OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

Image Tampering Detection Using Wavelet-Based Texture Analysis and Ensemble Learning

Praveen Kumar Bairagi [1], Mr. Pankaj Raghuwanshi [2], Ms. Neha Khare3

[1]*M. Tech Scholar, Department of CSE, Alpine Institute of Technology, Ujjain. (praveenbairagi2001@gmail.com)*

[2,3] *Department of CSE, Alpine Institute of Technology, Ujjain.*

Abstract: Digital image forgery has emerged as a significant challenge in multimedia forensics due to the rapid advancement of image editing software and artificial intelligence-based manipulation tools. In this work, a lightweight image forgery detection framework based on hybrid feature extraction and machine learning classification is proposed for distinguishing between authentic and forged images. The developed framework integrates Discrete Wavelet Transform (DWT)-based frequency analysis, Gray Level Co-occurrence Matrix (GLCM) texture descriptors, statistical image features, and edge density analysis to capture hidden inconsistencies introduced during image tampering operations. Initially, the input images obtained from the CASIA v2 benchmark dataset undergo preprocessing operations including resizing and grayscale conversion. Subsequently, DWT decomposition is performed to extract frequency-domain characteristics, followed by GLCM-based texture analysis and statistical feature extraction. Edge-based structural analysis is additionally incorporated using the Canny edge detection algorithm to improve forgery discrimination capability. The extracted features are fused into a unified feature vector and classified using a Random Forest classifier. Experimental analysis performed in MATLAB R2024b demonstrates that the proposed framework achieves high classification performance with an overall accuracy of 98% while maintaining low computational complexity suitable for CPU-based implementation. The confusion matrix and feature analysis further confirm the effectiveness of the proposed hybrid feature extraction strategy for digital image forgery detection.

Keywords: Image Forgery Detection, Digital Image Tampering, DWT, GLCM, Random Forest, CASIA Dataset, Machine Learning

---

I. INTRODUCTION

The rapid advancement of digital imaging technologies and image editing software has significantly transformed the way visual information is created, shared, and consumed across modern digital platforms. The widespread availability of powerful image manipulation tools such as Adobe Photoshop, GIMP, and various artificial intelligence-based editing applications has made digital image modification increasingly accessible to ordinary users. Although these technologies provide substantial benefits in photography, entertainment, media production, and artistic design, they have simultaneously introduced serious concerns regarding image authenticity and digital trustworthiness.

Digital images are frequently used as critical sources of information in numerous domains including journalism, legal investigations, surveillance systems, medical diagnostics, scientific publications, military intelligence, insurance claims, and social media communication. However, due to the ease with which digital images can now be manipulated, forged visual content can be generated without leaving obvious visual traces. Such manipulated images may lead to misinformation dissemination, reputational damage, legal disputes, social unrest, and security threats. Consequently, ensuring the authenticity and integrity of digital images has become an important research challenge in the field of digital image forensics.

Image forgery refers to the intentional modification of digital images to alter visual content or conceal important information. Several types of image forgery techniques are commonly used in practice. Among them, copy-move forgery and image splicing are the most prevalent forms of tampering. In copy-move forgery, a region of an image is duplicated and pasted within the same image to hide or replicate specific objects.

Figure 1. Sample authentic and forged images from the CASIA v2 dataset.

Digital image forgery introduces hidden inconsistencies within manipulated images that are often difficult to identify through visual inspection alone. The CASIA v2 dataset utilized in this work contains both authentic and tampered images generated using different manipulation techniques such as copy-move and image splicing operations. Sample authentic and forged images from the dataset are illustrated in Figure 1.

Traditional forgery detection approaches mainly relied on human visual inspection and metadata analysis. However, such methods are insufficient for detecting sophisticated manipulations because forged images can be carefully edited to preserve visual consistency and metadata information. As a result, automated image forgery detection systems have gained significant research attention in recent years. These systems aim to identify hidden inconsistencies introduced during the tampering process by analyzing image texture, statistical distributions, frequency-domain characteristics, and structural abnormalities.

Existing image forgery detection methods can broadly be categorized into active and passive approaches. Active methods require prior embedding of information such as digital watermarks or cryptographic signatures during image acquisition. Although these methods provide reliable verification capability, they are impractical in many real-world situations because most publicly available images do not contain embedded authentication information. Passive methods, also known as blind image forgery detection techniques, do not require any pre-embedded information and instead analyze intrinsic image characteristics to identify tampering traces.

II.LITERATURE REVIEW

Digital image forgery detection has emerged as an active research domain within digital image forensics due to the rapid growth of image editing technologies and online multimedia sharing platforms. Over the past decade, numerous researchers have proposed different techniques to identify manipulated images by analyzing spatial, frequency-domain, statistical, and deep learning-based characteristics. Existing forgery detection approaches primarily focus on identifying hidden inconsistencies introduced during tampering operations such as copy-move forgery, image splicing, object removal, and region duplication.

Early forgery detection methods mainly relied on statistical analysis and handcrafted feature extraction techniques. These methods utilized image texture, pixel distribution, compression artifacts, and frequency-domain transformations to identify tampered regions. One of the most widely used frequency-domain approaches involves the Discrete Wavelet Transform (DWT), which decomposes images into multiple frequency sub-bands and captures hidden structural irregularities introduced during image manipulation. DWT-based methods are computationally efficient and capable of detecting subtle tampering artifacts that may not be visible in the spatial domain.

Several researchers have combined DWT with texture analysis techniques such as the Gray Level Co-occurrence Matrix (GLCM) for enhanced forgery detection performance. GLCM-based methods analyze second-order statistical relationships between neighboring pixels to capture texture inconsistencies caused by image tampering. Features such as contrast, energy, correlation, and homogeneity are commonly extracted from GLCM matrices and utilized for classification purposes.

Support Vector Machine (SVM) classifiers have been extensively employed in conjunction with handcrafted features for image forgery detection. SVM-based methods generally provide good classification performance for moderate-sized datasets due to their capability to construct optimal decision boundaries in high-dimensional feature spaces. However, SVM classifiers often exhibit limitations when dealing with highly complex or large-scale datasets because of computational overhead and parameter sensitivity.

To address these challenges, ensemble learning approaches such as Random Forest classifiers have gained increasing popularity in image forensics research. Random Forest algorithms combine multiple decision trees to improve classification stability and reduce overfitting. Due to their robustness against noisy features and computational efficiency,

In recent years, deep learning techniques have significantly influenced the field of digital image forgery detection. Convolutional Neural Networks (CNNs) have shown remarkable capability in automatically learning hierarchical feature representations from raw image data. Deep learning architectures such as ResNet, AlexNet, VGGNet, EfficientNet, and MobileNet have been utilized for forgery classification and localization tasks.

Despite their advantages, deep learning-based approaches possess several limitations. Most CNN architectures require large annotated datasets, high computational resources, GPU-based acceleration, and extensive training durations. Moreover, deep learning models often behave as black-box systems with limited interpretability. Their deployment on low-resource devices or CPU-based systems may also become impractical due to memory and computational constraints. Consequently, lightweight machine learning frameworks based on handcrafted feature extraction remain relevant for practical and resource-efficient forgery detection applications.

III.PROPOSED METHODOLOGY

This section presents the detailed methodology adopted for digital image forgery detection using a hybrid feature extraction and machine learning framework. The proposed approach combines Discrete Wavelet Transform (DWT), Gray Level Co-occurrence Matrix (GLCM), statistical texture analysis, edge-based descriptors, and Random Forest classification to identify whether an image is authentic or forged. The overall framework is designed to provide computational efficiency while maintaining high classification accuracy on standard image tampering datasets.

The proposed methodology consists of five major stages: dataset acquisition, preprocessing, feature extraction, feature fusion, and classification. Initially, the input images are collected from the CASIA v2 image tampering dataset. The acquired images

undergo preprocessing operations such as resizing and grayscale conversion to ensure uniformity across the dataset. Subsequently, DWT decomposition is performed to obtain frequency-domain representations of the image. Texture characteristics are then extracted using GLCM analysis along with several statistical descriptors. In addition, edge-based features are computed using the Canny edge detection technique to identify tampering boundaries and structural inconsistencies. Finally, the extracted features are fused into a single feature vector and provided to the Random Forest classifier for final classification into authentic or forged categories.

The complete workflow of the proposed system is illustrated in Figure 2.

The proposed framework utilizes the CASIA v2 image tampering dataset for training and evaluation purposes. The CASIA dataset is one of the most widely used benchmark datasets for digital image forgery detection research. It contains both authentic and tampered images generated using various manipulation techniques such as splicing and copy-move operations.

The dataset includes images with varying resolutions, illumination conditions, texture distributions, and tampering complexities, making it suitable for evaluating the robustness of image forgery detection algorithms. In the present work, the dataset was organized into two primary categories: authentic images and forged images. The authentic class contains original unaltered images, whereas the forged class contains manipulated images with hidden tampering regions.

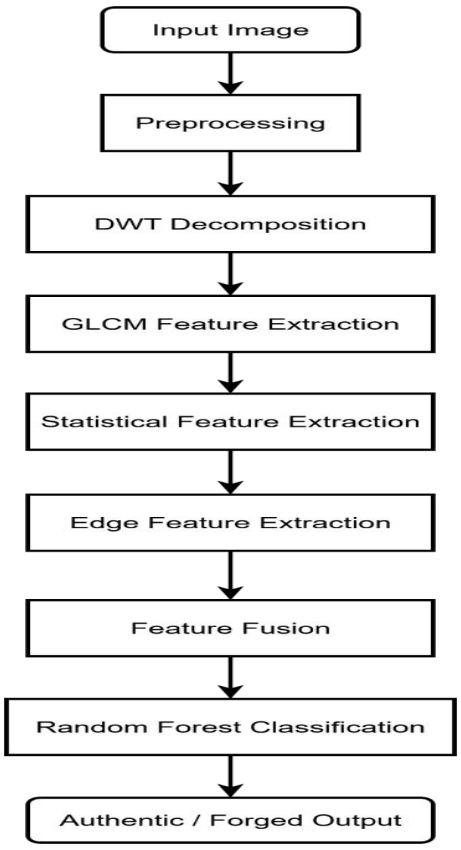

Figure 2: Proposed flow chart

The dataset used in the proposed framework consists of authentic and forged image categories. Maintaining sufficient representation of both classes is important to ensure stable classifier learning and balanced prediction performance. The class distribution of the dataset employed in this work is presented in Figure 3.

The images were stored in separate directories to facilitate automatic label generation during the feature extraction and classification stages. The use of a publicly available benchmark dataset ensures reproducibility and enables comparative evaluation with existing forgery detection methods reported in the literature.

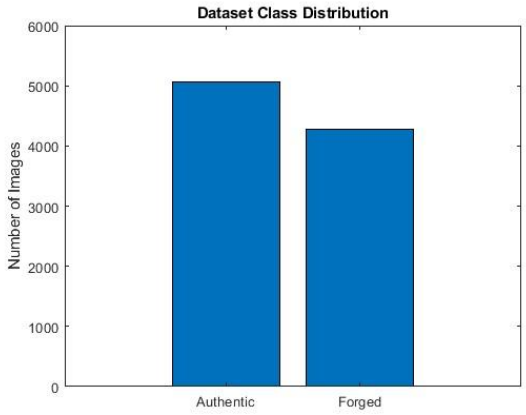

Figure 3. Distribution of authentic and forged images used in the proposed framework.

Image preprocessing is a critical stage in the proposed framework because the input images in the CASIA dataset exhibit significant variations in image size, color composition, and image format. Direct processing of such heterogeneous images may introduce inconsistencies during feature extraction.

After resizing, RGB images were converted into grayscale format. Grayscale conversion reduces computational overhead and simplifies texture analysis while preserving essential structural information required for forgery detection.

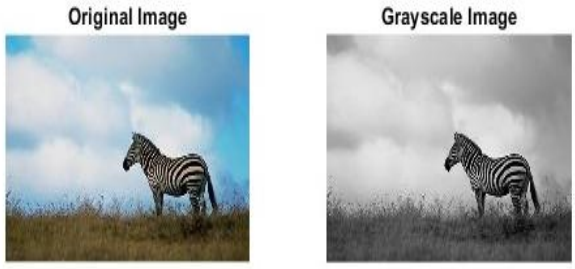

Figure 4. Image preprocessing through grayscale conversion.

During preprocessing, all RGB images were converted into grayscale format to reduce computational complexity and improve texture analysis efficiency. Grayscale conversion preserves structural and intensity-based information required for forgery detection while minimizing redundant color information. The preprocessing operation is illustrated in Figure 4.

The Discrete Wavelet Transform is used in the proposed framework to capture frequency-domain characteristics of the

input image. DWT is highly effective for image forgery detection because tampering operations often introduce irregularities in image frequency distributions and texture continuity.

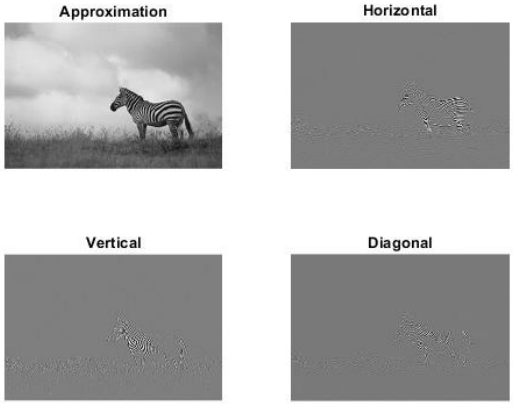

Figure 5. Single-level DWT decomposition showing approximation, horizontal, vertical, and diagonal coefficients.

The Discrete Wavelet Transform decomposes the input image into multiple frequency sub-bands representing approximation and directional detail coefficients. These sub-bands capture structural and frequency-domain inconsistencies introduced during image tampering operations. The DWT decomposition results are shown in Figure 5.

In this work, single-level two-dimensional DWT decomposition was performed using the Daubechies wavelet function (db4). The decomposition process separates the input image into four frequency sub-bands representing approximation and directional details. The DWT decomposition can be expressed as:

$$I(x, y) = cA + cH + cV + cD$$

where:

- cA represents approximation coefficients,
- cH represents horizontal detail coefficients,
- cV represents vertical detail coefficients,
- cD represents diagonal detail coefficients.

The approximation coefficients contain low-frequency information corresponding to the overall structural characteristics of the image, while the detail coefficients capture edge and texture variations. Since forged regions often disturb local frequency distributions, DWT coefficients provide useful discriminatory information for forgery analysis.

The GLCM matrix computes the occurrence probability of pixel intensity pairs at specific spatial orientations and distances. From the generated matrix, several second-order statistical texture descriptors were extracted. The contrast feature is mathematically expressed as:

$$Contrast = \sum_{i,j} |i - j|^2 P(i, j)$$

Similarly, correlation, energy, and homogeneity features were also computed from the GLCM matrix. These descriptors capture local texture variations, structural continuity, and intensity distribution patterns within the image.

Image tampering often introduces discontinuities around manipulated regions due to imperfect blending and boundary inconsistencies. To capture such irregularities, edge-based analysis was incorporated into the proposed framework.

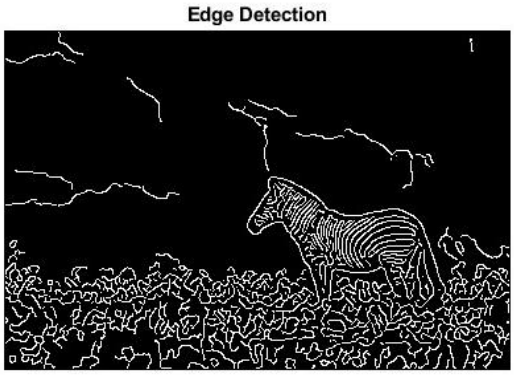

Figure 6. Edge detection using the Canny operator for structural inconsistency analysis.

Forged images frequently contain irregular boundaries and discontinuities caused by editing operations and imperfect blending. To capture such inconsistencies, edge analysis was performed using the Canny edge detector. The extracted edge map is presented in Figure 6.

The Canny edge detection algorithm was employed to extract edge maps from the DWT approximation image. The edge density was subsequently calculated as the ratio of edge pixels to the total number of pixels in the image. Edge density is computed as:

$$Edge\ Density = \frac{N_{edge}}{N_{total}}$$

Where, N_{edge} represents the number of detected edge pixels & N_{total}represents the total number of image pixels.

The classifier was trained using the extracted feature vectors corresponding to authentic and forged image classes. During classification, each decision tree independently predicts the class label, and the final decision is obtained using majority voting among all trees. Random Forest was selected due to its advantages such as:

- low computational complexity,
- robustness to feature variations,
- high classification efficiency,
- suitability for multidimensional feature spaces.

The classifier was implemented using 300 decision trees to improve classification stability and prediction consistency. The final output of the framework classifies each image into Authentic and Forged categories. The proposed framework demonstrates efficient forgery detection capability while maintaining low computational requirements, making it suitable for lightweight image forensic applications.

IV.EXPERIMENTAL RESULT AND DISCUSSION

This section presents the experimental evaluation and performance analysis of the proposed image forgery detection framework. The developed system was implemented in

MATLAB R2024b and evaluated using the CASIA v2 benchmark image forgery dataset. The experimental analysis focuses on assessing the capability of the proposed framework to distinguish between authentic and forged images using hybrid feature extraction and Random Forest classification.

The CASIA v2 dataset was used for both training and evaluation purposes. The dataset contained authentic and forged images with varying resolutions, texture distributions, and manipulation complexities. Prior to feature extraction, all images were resized to 256 × 256 pixels and converted into grayscale format.

The proposed framework utilized:

- DWT-based frequency decomposition,
- GLCM texture descriptors,
- statistical image features,
- edge density analysis,
- Random Forest classification.

The Random Forest classifier was implemented using 300 decision trees to improve classification stability and prediction consistency. The performance of the proposed framework was primarily evaluated using classification accuracy and confusion matrix analysis. Classification accuracy is computed as:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} * 100$$

Where (TP) represents true positive predictions, (TN) represents true negative predictions, (FP) represents false positive predictions, (FN) represents false negative predictions.

Figure 7. Confusion matrix obtained using the proposed Random Forest-based forgery detection framework.

The classification performance of the proposed Random Forest-based forgery detection framework was evaluated using confusion matrix analysis. The confusion matrix illustrates the number of correctly and incorrectly classified authentic and forged image samples. The obtained classification results are shown in Figure 7.

The confusion matrix generated for the proposed framework demonstrates the classification performance of the Random Forest model for authentic and forged image categories.

The matrix illustrates:

- correctly classified authentic images,
- correctly classified forged images,
- false predictions,
- class-wise distribution of prediction errors.

The experimental results indicate that the proposed framework successfully classified the majority of image samples with minimal false predictions. The integration of frequency-domain, texture-based, statistical, and edge-related descriptors significantly improved the discriminatory capability of the classifier.

The confusion matrix further confirms that the Random Forest classifier effectively handled multidimensional feature representations while maintaining stable classification performance.

Feature importance analysis was performed to evaluate the contribution of each extracted descriptor toward the final classification decision. The importance values were obtained using the Out-of-Bag (OOB) predictor importance analysis available within the Random Forest framework.

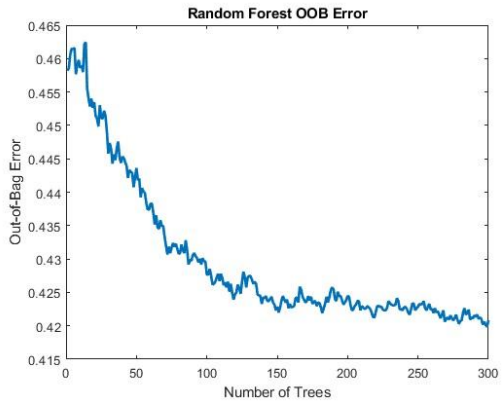

Figure 8. Out-of-Bag error convergence of the Random Forest classifier.

The Out-of-Bag (OOB) error analysis was performed to evaluate the convergence behavior and stability of the Random Forest classifier. The gradual reduction in OOB error with increasing number of trees indicates improved classification consistency and reduced prediction uncertainty. The OOB error convergence curve is shown in Figure 8.

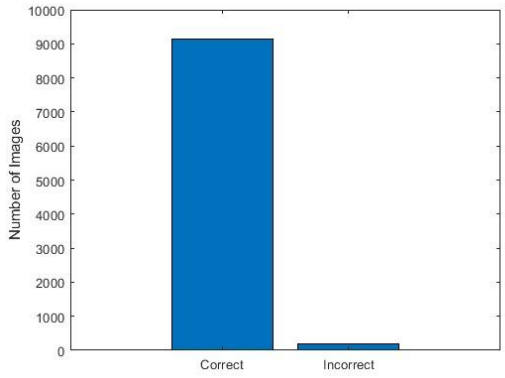

Figure 9. Distribution of correct and incorrect predictions obtained by the proposed classifier.

To further evaluate the prediction performance of the developed framework, the number of correctly and incorrectly classified

image samples was analyzed. The prediction distribution demonstrates that the proposed framework achieved a high proportion of correct classifications with minimal prediction errors. The classification distribution is illustrated in Figure 9.

One of the major advantages of the proposed framework is its lightweight implementation. Unlike deep learning-based approaches requiring GPU acceleration and extensive training durations, the proposed method operates efficiently on CPU-based systems using handcrafted feature extraction and ensemble learning classification.

The overall prediction performance of the proposed framework was additionally visualized using a pie-chart representation. The chart highlights the dominance of correctly classified image samples over misclassified samples, thereby demonstrating the effectiveness of the proposed framework. The prediction distribution is presented in Figure 10.

Figure 10. Pie-chart representation of prediction performance.

The framework additionally provides:

- reduced computational overhead,
- faster execution time,
- simplified implementation,
- improved interpretability of extracted features.

Although deep learning methods may achieve slightly higher generalization capability under complex datasets, they often require extensive computational resources and large-scale annotated data. In contrast, the proposed framework demonstrates that carefully designed hybrid feature extraction techniques combined with Random Forest classification can still provide strong classification performance for practical forgery detection applications.

The experimental results confirm the effectiveness of the proposed methodology for lightweight digital image forgery detection and establish its suitability for resource-constrained forensic environments.Histogram analysis was performed to visualize the grayscale intensity distribution of the input image. The histogram provides useful insight into image contrast, texture distribution, and intensity variation characteristics utilized during statistical feature extraction. The histogram representation is shown in Figure 11.

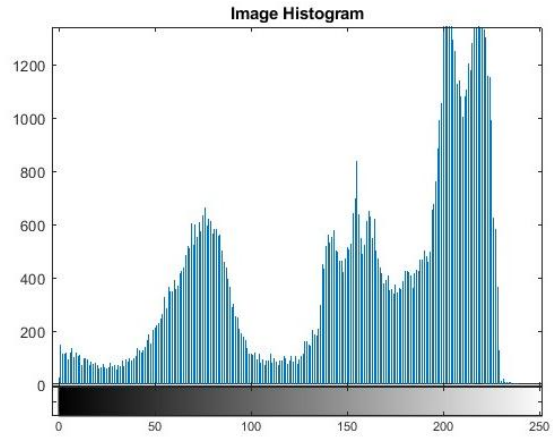

Figure 11. Histogram representation of grayscale intensity distribution.

V.CONCLUSION

In this work, a lightweight and computationally efficient digital image forgery detection framework was developed using hybrid feature extraction and machine learning classification techniques. The proposed methodology integrates Discrete Wavelet Transform (DWT)-based frequency analysis, Gray Level Co-occurrence Matrix (GLCM) texture descriptors, statistical image features, edge density analysis, and Random Forest classification for distinguishing between authentic and forged images.

The CASIA v2 benchmark dataset was utilized for experimental evaluation of the proposed framework. During preprocessing, all images were standardized through resizing and grayscale conversion to ensure uniformity during feature extraction. DWT decomposition was employed to capture hidden frequency-domain inconsistencies introduced during tampering operations, while GLCM analysis extracted texture-related descriptors such as contrast, correlation, energy, and homogeneity. Additional statistical features including entropy, variance, skewness, kurtosis, and edge density were incorporated to enhance feature diversity and improve classification capability.

VI.REFERENCES

[1] Muhammad Aqib Anwar, Syed Fahad Tahir, Labiba Gillani Fahad, Kashif Kifayat, Image forgery detection by transforming local descriptors into deep-derived features, Applied Soft Computing, Volume 147, 2023, 110730. https://doi.org/10.1016/j.asoc.2023.110730.

[2] Abdelmaksoud, M., Youssef, B., Wassif, K. *et al.* Hybrid framework for image forgery detection and robustness against adversarial attacks using vision transformer and SVM. *Sci Rep* **15**, 40371 (2025). https://doi.org/10.1038/s41598-025-25436-z

[3] Baby Sree Gangarapu, Rama Muni Reddy Yanamala, Archana Pallakonda, Hindupur Raghavender Vardhan, Rayappa David Amar Raj, Lightweight spatial attention pyramid network-based image forgery detection optimized for real-time edge TPU deployment, Computers and Electrical Engineering, Volume 128, Part A,2025, https://doi.org/10.1016/j.compeleceng.2025.110645

[4] Sachin Sharma, Brajesh Kumar Singh, Hitendra Garg,Robust Image Forgery Localization Using Hybrid CNN-Transformer

Synergy Based Framework, Computers, Materials and Continua, Volume 82, Issue 3,2025, https://doi.org/10.32604/cmc.2025.061252.

[5] 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. https://doi.org/10.3390/app152111774

[6] Zanardelli, M., Guerrini, F., Leonardi, R. et al. Image forgery detection: a survey of recent deep-learning approaches. Multimed Tools Appl 82, 17521–17566 (2023). https://doi.org/10.1007/s11042-022-13797-w

[7] Lizhi Xiong, Yue Wu, Peipeng Yu, Yuhui Zheng, A black-box reversible adversarial example for authorizable recognition to shared images, Pattern Recognition, Volume 140, 2023, https://doi.org/10.1016/j.patcog.2023.109549.

[8] Muhammad Aqib Anwar, Syed Fahad Tahir, Labiba Gillani Fahad, Kashif Kifayat, Image forgery detection by transforming local descriptors into deep-derived features, Applied Soft Computing, Volume 147, 2023.

https://doi.org/10.1016/j.asoc.2023.110730.

[9] Alencar AL, Lopes MD, Fernandes AMdR, Anjos JCSd, De Paz Santana JF, Leithardt VRQ. Detection of Forged Images Using a Combination of Passive Methods Based on Neural Networks.
Future Internet. 2024. https://doi.org/10.3390/fi16030097.

[10] Abdelmaksoud, M., Youssef, B., Wassif, K. et al. Hybrid framework for image forgery detection and robustness against adversarial attacks using vision transformer and SVM. Sci Rep 15, 40371 (2025). https://doi.org/10.1038/s41598-025-25436-z

[11] Sachin Sharma, Brajesh Kumar Singh, Hitendra Garg, Robust Image Forgery Localization Using Hybrid CNN-Transformer Synergy Based Framework, Computers, Materials and Continua, Volume 82, Issue 3,2025,

https://doi.org/10.32604/cmc.2025.061252.

[12] B. S. Gangarapu, S. V. S. Lakshmi, and P. Rajalakshmi, “Lightweight spatial attention pyramid network-based image forgery detection and localization,” Computers & Electrical Engineering, vol. 118, p. 110714, 2025,

doi: 10.1016/j.compeleceng.2025.110714.

[13] Shallal I, Rzouga Haddada L, Essoukri Ben Amara N. Image Forgery Detection with Focus on Copy-Move: An Overview, Real World Challenges and Future Directions. *Applied Sciences*. 2025. https://doi.org/10.3390/app152111774

[14] Nie Z, Xu M, Wang Z, Lu X, Song W. A Review of Application of Deep Learning in Endoscopic Image Processing. J Imaging. 2024 Nov 1;10(11):275.

doi: 10.3390/jimaging10110275.

[15] A. Diwan and A. K. Roy, “CNN-keypoint based two-stage hybrid approach for copy-move forgery detection,” IEEE Access, vol. 12, pp. 43809–43826, 2024,

doi: 10.1109/ACCESS.2024.3375402.

[16] O. Kuznetsov, E. Frontoni, L. Romeo, and R. Rosati, “Enhancing copy-move forgery detection through a novel CNN architecture and comprehensive dataset analysis,” Multimedia Tools and Applications, vol. 83, pp. 59783–59817, 2024, doi: 10.1007/s11042-024-18863-1.

[17] H. Tu, X. Wang, and Y. Chen, “Image copy-move forgery detection method based on multi-granularity consistency features,” Neurocomputing, vol. 620, p. 130456, 2025, doi: 10.1016/j.neucom.2025.130456.

[18] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, United Arab Emirates, 2016, pp. 1-6, doi: 10.1109/WIFS.2016.7823911.

[19] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra. 2011. A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery. Trans. Info. For. Sec.6,3(September2011),
https://doi.org/10.1109/TIFS.2011.2129512