure 8. If authentication succeeds, the original image can be recovered. If verification fails, the image is considered non-authentic.

The watermarked image is verified to determine authenticity. Upon successful authentication, the original image is recovered. Although watermark-based techniques provide controlled authentication, they require modification of the original image and specialized acquisition systems. In many real-world scenarios, such embedding mechanisms are not available. For this reason, passive image authentication techniques have gained considerable attention. These approaches analyze intrinsic image characteristics without requiring prior embedded information.

2.2 Passive Image Forgery Detection

Passive methods operate without pre-embedded information and analyze intrinsic image artifacts. They are broadly categorized into copy-move detection, splicing detection, and generalized tamper detection frameworks [12]. These methods rely on statistical inconsistencies, compression traces, noise patterns, or structural irregularities introduced during manipulation. Copy-move forgery is one of the most investigated forms of tampering. It involves duplicating a region within the same image to conceal or replicate content. Early

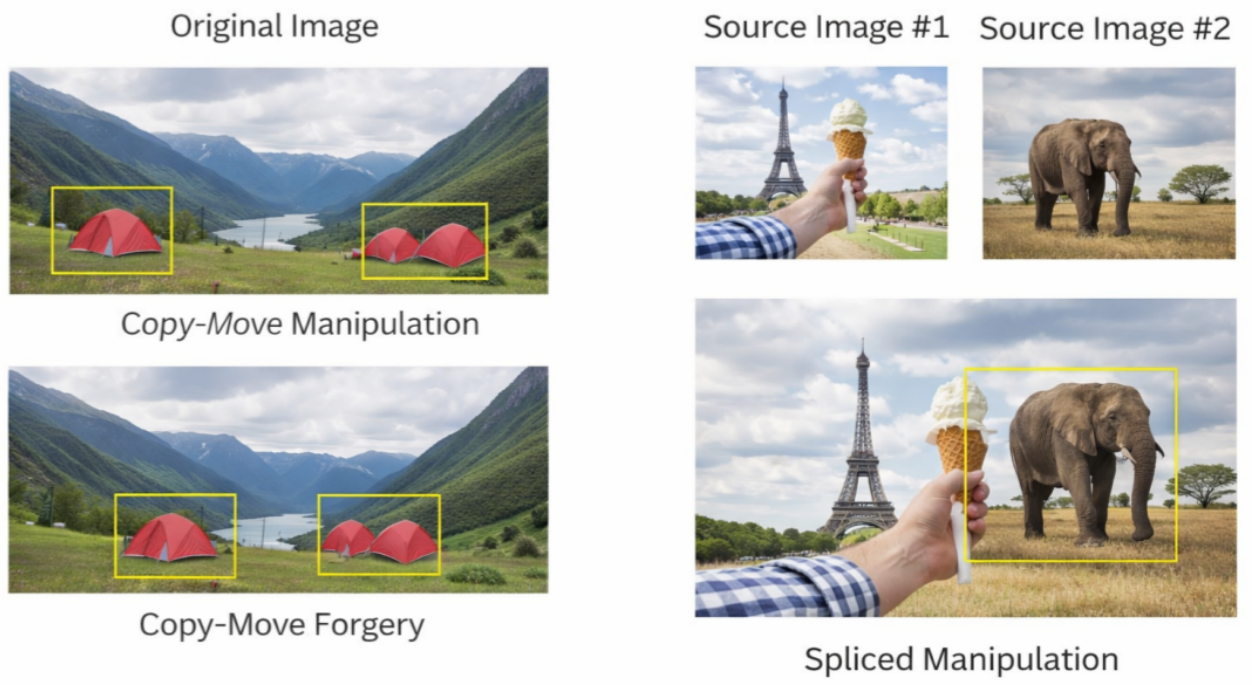

Figure 5. Common types of image forgery include copy-move, and splicing manipulations.

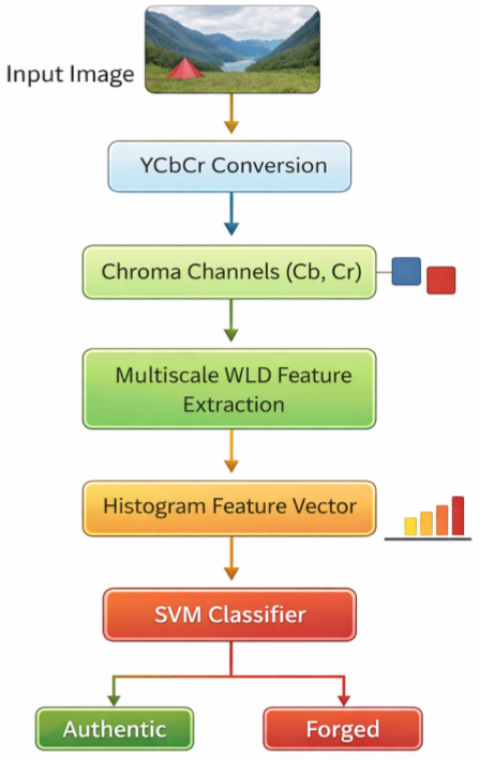

Figure 6. Proposed passive image forgery detection framework based on chroma analysis and multiscale Weber Local Descriptor features.

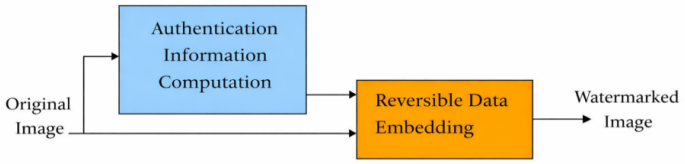

Figure 7. Watermark embedding framework illustrating the process of embedding authentication information into a digital image.

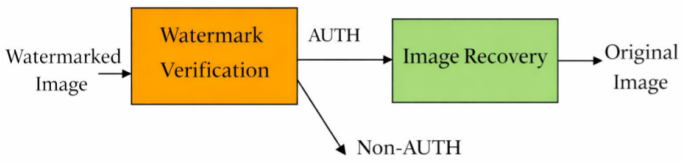

Figure 8. Watermark verification and image recovery process illustrating the authentication stage of the watermarking framework.

approaches were predominantly block-based, where overlapping blocks are extracted and compared using lexicographical sorting or transform domain features [17]. However, such methods are sensitive to geometric transformations and post-processing operations. Key point-based methods were introduced to address these limitations. Techniques employing SIFT, SURF, MSER, FAST, and Harris features have demonstrated improved resilience to rotation and scaling [18]. These approaches detect salient points and match descriptors across the image. While computationally efficient, they may struggle in homogeneous regions where distinctive key points are sparse. Transform domain techniques have also been explored. PCA-based quantization noise analysis has been used to localize tampered regions in JPEG compressed images by exploiting high-frequency artifacts. Similarly, wavelet and

gray-level co-occurrence matrix features have been combined with SVM for recaptured image detection. These methods focus on frequency domain inconsistencies rather than spatial duplication alone.

2.3 Copy-move Forgery Detection

Copy-move forgery has been extensively investigated in the domain of passive image forensics due to its frequent occurrence and practical relevance. It involves duplicating a region within the same image to conceal or replicate objects while maintaining visual consistency. Since the copied region shares a similar color distribution, noise patterns, and illumination conditions with the source region, detection becomes inherently challenging. Early studies highlighted that such manipulations often preserve low-level statistical properties, which reduces the effectiveness of naive detection techniques [19]. Initial research efforts primarily focused on block-based approaches. In these methods, the image is partitioned into overlapping blocks, and feature vectors are extracted for similarity matching. Fridrich et al. [19] introduced one of the earliest block-based frameworks using discrete cosine transform features and lexicographical sorting for efficient matching.

Popescu and Farid [20] further extended this idea by employing principal component analysis to reduce feature dimensionality while preserving discriminative information. Although these methods demonstrated promising results, their performance was observed to degrade under geometric transformations such as rotation and scaling, as well as under compression artifacts. To overcome these limitations, key point-based approaches were proposed. These methods rely on detecting salient feature points and computing invariant descriptors. Bay et al. [21] introduced the SURF descriptor, which has been widely adopted in copy-move detection due to its computational efficiency. Amerini et al. [22] utilized SIFT-based key points to identify duplicated regions, achieving improved robustness against rotation and scaling transformations. Similarly, methods based on MSER and Harris corner detection have been explored to enhance detection in complex scenarios [23]. However, it has been reported that key point-based methods may struggle in smooth or low-texture regions where distinctive features are sparse.

Recent studies have also investigated hybrid and transform domain techniques to improve robustness. Wavelet-based representations and frequency domain features have been employed to capture structural characteristics of duplicated regions [24]. These approaches aim to balance detection accuracy with computational efficiency while maintaining resilience under post-processing operations. Despite these advancements, challenges persist in handling complex manipulations involving multiple transformations and varying image quality conditions. Copy-move forgery becomes more challenging when transformations are applied to duplicated regions. Simple duplication can often be detected through direct similarity analysis. However, geometric modifications such as scaling, rotation, and reflection alter the appearance of copied regions while preserving underlying texture patterns. These variations reduce the effectiveness of traditional detection methods and increase the complexity of accurate localization. Figure 9 presents representative cases of copy-move manipulation under varying geometric transformations. Each row illustrates the original image, the corresponding forged image, and the detection results highlighting duplicated regions. The examples include basic duplication, scaling, rotation, and reflection, demonstrating the challenges associated with identifying manipulated regions under diverse transformation scenarios.

These techniques indicate that no single method provides consistent performance across all scenarios. Block based approaches offer dense coverage but lack transformation invariance, whereas key point-based methods improve robustness but may miss homogeneous regions. This trade off highlights the need for feature representations that can capture intrinsic texture variations while maintaining stability under diverse manipulation conditions.

2.4 Splicing Forgery Detection

Image splicing combines content from multiple images into a composite. Unlike copy-move manipulation, splicing often introduces discrepancies in illumination, color distribution, and noise characteristics. Detection strategies therefore emphasize chrominance statistics and texture inconsistencies [14]. LBP combined with DCT features extracted from chroma components has shown strong performance on CASIA and Columbia datasets when classified using SVM. Run length and chroma-based statistical features have also been proposed to capture cross channel inconsistencies [25]. Texture based analysis using median filter residuals and entropy descriptors has achieved high detection rates in cut paste scenarios. Recent works have incorporated convolutional neural networks to learn

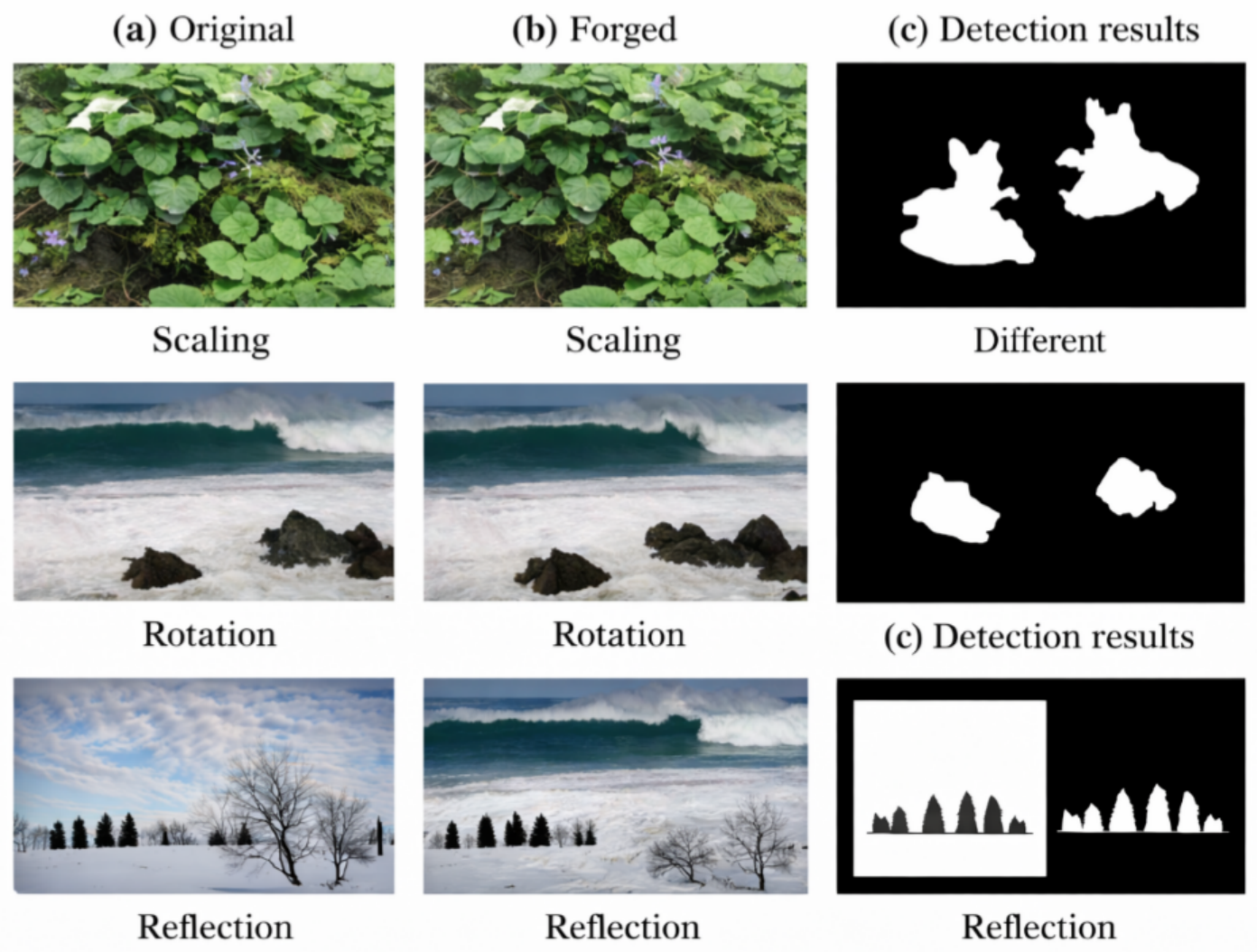

Figure 9. Examples of copy-move forgery under different transformation conditions.

hierarchical representations. A coarse to fine CNN framework was proposed for splicing detection, integrating adaptive clustering for localization. Deep learning approaches have demonstrated improved generalization, yet they demand large annotated datasets and extensive computational resources [26]. Figure 10 illustrates the process of image splicing, where regions from two different source images are combined to generate a composite image.

Figure 10. Example of image splicing figure illustrating a typical image splicing manipulation.

2.5 Texture Descriptors in Forgery Detection

Texture descriptors play a central role in passive detection frameworks. Forgery operations alter micro patterns within local neighborhoods. Consequently, descriptors such as LBP, DRLBP, and Weber Local Descriptor have been extensively studied [13]. The Weber Local Descriptor was originally inspired by Weber law in human perception theory. It encodes differential excitation and orientation components, capturing relative intensity variations. Its sensitivity to local contrast makes it suitable for detecting subtle manipulation traces. Multiresolution WLD variants have been applied to chrominance channels for forgery detection, achieving competitive performance across benchmark datasets [15]. Comparative studies indicate that multiscale WLD often surpasses Multi LBP in splicing and copy-move detection tasks. The effectiveness of chroma space representation has been repeatedly emphasized. Manipulation artifacts are sometimes less perceptible in luminance but remain

detectable in chrominance components [27]. This observation supports the integration of WLD features extracted from Cb and Cr channels in passive detection frameworks.

2.6 Classification Strategies and SVM

Feature extraction alone is insufficient without reliable classification. Support Vector Machine has been widely adopted in image forensics due to its strong generalization capability and effectiveness in high dimensional feature spaces [28]. SVM constructs an optimal separating hyperplane, and through kernel functions can handle nonlinear boundaries. Numerous forgery detection frameworks integrate SVM with texture descriptors. LBP DCT based chroma features classified with SVM achieved high detection accuracy across multiple datasets. Hybrid feature representations evaluated with SVM have demonstrated balanced tradeoffs between accuracy and execution time.

Performance evaluation typically employs accuracy, precision, recall, F1 score, ROC analysis, and confusion matrices. Statistical measures such as Youden index and discriminant strength have also been discussed in classifier evaluation literature. These metrics provide insight into sensitivity and specificity, particularly in imbalanced forensic datasets. Standardized datasets are essential for fair evaluation. CASIA TIDE v1.0 and v2.0 remain widely used benchmarks for splicing and copy-move detection. The MICC F2000 and CoMoFoD datasets have also contributed structured manipulation scenarios including scaling, rotation, and compression artifacts. However, cross dataset generalization remains a challenge. Some methods perform well on controlled datasets yet exhibit reduced robustness under diverse post processing conditions. This limitation highlights the importance of designing descriptors capable of capturing invariant manipulation traces.

2.7 Research Gap

Despite significant progress, several limitations persist. Block based techniques remain sensitive to heavy compression. Keypoint-based methods underperform in low texture regions. Deep learning approaches require extensive training data and computational infrastructure. Texture descriptors such as WLD offer a balance between computational efficiency and discriminative capability. Yet their performance depends on scale configuration and color space selection [29, 30]. A systematic integration of multiscale WLD with an optimized SVM framework, evaluated across standard datasets, remains an important direction for strengthening passive image authentication systems.

In light of these observations, the present study builds upon established passive forensic methodologies. It emphasizes multiscale WLD feature extraction from chrominance components combined with SVM classification, targeting reliable detection of copy-move and splicing forgeries across benchmark datasets.

3 Materials and Methods

This study presents a passive image authentication framework for detecting digital image forgeries. The system classifies images as authentic or manipulated by analyzing intrinsic texture characteristics instead of relying on embedded watermark or signature information. The methodological pipeline includes dataset preparation; chroma-based preprocessing, multiscale Weber Local Descriptor feature extraction, and supervised classification using a Support Vector Machine. Training and testing stages were implemented separately to avoid data leakage.

3.1 Dataset Selection and Characteristics

Two benchmark datasets were selected to evaluate the proposed authentication framework. The CASIA v2.0 dataset can be accessed from the Chinese Academy of Sciences Institute of Automation repository [31]. The MICC F2000 dataset is available through the University of Florence Visual Information Processing and Protection [32, 33]. The selection was guided by the presence of realistic manipulation scenarios and the availability of both authentic and forged samples. Diversity in scene content and manipulation types was also considered. Dataset preparation followed a structured organization procedure. Images were collected from the dataset source and categorized into authentic and forged classes before training and evaluation. The dataset organization process is illustrated in Figure 11.

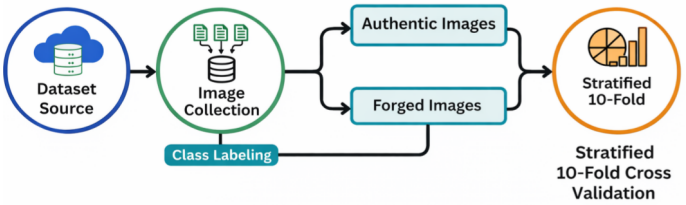

Figure 11. Dataset preparation and organization workflow.

The first dataset is the CASIA Tampered Image

Table 1. Dataset characteristics.

Dataset	Image Classes	Forgery Types	Color Format	Scene Variability	Post Processing
CASIA v2.0	Authentic and Tampered	Copy-move, Splicing	Color	High	Present in several samples
MICC F2000	Authentic and Tampered	Copy-move	Color	Moderate to High	Limited

Detection Evaluation Database Version 2.0. It contains color images categorized into authentic and tampered classes. The tampered images include both copy-move and splicing manipulations. In splicing cases, regions from external images are inserted into a host image. In copy-move cases, regions are duplicated within the same image. The dataset presents variations in image resolution, object distribution, and scene complexity. Some manipulated images also include post-processing operations, such as compression and slight visual adjustments, which increase classification difficulty.

The second dataset is MICC F2000. This dataset primarily focuses on copy-move forgeries. It includes original images and corresponding manipulated versions generated by duplicating selected regions within the same image. The forged regions may involve translation and resizing. Scene content varies across images, including natural and structured environments. Unlike CASIA v2.0, splicing manipulation is not a primary component of this dataset. A summary of the dataset characteristics is presented in Table 1.

Both datasets contain labeled samples, which enabled supervised training and evaluation of the classifier. Training and testing subsets were defined to ensure that evaluation was conducted on unseen data. Representative examples from the CASIA v2.0 dataset are illustrated in Figure 12. The dataset contains diverse scene categories including architecture, objects, and outdoor environments.

A detailed summary of the evaluated datasets is provided in Table 2, including the number of authentic and tampered images, total sample size, image formats, and resolution ranges for each dataset. These characteristics reflect differences in scene diversity, manipulation types, and image quality, which collectively influence the complexity of forgery detection.

CASIA v2.0 contains realistic manipulated images with post processing applied around tampered regions.

Figure 12. Dataset preparation and organization workflow.

The dataset includes diverse scene categories such as animals, architecture, nature, and texture. Tampered images are generated through copy-paste operations and geometric modifications, including scaling and rotation. MICC F2000 consists of high-resolution JPEG images. Forged images are produced by duplicating selected regions within the same image.

3.2 Dataset Preprocessing

All images underwent a preprocessing stage before feature extraction. Color images were converted from RGB space into a representation separating luminance and chrominance components. Feature extraction was performed on selected chroma channels. Chroma information was emphasized because manipulation artifacts frequently introduce subtle variations in these components that remain less visible in luminance. No filtering or enhancement operations were applied that could alter the intrinsic texture structure of the images. Original dataset characteristics were preserved throughout preprocessing. The processed images were then forwarded to the feature extraction stage for multiscale texture analysis. The preprocessing workflow is presented in Figure 13.

To evaluate classifier performance, a 10-fold cross-validation was employed. The entire dataset was divided into ten equal subsets. In each iteration,

Table 2. Description of the evaluated datasets.

Dataset	Authentic Images	Tampered Images	Total Images	Image Format	Image Size
CASIA v2.0	7491	5123	12614	JPEG, BMP, TIFF	240×160 to 900×600
MICC F2000	1300	700	2000	JPEG	2048×1536

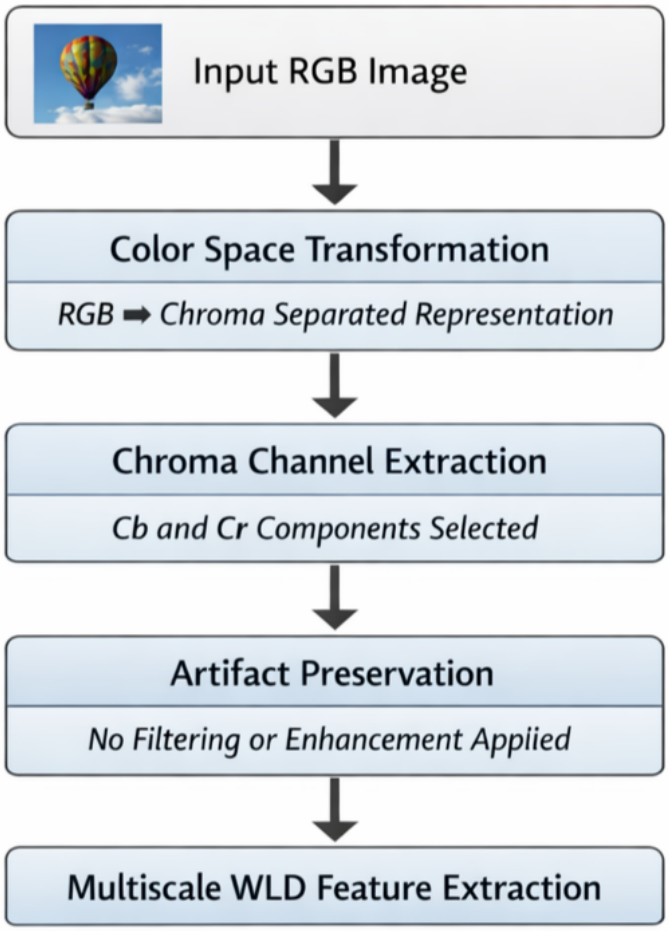

Figure 13. Image preprocessing workflow.

nine subsets were used for training, and the remaining subset was used for testing. This process was repeated ten times. Each subset was used exactly once as the testing set. The final performance was obtained by averaging the results across all folds. This evaluation strategy allows performance variation across folds to be implicitly considered, providing an indication of model stability under different data partitions. Both authentic and forged images were distributed across folds to maintain class representation. This validation strategy ensures that all samples contribute to both training and testing while preventing overlap within a single fold.

3.2.1 *Feature extraction*

The proposed framework was developed to perform passive image authentication through texture-based feature analysis and supervised classification. The method operates without embedded watermark information. All decisions are derived from intrinsic image characteristics. The complete procedure consists of feature extraction using the multiscale Weber Local Descriptor and classification using a Support Vector Machine. Each stage is described below. Texture information was used to represent image content. Forgery operations alter local intensity relationships, even when visual perception remains unchanged. For this reason, a local descriptor was employed. The Weber Local Descriptor encodes local intensity variation within a defined neighborhood. It is composed of two components. The first component is differential excitation. This measures the relative intensity difference between a central pixel and its neighboring pixels. The second component is orientation. This represents gradient direction information.

A multiscale configuration was implemented. Neighborhood parameters were adjusted to capture both fine and coarse texture variations. This allows the descriptor to represent manipulation artifacts that appear at different spatial resolutions. For each processed chroma channel image, WLD responses were computed across the image grid. Histogram representations were then generated from these responses. The resulting histograms form the feature vectors used for classification. No dimensionality reduction technique was introduced at this stage. The extracted feature vectors were directly used for training and testing.

The Weber Local Descriptor is composed of two main components as presented in equation (1) and (2). These components model local intensity variation and gradient orientation within a predefined neighborhood. For a central pixel x_c, differential excitation is defined as:

$$\xi(x_c) = \arctan\left(\frac{\sum_{i=1}^{P-1}(x_i - x_c)}{x_c}\right) \quad (1)$$

In equation (1), x_c denotes the intensity value of the central pixel. The term x_i represents the intensity of the i-th neighboring pixel within a local region. The parameter P indicates the total number of neighboring pixels considered around x_c. The function arctan is applied to normalize the accumulated relative intensity differences, and $\xi(x_c)$ represents differential excitation. This formulation captures relative contrast information.

Absolute intensity values are therefore not directly used. The second component captures directional information and is defined as:

$$\theta(x_c) = \arctan\left(\frac{I_y}{I_x}\right) \quad (2)$$

In equation (2), I_x and I_y denote horizontal and vertical image gradients computed at the central pixel location. These gradients are typically obtained using first-order derivative operators. The ratio between vertical and horizontal gradients encodes the dominant local edge direction. $\xi(x_c)$ and $\theta(x_c)$ describe local structural variation. The normalization by x_c reflects Weber's law, where perceived intensity change is relative to the reference intensity. Their joint histogram representation forms the feature vector used for classification.

3.3 Classification

Supervised classification was performed using a Support Vector Machine. The SVM classifier constructs a separating boundary between authentic and forged image classes within the feature space. Feature vectors extracted from labeled training images were used to train the classifier. During training, the optimal separating hyperplane was determined in the transformed feature space. Kernel functions were employed to allow separation under nonlinear conditions when necessary. Once the training phase was completed, the learned model was applied to unseen feature vectors in the testing phase. Each image was assigned to either the authentic or forged class based on its position relative to the decision boundary. The classification procedure followed a clear separation between training and testing subsets. This ensured that the evaluation was conducted on previously unseen data. The methodology integrates chroma-based multiscale WLD feature extraction with supervised SVM classification.

This combination forms the core analytical component of the proposed image authentication system. The overall training and testing workflow of the proposed authentication framework is illustrated in Figure 14. The process includes preprocessing, feature extraction, model training, and final decision generation for both training and testing phases.

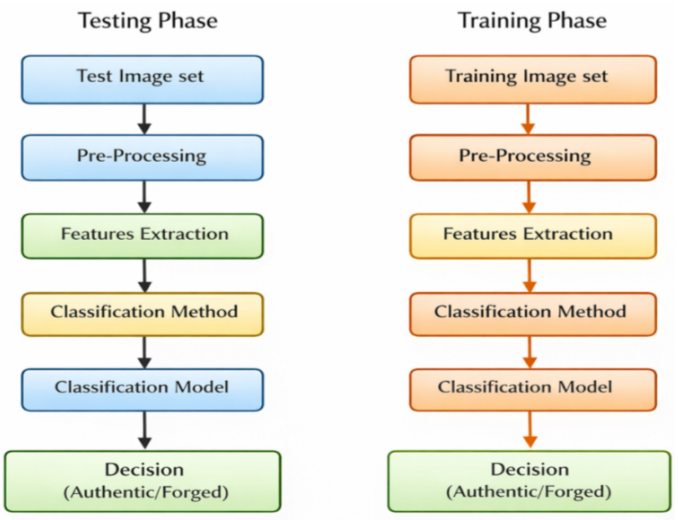

Figure 14. Training and testing workflow of the proposed authentication framework.

It presents the complete processing pipeline for both training and testing phases. Each phase includes preprocessing, feature extraction, classification, and final decision generation for authentic or forged image classification.

The proposed framework includes parameters related to preprocessing, multiscale WLD configuration, and SVM classification. Parameter tuning was conducted in a controlled manner. Individual parameters were varied while keeping others fixed in order to observe their influence on classification behavior. Although this sequential tuning strategy does not guarantee a globally optimal configuration, it enables systematic exploration of parameter effects. The final parameter configuration was selected based on cross-validated evaluation results.

Parameter configuration was carried out at different stages of the proposed framework. The overall tuning structure is presented in Figure 15. The preprocessing stage includes color space conversion to YCbCr and subsequent block division. Feature extraction is governed by multiscale WLD parameters denoted by T, M, and S. The classification stage involves selection

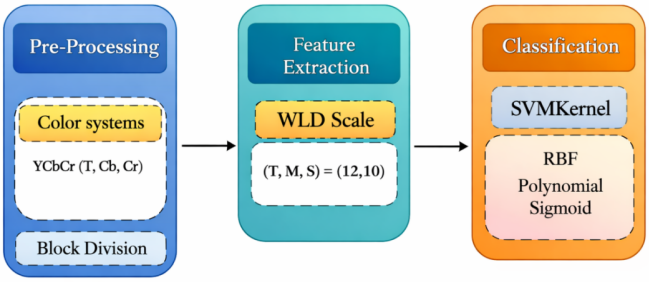

Figure 15. Overview of the parameter configuration strategy across preprocessing, feature extraction, and classification stages.

of the SVM kernel function. These parameters were adjusted in a controlled manner to obtain a consistent configuration for forgery detection.

This Figure 15 illustrates the parameter configuration strategy applied across preprocessing, feature extraction, and classification stages. Preprocessing includes YCbCr color space selection and block division. Feature extraction is controlled through multiscale WLD scale parameters. Classification is performed using SVM with kernel options including Radial Basis Function (RBF), Polynomial, and Sigmoid.

3.4 Experimental Setup

All experiments were conducted in Python. OpenCV was used for image processing, and scikit learn was employed for classification tasks. The implementation was executed on a workstation equipped with an Intel Core i7 processor at 3.40 GHz and 16 GB RAM. Extracted WLD histogram features were directly supplied to the Support Vector Machine classifier. RBF, Polynomial, and Sigmoid kernels were examined during training. The regularization parameter C was varied, and the gamma parameter was tuned for the RBF kernel. Ten-fold cross validation was performed independently for each dataset. In every cycle, nine folds were assigned for training and one-fold was retained for testing. Class proportions were preserved within each fold. Final results were computed as the mean performance across all validation folds.

Figure 16 presents the complete processing pipeline of the proposed system, starting from input image acquisition to final authentication. The image is first subjected to preprocessing, followed by texture characterization using the Weber Local Descriptor and subsequent feature extraction. The extracted features are then classified using a Support Vector Machine to construct a decision boundary between authentic and forged images. Based on this classification, the system determines whether the image is valid or manipulated.

3.5 Evaluation Metrics

Classifier performance was evaluated using standard measures derived from the confusion matrix. Four outcomes were considered: True Positive, True Negative, False Positive, and False Negative. True Positive denotes forged images correctly classified as forged. True Negative represents authentic images correctly classified as authentic. False Positive corresponds to authentic images incorrectly labeled as forged. False Negative indicates forged images incorrectly classified as authentic. The evaluation metrics are summarized in Table 3.

Table 3. Performance evaluation metrics.

Metric	Equation
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
True Positive Rate (TPR)	$\frac{TP}{TP+FN}$
False Positive Rate (FPR)	$\frac{FP}{FP+TN}$
Precision	$\frac{TP}{TP+FP}$
F1 Score	$2 \times \frac{\text{Precision} \times \text{TPR}}{\text{Precision} + \text{TPR}}$
Area Under Curve (AUC)	Area under ROC curve

Receiver Operating Characteristic analysis was conducted by plotting False Positive Rate against True Positive Rate across varying decision thresholds. The Area Under the Curve quantifies the discriminative capability of the classifier. An AUC value of 1 reflects perfect classification, whereas 0.5 indicates random performance. The overall experimental workflow adopted in this study is illustrated in Figure 17. The framework includes dataset preparation, feature extraction using the Weber Local Descriptor, model training, testing on unseen samples, and final performance evaluation.

3.6 Computational Complexity Analysis

The computational complexity of the proposed framework is primarily influenced by feature extraction and classification stages. For an image of size $N \times M$, multiscale Weber Local Descriptor features are computed by scanning each pixel across multiple

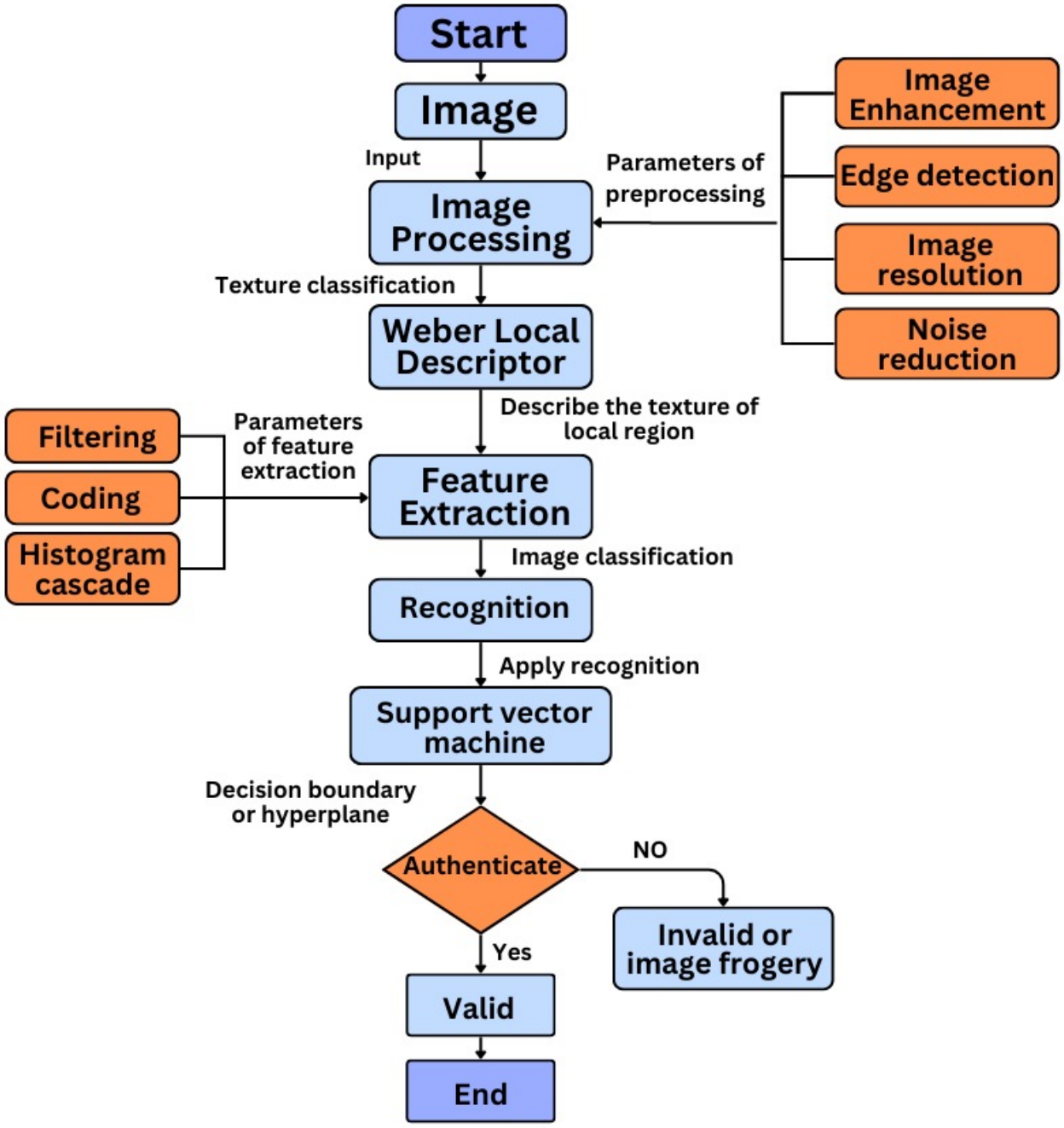

Figure 16. Overall workflow of the proposed passive image forgery detection framework.

Table 4. Computational characteristics of the proposed framework.

Component	Operation Description	Complexity Behavior	Remarks
Preprocessing	RGB to YCbCr conversion and chrominance extraction	Linear with number of pixels	Simple color space transformation
Feature Extraction	Multiscale WLD computation over image grid	Linear with pixels and scales	Dominant computational stage
Feature Representation	Histogram generation from WLD responses	Linear with feature bins	Fixed feature dimensionality
Classification (SVM)	Training and prediction using extracted features	Depends on kernel and samples	Linear kernel is computationally efficient
Overall Framework	Combined processing pipeline	Linear with image size	No iterative training required

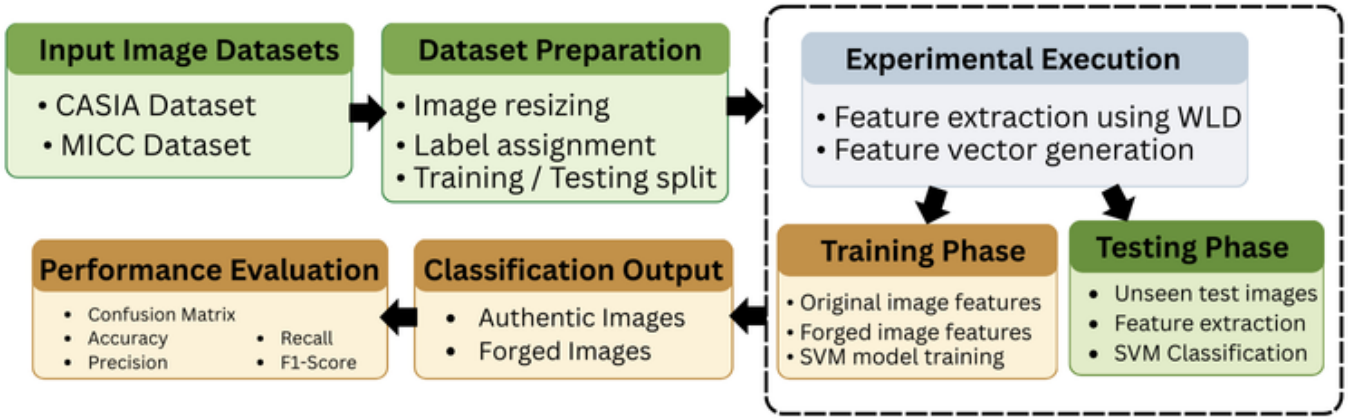

Figure 17. Experimental workflow of the proposed image authentication system.

neighborhood configurations. The complexity of this process increases linearly with the number of pixels and the number of scales considered. The extracted features are represented using histogram-based descriptors. The dimensionality of the feature vector depends on the number of bins used for differential excitation and orientation components. If B_ξ and B_θ denote the number of bins for differential excitation and orientation, respectively, the total feature dimension is given by equation (3) as:

$$D = B_\xi \times B_\theta \tag{3}$$

In the current implementation, the feature dimensionality remains moderate and does not require dimensionality reduction, which simplifies the overall pipeline. The classification stage is performed using a Support Vector Machine. The computational cost depends on the number of training samples and the selected kernel function. Linear kernels result in lower computational overhead, while nonlinear kernels introduce additional cost due to kernel evaluations.

In practical implementation, the feature extraction stage dominates the overall processing time. However, the absence of iterative training procedures makes the method computationally efficient compared to deep learning approaches. Deep models require multiple training epochs and large datasets, whereas the proposed framework operates with fixed feature extraction and relatively fast classification. The proposed method maintains a balance between computational cost and detection performance, making it suitable for applications where computational resources are limited. The computational characteristics of each stage in the proposed framework are summarized in Table 4.

The Table 4 highlights that feature extraction is the most computationally demanding stage due to multiscale processing. Other components contribute less to the overall cost, and no iterative optimization is required. A comparison with deep learning-based approaches is provided in Table 5.

Deep learning-based methods have demonstrated strong performance in image forgery detection, particularly in capturing complex and high-level manipulation patterns. However, these approaches typically require large annotated datasets and significant computational resources for training and inference. In contrast, the proposed method relies on handcrafted feature extraction and does not require iterative training, which reduces computational overhead. This trade-off highlights the relevance of lightweight feature-based approaches in scenarios where computational resources or labeled data are limited.

4 Results

The performance of the proposed passive image forgery detection framework was evaluated using two benchmark datasets, CASIA v2.0 and MICC F2000. Experimental analysis was conducted to assess classification capability across different manipulation types, including copy-move and splicing forgeries. The evaluation focuses on quantitative metrics derived from cross-validated experiments, including accuracy, precision, F1 score, true positive rate, false negative rate, and AUC. The reported performance values represent the mean across ten validation folds. The consistency of results across folds indicates stable classifier behavior under varying training and testing splits.

Table 5. Comparison with deep learning-based image forgery detection approaches.

Aspect	Proposed Method (Multiscale WLD + SVM)	CNN-based Methods	Transformer-based Methods
Feature Representation	Handcrafted texture features (WLD)	Learned hierarchical features [1, 3]	Global attention-based representations [26]
Training Requirement	No iterative training	Multi-epoch supervised training [3]	Large-scale training and fine-tuning [26]
Computational Cost	Moderate	High [1]	Very high [26]
Data Requirement	Low	High [1, 3]	Very high [3]
Generalization	Stable within dataset	May require retraining across datasets [1]	Sensitive to data distribution shifts [26]
Detection Capability	Effective for texture inconsistencies	Strong for semantic and complex manipulations [3]	Strong for global contextual inconsistencies [26]
Model Complexity	Low	High [1]	Very high [26]
Interpretability	Relatively interpretable	Limited interpretability [1]	Low interpretability [26]

Table 6. Evaluation results of WLD using different datasets and SVM kernels.

Dataset	SVM Kernel	Class	Accuracy (%)	TPR (%)	FNR (%)	Precision (%)	F1 Score (%)	AUC
CASIA v2.0	Linear	Authentic	97.0	95.1	4.9	97.8	96.4	0.98
		Spliced		98.4	1.6	96.4	97.4	
MICC F2000	Fine Gaussian	Authentic	97.4	96.1	3.9	99.8	97.9	0.98
		Copy-move		99.7	0.3	93.2	96.3	

4.1 Evaluation on Benchmark Datasets

The proposed authentication framework was evaluated using CASIA v2.0 and MICC F2000 datasets. Experiments were conducted using multiscale Weber Local Descriptor features extracted from Cb and Cr chrominance channels. The descriptor parameters were configured with (T = 12), (M = 2), and (S = 10). Different SVM kernels were examined during training. These included linear, quadratic, cubic, RBF kernel with different parameter settings (fine, medium, and coarse gamma values). The kernel producing the highest classification accuracy for each dataset was selected for final testing. Performance was measured using accuracy, true positive rate, false negative rate, and area under the ROC curve. The summarized results for both datasets are presented in Table 6.

For the CASIA v2.0 dataset, the linear SVM kernel produced the best overall performance. The classifier achieved an overall accuracy of 97.0 % across both classes. For authentic images, the true negative rate (specificity) reached 95.1 %, with a false positive rate of 4.9 %. The precision for authentic images was 97.8 %, indicating high reliability in identifying non-manipulated content. For spliced images, the true positive rate (sensitivity) reached 98.4 %, with a corresponding false negative rate of only 1.6 %. The precision for spliced images was 96.4 %, while the F1 score reached 97.4 %. The area under the ROC curve (AUC) was 0.98, indicating strong discriminative capability. These values demonstrate that the proposed framework maintains balanced and reliable performance across both authentic and spliced image classes.

For the MICC F2000 dataset, the fine Gaussian kernel achieved the highest classification performance. Authentic samples were classified with an accuracy of 97.4 % and a true positive rate of 96.1 %. The false negative rate remained low at 3.9 %. Precision for the authentic class reached 99.8 %, indicating highly reliable identification of non-manipulated images. The corresponding F1 score was 97.9 %, demonstrating strong overall classification balance. The area under the ROC curve again reached 0.98, indicating stable model behavior. Copy-move forgeries were detected with a true positive rate of 99.7 % and a very low false negative rate of 0.3 %. Precision for the forged class was 93.2 %, reflecting a small number of false positive predictions, while the F1 score reached 96.3 %, indicating effective detection performance. The AUC value remained consistent at 0.98. Overall, the results demonstrate that the proposed WLD-based representation provides reliable and balanced discrimination across different manipulation types and dataset characteristics.

4.2 Confusion Matrix Analysis for CASIA v2.0

Classification performance was further examined using the confusion matrix presented in Figure 18.

The confusion matrix provides a detailed breakdown of prediction outcomes by comparing actual class labels with predicted labels. It enables a deeper understanding of classifier behavior beyond overall accuracy by highlighting both correct classifications and error patterns.

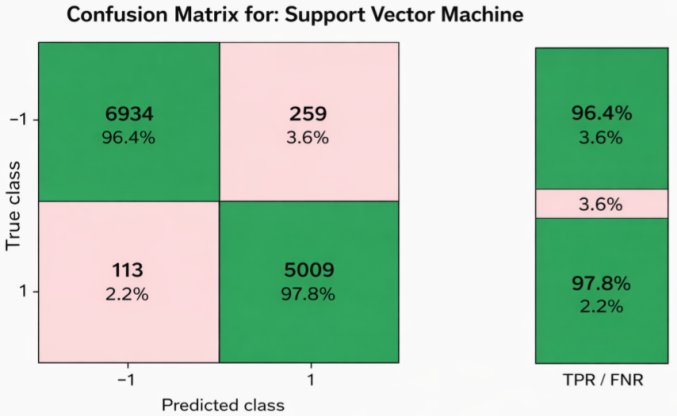

Figure 18. Confusion matrix using SVM on CASIA v2.0.

For the CASIA v2.0 dataset, the classifier achieved a high number of correct predictions. A total of 6,934 spliced samples were correctly identified as spliced, achieving a true positive rate of 98.4%. This indicates strong sensitivity toward detecting manipulated images. Similarly, 5,009 authentic samples were correctly classified as authentic, corresponding to a true negative rate of 95.1%.

Misclassification errors were limited in comparison to correct predictions. A total of 259 authentic images were incorrectly classified as spliced, representing false positive cases (4.9% of authentic samples). These errors suggest that certain authentic images contain texture patterns or chrominance variations that resemble manipulation artifacts. In contrast, only 113 spliced images were misclassified as authentic, representing false negative cases (1.6% of spliced samples). This relatively low false negative rate indicates that the model is effective in capturing manipulation traces and rarely fails to detect forged content.

The distribution of errors provides further insight into classifier characteristics. The false positive rate (4.9%) is higher than the false negative rate (1.6%), indicating that the model exhibits a mild tendency to classify uncertain samples as forged. This behavior may be considered desirable in forensic applications, where missing a manipulated image (false negative) could have more serious implications than incorrectly flagging an authentic one (false positive). The low false negative count reflects strong detection capability.

From a class-wise perspective, the true positive rate for spliced images reaches 98.4%, while the true negative rate for authentic images is 95.1%. These values indicate consistent performance across both categories, with slightly higher reliability in detecting manipulated content.

The confusion matrix also reflects the effectiveness of multiscale texture representation in distinguishing between authentic and spliced images. The high number of correct classifications suggests that the extracted WLD features capture discriminative local patterns associated with manipulation. The presence of a small number of misclassifications highlights the inherent difficulty of detecting subtle forgeries, particularly in cases involving complex textures or minimal editing. This confusion matrix analysis confirms that the proposed framework achieves stable and reliable classification performance on the CASIA v2.0 dataset.

4.3 Confusion Matrix Analysis (MICC F2000)

Classification performance on the MICC F2000 dataset was further evaluated using the confusion matrix presented in Figure 19. The confusion matrix provides a detailed representation of prediction outcomes by comparing actual and predicted class labels. It enables close examination of both correct classifications and error distribution across classes. For this dataset, the classifier demonstrated strong performance with a high number of correct predictions. A total of 1249 authentic samples were correctly classified as authentic, indicating reliable identification of non-manipulated images. Similarly, 698 forged samples were correctly identified as forged, reflecting high sensitivity toward copy-move manipulations [36].

Misclassification errors were minimal. Only 51 authentic images were incorrectly classified as forged, representing false positive cases. These errors suggest that certain authentic regions may exhibit texture similarities to duplicated areas, leading to misclassification. In contrast, only 2 forged images were misclassified as authentic, representing false negative cases. This extremely low false negative count indicates that the model rarely fails to detect manipulated content. The distribution of errors highlights a slight imbalance between false positives and false negatives. The false positive rate is marginally higher, indicating that the classifier tends

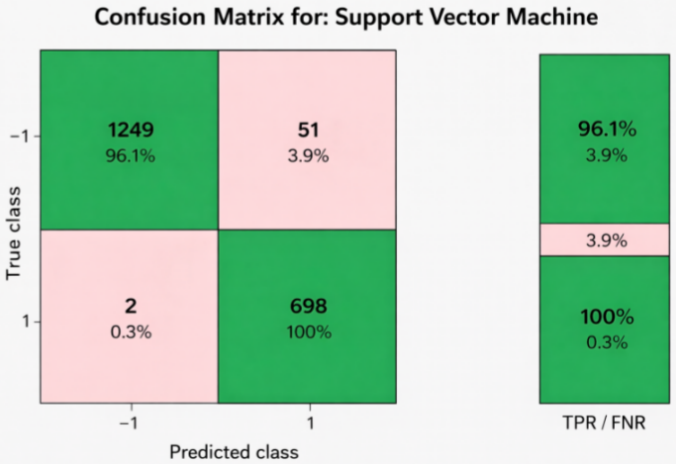

Figure 19. Confusion matrix using SVM on MICC F2000.

to label uncertain samples as forged. This tendency can be considered acceptable in forensic applications, where failing to detect a manipulated image is often more critical than incorrectly flagging an authentic one. The very low false negative rate reflects strong detection capability and reliable identification of copy-move forgeries.

From a class-wise perspective, the true positive rate for forged images reaches nearly 100 %, while the true negative rate for authentic images is approximately 96.1 %. These values indicate highly consistent classification behavior, with particularly strong performance in detecting manipulated samples. The model shows no significant bias and maintains balanced performance across both classes. The confusion matrix further supports the effectiveness of the proposed feature representation. Multiscale WLD features appear to capture discriminative texture patterns associated with copy-move forgery, even under varying scene conditions. The very low error rates suggest that the descriptor is well suited for identifying duplicated regions within the same image.

Overall, the confusion matrix analysis confirms that the proposed framework achieves highly reliable classification performance on the MICC F2000 dataset. The model demonstrates strong detection capability with minimal misclassification, particularly in identifying forged images, which is critical for practical image forensics applications.

4.4 Receiver Operating Characteristic Analysis

Receiver Operating Characteristic analysis was used to evaluate classifier performance across different decision thresholds, as illustrated in Figure 20. The ROC curve represents the relationship between the true positive rate and the false positive rate. It provides a comprehensive view of classifier behavior beyond fixed threshold evaluation. For the CASIA v2.0 dataset, the ROC curve shows a sharp increase toward the upper left region of the plot. This pattern indicates that high detection rates are achieved while maintaining low false positive values. The curve quickly approaches the top boundary and remains stable across a wide range of thresholds. This behavior reflects consistent separation between authentic and forged samples within the feature space.

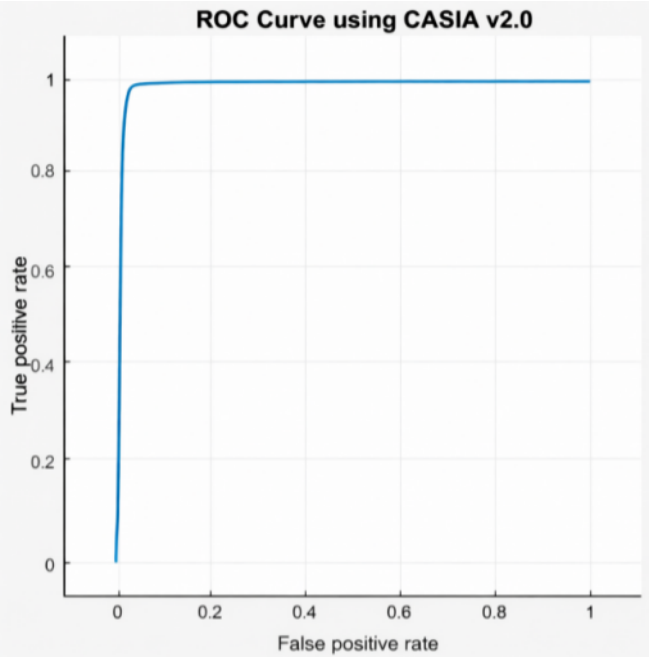

Figure 20. ROC curve for CASIA v2.0.

The area under the curve reaches a value of 0.98. This value indicates strong discriminative capability and reliable ranking between the two classes. It suggests that the classifier assigns higher confidence scores to forged samples compared to authentic ones in most cases. The high AUC value also supports the effectiveness of the extracted multiscale texture features. The true positive rate remains high even when the false positive rate is reduced. This property is important in forensic applications where strict control over false alarms may be required. At the same time, detection performance does not degrade significantly under stricter threshold settings. Overall, the ROC analysis confirms that the proposed framework maintains stable and reliable classification performance on the CASIA v2.0 dataset. The curve shape and AUC value together indicate effective separation of classes and consistent behavior across varying decision thresholds.

A similar Receiver Operating Characteristic analysis was conducted using the MICC F2000 dataset, as illustrated in Figure 21. The ROC curve represents the relationship between the true positive rate and the false positive rate across different decision thresholds. It provides a detailed view of classifier performance under varying operating conditions.

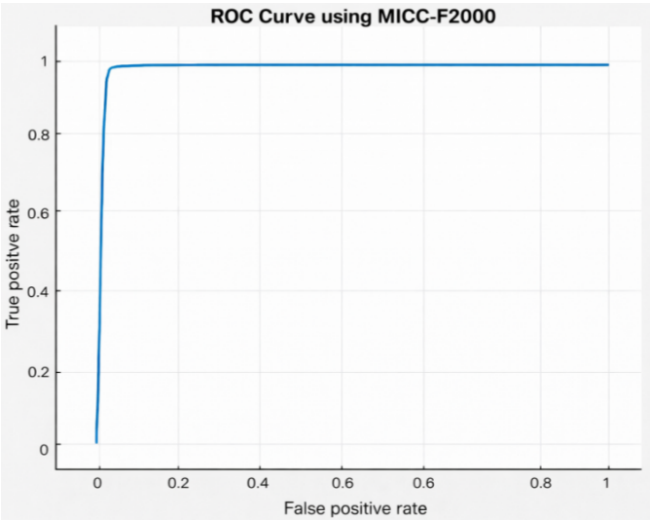

Figure 21. ROC curve for MICC F2000.

For the MICC F2000 dataset, the ROC curve exhibits a steep rise toward the upper left region of the plot. This pattern indicates that the classifier achieves high detection rates with very low false positive values. The curve quickly approaches the top boundary and remains stable across a wide range of thresholds. Such behavior reflects strong separation between authentic and forged samples in the feature space. The area under the curve reaches a value of 0.98. This value indicates strong discriminative capability and confirms that the classifier performs consistently across different datasets. It suggests that forged samples are assigned higher confidence scores compared to authentic samples in most cases. The high AUC also supports the effectiveness of multiscale texture features in capturing duplication artifacts specific to copy-move forgery.

The curve maintains stability across different threshold settings. The true positive rate remains close to its maximum value even when the false positive rate is minimized. This indicates that detection performance is not significantly affected by threshold variation. Such behavior is desirable in forensic applications where reliable detection must be maintained under strict conditions. Overall, the ROC analysis for the MICC F2000 dataset confirms stable and consistent classifier performance. The curve shape and AUC value together indicate effective separation between authentic and manipulated images, supporting the reliability of the proposed framework across different forgery scenarios.

4.5 Ablation Study on Feature Representation

To further examine the contribution of individual components in the proposed framework, an ablation analysis was conducted. The evaluation focuses on two key aspects: multiscale representation and color space selection. Specifically, three configurations were tested: single-scale WLD, multiscale WLD, and feature extraction using RGB and YCbCr color spaces. The purpose of this analysis is to isolate the impact of scale variation and chrominance-based processing on classification performance. All experiments were performed under identical conditions using the same SVM configuration and cross-validation protocol as shown in Table 7.

Table 7. Ablation Study Results on CASIA v2.0 Dataset.

Configuration	Color Space	Accuracy (%)	Average TPR (%)	AUC
WLD (Single Scale)	YCbCr (Cb, Cr)	94.8	94.2	0.95
WLD (Multiscale)	YCbCr (Cb, Cr)	**97.0**	**96.8**	**0.98**
WLD (Multiscale)	RGB	95.6	95.1	0.96

The results indicate multiscale representation significantly improves classification performance compared to single-scale feature extaction. The increase in accuracy and AUC suggests that capturing texture information at multiple spatial resolutions enhances the discriminative capability of the descriptor. A comparison between RGB and YCbCr color spaces further highlights the importance of chrominance components. Features extracted from Cb and Cr channels consistently outperform those derived from RGB space. This observation supports the hypothesis that manipulation artifacts are more effectively preserved in chrominance information. The ablation study confirms that both multiscale WLD and chroma-based processing contribute positively to the robustness of the proposed framework.

4.6 Discussion

The obtained results indicate consistent classification behavior across both evaluated datasets. The use of cross-validation provides a reliable estimate of model performance and reduces the likelihood of overfitting to a specific data split. High accuracy and AUC values were observed, suggesting effective separation between authentic and manipulated samples. This behavior can be attributed to the ability of the Weber

Local Descriptor to capture local intensity variations that remain affected even after visual post processing. Texture irregularities are preserved at the micro level. These irregularities are effectively encoded through multiscale representation.

The use of chrominance components contributed noticeably to detection performance. Manipulation artifacts are often less visible in luminance but remain embedded within color components. By focusing on Cb and Cr channels, subtle inconsistencies were retained and utilized during feature extraction. This design choice allowed the framework to detect both copy-move and splicing forgeries under varying conditions. The improvement is evident in stable performance across both datasets. Kernel selection also influenced classification behavior. Linear separation was sufficient for the CASIA dataset, indicating that extracted features form a relatively structured feature space. In contrast, the MICC dataset required a nonlinear decision boundary, which was better handled by the Gaussian kernel. This variation reflects differences in manipulation complexity and dataset characteristics. The classifier adapts based on feature distribution.

Confusion matrix analysis further supports these observations. A low number of false positives and false negatives was recorded in both datasets. Most samples were correctly classified. Misclassifications were limited and appear to be associated with cases involving subtle manipulations or complex background textures. Such conditions may reduce the distinctiveness of local descriptors. The overall error distribution remains balanced. The ROC analysis confirms the stability of the proposed framework. AUC values remained consistently high across both datasets. This indicates that the classifier maintains reliable performance across different threshold settings. The model does not exhibit sensitivity to threshold variation.

Failure cases were primarily observed in images containing complex textures or minimal manipulation. In such scenarios, the difference between authentic and manipulated regions becomes less pronounced, which reduces the discriminative capability of texture descriptors. In addition, images with smooth regions or uniform intensity may not provide sufficient local variation for reliable feature extraction. These conditions contribute to false positive and false negative predictions observed in the confusion matrix analysis.

In comparison with existing methods, the proposed approach achieves comparable performance to existing methods while requiring lower computational resources. Methods reporting higher accuracy often rely on more complex feature representations or deep learning architectures, which increase computational requirements. The present framework maintains a balance between performance and computational simplicity. Feature extraction remains lightweight. Training requirements are moderate. The proposed framework is suitable for practical image authentication scenarios where prior information is not available. It can be applied in domains such as digital forensics, media verification, and content authenticity assessment. The reliance on handcrafted features and non-iterative classification makes the method applicable in environments with limited computational resources. This is particularly relevant for large-scale screening systems and real-time verification tasks. This suggests that the proposed framework is well suited for lightweight forensic applications, while deep learning approaches remain advantageous for large-scale and high-complexity detection tasks.

Despite the observed performance, several limitations should be considered. The proposed framework relies on handcrafted texture descriptors, which may not fully capture complex manipulation patterns introduced by advanced editing techniques. In such cases, feature representation may become less discriminative. Performance may also be affected under heavy compression or aggressive post-processing operations. Compression algorithms tend to smooth local intensity variations, which can reduce the effectiveness of texture-based descriptors. As a result, subtle manipulation artifacts may become less distinguishable.

In addition, the evaluation was conducted within individual datasets using cross-validation. Although this provides reliable performance estimates, it does not fully reflect generalization across unseen datasets. Differences in image quality, acquisition conditions, and manipulation characteristics may influence performance when applied to external data. Scalability is another consideration. The feature extraction process operates on the full image and involves multiscale analysis, which increases computational cost for high-resolution images. While the method remains efficient compared to deep learning approaches, processing time may increase with image size and dataset scale. These limitations

indicate potential directions for future work, including evaluation across diverse datasets, integration with complementary feature representations, and optimization of feature extraction for large-scale applications.

Overall, the integration of multiscale WLD features with SVM classification demonstrates stable and reliable performance for passive image forgery detection. The results support the effectiveness of chroma-based texture analysis in identifying manipulation artifacts across different forgery scenarios.

4.7 Comparative Analysis with Existing Methods

The proposed framework was compared with previously reported methods using CASIA v2.0 and MICC F2000 datasets. Unlike deep that learning-based approaches, the proposed method does not rely on end-to-end training and therefore avoids dependence on large annotated datasets. Evaluation metrics included classification accuracy, true positive rate, and area under the ROC curve as presented in Table 8. Some methods in the literature do not report all evaluation metrics. Missing values are indicated where results are not available in the original studies.

Table 8. Comparative Results with State of the Art Methods on CASIA v2.0 Dataset.

Method	ACC (%)	TPR (%)	AUC
Proposed (Multiscale WLD + SVM)	**97.0**	**98.4**	**0.98**
alZahir and Hammad [34]	90.00	–	–
Farid [33]	97.50	98.45	0.97
Mahmood et al. [35]	99.00	99.55	0.99

For the CASIA v2.0 dataset, the proposed approach achieved an accuracy of 97.0% with a true positive rate of 98.4% and an AUC value of 0.98. Several existing approaches reported competitive results. alZahir and Hammad [34] achieved an accuracy of 90.00%. Farid [33] reported an accuracy of 97.50% with a true positive rate of 98.45 % and an AUC value of 0.97. Mahmood et al. [35] reported the highest accuracy of 99.00% with a true positive rate of 99.55%. The proposed method demonstrates competitive performance across benchmark datasets. The results indicate that multiscale WLD features combined with SVM classification provide reliable detection of image manipulations.

This analysis highlights that feature-based methods remain relevant in scenarios where computational resources are limited.

The comparative analysis indicates that the proposed method achieves consistent performance across both datasets. For the CASIA v2.0 dataset, the accuracy and AUC values remain comparable to existing approaches. Some methods report higher accuracy values, which may be attributed to the use of more complex feature representations or deep learning architectures. These approaches typically rely on large training datasets and higher computational cost. In contrast, the proposed framework employs a handcrafted feature representation based on multiscale texture analysis. This results in stable performance while maintaining lower computational requirements. The observed performance difference is therefore associated with the trade-off between model complexity and efficiency.

For the MICC F2000 dataset, the proposed method demonstrates strong detection capability for copy-move forgery. The high true positive rate indicates that the multiscale representation effectively captures duplication artifacts. Variations in reported results across studies may also arise from differences in preprocessing steps, evaluation protocols, and dataset characteristics. Overall, the proposed method provides a balanced performance across different manipulation types without requiring large-scale training data or complex model architectures.

5 Conclusion

This study presented a passive image forgery detection framework based on chroma analysis and multiscale Weber Local Descriptor features. The method operates without embedded authentication information and relies on intrinsic texture characteristics for classification. Feature extraction was performed on chrominance components, and classification was carried out using a Support Vector Machine under a cross-validated evaluation setting.

Experimental results demonstrated consistent performance across benchmark datasets. The proposed framework achieved an accuracy of 97.0% on the CASIA v2.0 dataset, with a true positive rate of 98.4% for spliced image detection. On the MICC F2000 dataset, an accuracy of 97.4% was achieved, with a true positive rate of 99.7% for copy-move forgery detection. The AUC values reached 0.98 for both datasets. These results indicate that multiscale texture representation combined with chroma-based analysis can effectively capture manipulation artifacts. The framework maintains a balance between detection capability and computational simplicity. Feature extraction remains efficient, and the classification

model does not require large-scale training data.

At the same time, certain limitations can be noted. Performance may be affected under severe post-processing conditions, and handcrafted descriptors may not fully represent highly complex manipulation patterns. Future work may focus on integrating hybrid feature representations and exploring advanced learning-based classifiers to improve generalization. Cross-dataset evaluation and dimensionality reduction strategies may also be considered to enhance scalability. Overall, the proposed approach provides a reliable and efficient solution for passive image forgery detection across different manipulation scenarios.

Data Availability Statement

The datasets used in this study are publicly available. The CASIA v2.0 dataset can be accessed via the Kaggle repository provided by the Institute of Automation, Chinese Academy of Sciences, China: https://www.kaggle.com/datasets/divg07/casia-20-image-tampering-detection-dataset.

The MICC-F2000 dataset is available from the Visual Information Processing and Protection Group at the University of Florence: http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/.

Both datasets were used without modification for model training and evaluation.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

AI Use Statement

The authors declare that no generative AI was used in the preparation of this manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Sharma, P., Kumar, M., & Sharma, H. (2023). Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. *Multimedia Tools and Applications, 82*(12), 18117-18150. [CrossRef]

[2] Singh, S., & Kumar, R. (2024). Image forgery detection: comprehensive review of digital forensics approaches. *Journal of Computational Social Science, 7*(1), 877-915. [CrossRef]

[3] Agarwal, S., Sharma, D., Girdhar, N., Kim, C., & Jung, K. H. (2025). A survey of image forensics: Exploring forgery detection in image colorization. *Computers, Materials & Continua, 84*(3), 4195-4221. [CrossRef]

[4] Zhao, X., Li, S., Wang, S., Li, J., & Yang, K. (2012). Optimal chroma-like channel design for passive color image splicing detection. *EURASIP Journal on Advances in Signal Processing, 2012*(1), 240. [CrossRef]

[5] Parekh, R. (2025). *Principles of multimedia*. CRC Press. [CrossRef]

[6] Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital investigation, 10*(3), 226-245. [CrossRef]

[7] Thakur, R., & Rohilla, R. (2020). Recent advances in digital image manipulation detection techniques: A brief review. *Forensic science international, 312*, 110311. [CrossRef]

[8] Burger, W., & Burge, M. J. (2022). *Digital image processing: An algorithmic introduction*. Springer Nature. [Link]

[9] Tyagi, S., & Yadav, D. (2023). A detailed analysis of image and video forgery detection techniques. *The Visual Computer, 39*(3), 813-833. [CrossRef]

[10] Timothy, D. P., & Santra, A. K. (2024). Detecting Digital Image Forgeries with Copy-Move and Splicing Image Analysis using Deep Learning Techniques. *International Journal of Advanced Computer Science & Applications, 15*(5). [CrossRef]

[11] Kaur, G., Singh, N., & Kumar, M. (2023). Image forgery techniques: a review. *Artificial Intelligence Review, 56*(2), 1577-1625. [CrossRef]

[12] Shallal, I., Rzouga Haddada, L., & Essoukri Ben Amara, N. (2025). Image forgery detection with focus on copy-move: An overview, real world challenges and future directions. *Applied Sciences, 15*(21), 11774. [CrossRef]

[13] Ganguly, S., Mandal, S., Malakar, S., & Sarkar, R. (2023). Copy-move forgery detection using local tetra pattern based texture descriptor. *Multimedia Tools and Applications, 82*(13), 19621-19642. [CrossRef]

[14] Xu, Y., Zheng, J., Fang, A., & Irfan, M. (2023). Feature enhancement and supervised contrastive learning for image splicing forgery detection. *Digital Signal Processing, 136*, 104005. [CrossRef]

[15] Chen, J., Shan, S., He, C., Zhao, G., Pietikäinen, M., Chen, X., & Gao, W. (2009). WLD: A robust local image descriptor. *IEEE transactions on pattern analysis and machine intelligence, 32*(9), 1705-1720. [CrossRef]

[16] Nadimpalli, A. V., & Rattani, A. (2024). Social

media authentication and combating deepfakes using semi-fragile invisible image watermarking. *Digital Threats: Research and Practice, 5*(4), 1-30. [CrossRef]

[17] Qazi, T., Ali, M., Hayat, K., & Magnier, B. (2022). Seamless copy–move replication in digital images. *Journal of Imaging, 8*(3), 69. [CrossRef]

[18] Li, H., Wang, L., Zhao, T., & Zhao, W. (2024). Local-peak scale-invariant feature transform for fast and random image stitching. *Sensors, 24*(17), 5759. [CrossRef]

[19] Fridrich, J., Soukal, D., & Lukas, J. (2003, August). Detection of copy-move forgery in digital images. In *Proceedings of digital forensic research workshop* (Vol. 3, No. 2, pp. 652-63). [Link]

[20] Popescu, A. C., & Farid, H. (2004). Exposing digital forgeries by detecting duplicated image regions. [Link]

[21] Bay, H., Tuytelaars, T., & Van Gool, L. (2006, May). Surf: Speeded up robust features. In *European conference on computer vision* (pp. 404-417). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[22] 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]

[23] 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]

[24] 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]

[25] Asghar, K., Sun, X., Rosin, P., Saddique, M., Hussain, M., & Habib, Z. (2019). Edge-texture feature based image forgery detection with cross dataset evaluation. *Machine Vision and Applications, 30*(7-8), 1243-1262. [CrossRef]

[26] Yang, Z., Liu, B., Bi, X., Xiao, B., Li, W., Wang, G., & Gao, X. (2024). D-Net: A dual-encoder network for image splicing forgery detection and localization. *Pattern Recognition, 155*, 110727. [CrossRef]

[27] Hussain, M., Saleh, S. Q., Aboalsamh, H., Muhammad, G., & Bebis, G. (2014, June). Comparison between WLD and LBP descriptors for non-intrusive image forgery detection. In *2014 IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA) Proceedings* (pp. 197-204). IEEE. [CrossRef]

[28] Guido, R., Ferrisi, S., Lofaro, D., & Conforti, D. (2024). An overview on the advancements of support vector machine models in healthcare applications: a review. *Information, 15*(4), 235. [CrossRef]

[29] Saleh, S. Q., Hussain, M., Muhammad, G., & Bebis, G. (2013, July). Evaluation of image forgery detection using multi-scale weber local descriptors. In *International symposium on visual computing* (pp. 416-424). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[30] Ryu, S. J., Kirchner, M., Lee, M. J., & Lee, H. K. (2013). Rotation invariant localization of duplicated image regions based on Zernike moments. *IEEE Transactions on Information Forensics and Security, 8*(8), 1355-1370. [CrossRef]

[31] CASIA 2.0 image tampering detection dataset. (n.d.). Kaggle. Retrieved March 18, 2026, from [Link]

[32] MICC-F2000. (n.d.). MICC, University of Florence. [Link]

[33] Farid, H. (2009). Image forgery detection. *IEEE Signal Processing Magazine, 26*(2), 16–25. [CrossRef]

[34] alZahir, S., & Hammad, R. (2020). Image forgery detection using image similarity. *Multimedia Tools and Applications, 79*(39), 28643-28659. [CrossRef]

[35] Mahmood, T., Irtaza, A., Mehmood, Z., & Mahmood, M. T. (2017). Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images. *Forensic science international, 279*, 8-21. [CrossRef]

[36] Diwan, A., Mahadeva, R., & Gupta, V. (2024). Advancing copy-move manipulation detection in complex image scenarios through multiscale detector. *IEEE Access, 12*, 64736-64753. [CrossRef]

Aamir Ali is a dedicated researcher in artificial intelligence, healthcare analytics, and IoT environments. His expertise includes machine and deep learning applications in medical diagnosis, speech recognition, and facial emotion recognition. He has also worked on IoT-focused projects such as malware classification, anomaly detection, and cyberattack prediction. Aamir is passionate about developing AI-driven solutions for early disease detection and improving patient care. He actively contributes to interdisciplinary research across clinical and image data domains. (Email: amirali4436823@gmail.com)

Aamir Raza is currently pursuing a Master's degree in the Department of Information Technology and Management at the Illinois Institute of Technology, Chicago, USA. His research interests include Industrial IoT security, secure software development, DevSecOps practices, and threat modeling. He is particularly focused on integrating software engineering principles with modern cybersecurity approaches to build resilient systems in industrial environments. (Email: araza7@hawk.iit.edu)

Khaleelullah Syed holds a degree in Computer/Information Technology Services Administration and Management from Hellenic American University. His academic background focuses on the management and administration of information technology systems, with interests in the integration of technology within

organizational and service environments. He is associated with research and professional activities related to information systems and digital technologies. (Email: ksyed@hauniv.edu)

Swetank Mohan is affiliated with The University of Texas Rio Grande Valley (UTRGV), USA. His academic and research interests lie in the field of computing and information technologies, with a focus on the application of modern computational methods to real world technological challenges. He has been involved in academic and research activities related to computer science and emerging digital technologies. (Email: Swetank.mohan01@utrgv.edu)

Nikhat Fatima holds a degree in Computer/Information Technology Services Administration and Management from Concordia University, Mequon, Wisconsin, USA. Her academic training centers on the administration and management of information technology services, with an emphasis on the application of computing solutions in organizational contexts. Her interests include information systems, technology management, and digital service infrastructure. (Email: nikhatfatima.lnu@cuw.edu)

Muhammad Umar is a dedicated student with a strong interest in Machine Learning and data-driven technologies. He is actively building his foundation in programming, data analysis, and core ML concepts. Alongside his studies, he explores algorithms and works on small projects to strengthen his practical skills. He remains focused on continuous learning and aims to apply machine learning techniques to solve real-world problems in the future. (Email: Um0888921@gmail.com)

Misbah Ali is a PhD scholar at COMSATS university Islamabad, with research interests in Machine Learning, Deep Learning, Generative Artificial Intelligence, and Software Engineering. Her work focuses on the development of secure, intelligent systems across domains such as healthcare, education, and industrial cyber-security. She has authored multiple peer-reviewed publications and presented her research at international conferences. She also contributes to the academic community as a reviewer for several reputed journals. (Email: talktomisbah.ali@gmail.com)