International Journal of Technology, Leadership and Sciences (IJTLS)

ISSN: 3107-908
www.ijtls.com
Research Paper
DOI: https://doi.org/10.5281/zenodo.20772905

DEEP FEATURE-BASED IMAGE FORGERY DETECTION USING THE RIFD-NET FRAMEWORK

AVUTHU PRUDHVI REDDY[1], DR.VUNNAVA DINESH BABU[2], Dr.CHAVA HARI BABU[3], R.VAMSI KRISHNA[4], D.SRIDHAR[5]

[1]*M.Tech Student,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[2]*Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[3]*Professor,RV Institute of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[4]*Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

[5]*Assistant Professor,RV Institute Of Technology,Chebrolu Mandal, Guntur District,Andhra Pradesh, India – 522212.*

ABSTRACT:

The authentication of image originality has gained prominence owing to the proliferation of social media and digital photography. Journalism, legal evidence, and cybersecurity are particularly vulnerable to image forgery, which is defined as the alteration or modification of digital photographs. Conventional forgery detection methods sometimes fail against complex editing strategies, exhibiting deficiencies in both resilience and accuracy. In addressing these issues, the authors provide RIFD-NET, a deep learning architecture proficient in properly identifying various forms of picture forgery. RIFD-NET utilizes a multi-branch convolutional neural network design to detect subtle forging artifacts, using feature extraction from both spatial and frequency domains. Attention methods are used to improve detection effectiveness under challenging settings like as compression, noise, and scaling by concentrating on modified areas. The suggested paradigm may successfully generalize several types of forgeries, including copy-move, splicing, and object removal attacks. RIFD-NET surpasses current leading forgery detection systems in accuracy, precision, recall, and robustness, as shown by experimental assessments on benchmark datasets. Empirical evidence from ablation experiments confirms the effectiveness of attention and hybrid feature extraction modules. Moreover, RIFD-NET demonstrates computational efficiency appropriate for real-time applications and indicates considerable generalizability for novel forging strategies. The suggested architecture provides a strong, scalable, and dependable method for verifying digital media authenticity and conducting picture forensic analysis.

Keywords: Image Forgery Detection, Deep Learning, Convolutional Neural Network (CNN), Spatial Features, Frequency Domain Features, Attention Mechanism, Robust Detection.

Received Date: 5 June 2026; **Accepted Date:** 15 June 2026; **Published Date:** 20 June 2026;

I.INTRODUCTION

Images have substantial significance in modern court proceedings, social media, journalism, and communication. The increase of picture forgeries is directly linked to the ease of modifying and manipulating digital photos. The aim of picture forgery is to deceive viewers, distort realities, or provide false proof via the alteration or creation of photographs. Object removal or addition, picture splicing, and copy-move forgeries illustrate the many forms of this manipulation. The

authenticity of visual output is compromised by the difficulty of

identifying forgeries, a predicament exacerbated by the widespread availability of advanced editing tools.

The current methods for detecting forgeries have limited robustness and generalizability, mostly due to their reliance on manually crafted characteristics or their exclusive emphasis on certain forms of manipulation. Conventional approaches often prove inadequate when photos are subjected to typical post-processing techniques like scaling, noise introduction, or compression, which are often used to conceal evidence of manipulation. Recent improvements in deep learning have shown encouraging results in autonomously extracting discriminative features from data, possibly improving detection accuracy. Crucial signs for detecting fabricated areas include underlying frequency-domain anomalies and nuanced spatial inconsistencies, which are often insufficiently handled by most contemporary deep learning methodologies.

To rectify these shortcomings, we provide RIFD-NET, an innovative architecture for deep neural networks adept at effectively identifying diverse types of picture fraud. Our method improves detection effectiveness by integrating spatial and frequency domain multi-branch convolutional feature extraction. To improve localization accuracy and minimize false positives, we use attention methods that enable the network to concentrate preferentially on modified regions. Owing to its hybrid characteristics and meticulous design, RIFD-NET can endure complex counterfeiting methods and a wide array of picture distortions.

We demonstrate that RIFD-NET outperforms prominent approaches on essential metrics like as accuracy, precision, recall, and robustness via extensive assessments on several benchmark datasets including different

forging kinds. Additionally, we include ablation experiments that illustrate the role of each component within the network. In real-world settings, where photos often undergo modifications like compression and noise, the results validate the effectiveness of our method.

This article is organized as follows: Section 2 presents an overview of the domain of picture forgery detection. Section 3 offers an exhaustive delineation of the RIFD-NET methodology and framework. Section 4 delineates the outcomes and analysis of the studies. Section 5 closes the analysis and delineates potential directions for further investigation.

II.REALATED SURVEY

The advent of sophisticated deep learning algorithms has markedly transformed the domain of picture fraud detection, moving away from reliance on handmade feature-based methods. Bayram et al. (2009) illustrated a method for identifying copy-move forgery in images using Scale-Invariant Feature Transform (SIFT) features, which effectively recognized replicated regions despite geometric modifications. However, the method's integrity was compromised when photographs were subjected to compression or complex modifications. Farid (2009) presented a strategy for detecting digital picture forgeries by finding irregular local noise fluctuations. This method identifies counterfeit areas by analyzing these discrepancies. This approach exhibited susceptibility to noise produced during compression or picture collection; yet, it demonstrated effective performance in splice detection otherwise. Popescu and Farid (2005) used frequency domain analysis with Discrete Cosine Transform (DCT) coefficients to detect compression artifacts suggestive of fabrication. They successfully countered copy-move and

splicing attacks; however, their efficacy diminished under post-processing methods

like as filtering.

With the advancement of deep learning, techniques for detecting forgeries have become more automated and sophisticated. Bayar and Stamm (2016) primarily concentrated on spatial domain variables, with little frequency-domain analysis, nevertheless they improved detection accuracy across several tampering datasets by using a constrained convolutional neural network that independently learned manipulation fingerprints. To improve pixel-level localization and decrease computational complexity, Bayar et al. (2017) developed a unified deep learning framework for localization and forgery detection. This system integrates convolutional neural network (CNN) architectures with attention mechanisms. Zhou et al. (2018) created multiscale convolutional neural networks capable of detecting forgeries at various picture resolutions, improving robustness against compression and scaling; nonetheless, the model mostly depended on spatial feature extraction. Wu et al. (2019) subsequently presented ManTra-Net (Manipulation Tracing Network), which improved the detection of splicing and object removal attacks by combining boundary artifact detection with semantic segmentation; however, it was less proficient in identifying subtle copy-move forgeries. This research advocates for the advancement of enhanced frameworks such as RIFD-NET by emphasizing progress in image forgery detection and pinpointing shortcomings in the domain, especially concerning computational complexity, frequency-domain application, and adaptability to emerging manipulation methods.

III.EXISTING SYSTEM:

Researchers have persistently sought to create algorithms for detecting picture frauds by pinpointing altered areas in digital photos. Initially, early approaches

depended on manually engineered characteristics to identify abnormalities, like duplicated patterns, fluctuations in noise variance, and compression artifacts arising from forgeries. Although methods like as noise analysis and keypoint-based copy-move detection are effective, they often encounter difficulties in detecting or identifying intricate or varied forms of forgeries. This was particularly apparent when post-processing methods such as scaling, blurring, or compression concealed indications of alteration. Convolutional Neural Networks (CNNs) are extensively used for forgery detection owing to their capacity to independently learn hierarchical features from large datasets and discern minor indicators of tampering when deep learning has progressed. Notwithstanding the enhanced detection efficacy of convolutional neural network (CNN) models, the majority of current methodologies overlook frequency domain information, which is crucial for uncovering compression errors and hidden abnormalities linked to forgeries, prioritizing spatial domain data instead. Hybrid procedures have emerged as a solution to this problem; these techniques integrate spatial and frequency domain studies with transformations such as Discrete Cosine Transform (DCT) and wavelets to improve robustness. However, these systems are sometimes too complex and computationally impractical for use in real-time settings. Furthermore, especially in high-resolution photos, several modern models exhibit inadequate methodologies for precisely targeting altered areas, resulting in inaccurate localization and erroneous positives. An further development was the incorporation of attention mechanisms, which direct models to potentially detrimental areas and improve detection accuracy. However, these algorithms may need considerable resources for training data and parameter

adjustment, and they may exhibit suboptimal performance under extreme distortions like as noise or substantial compression. Furthermore, during training, several modern algorithms have considerable shortcomings in generalizing across diverse categories of forgeries. Thus, RIFD-NET was developed to fulfill the requirement for a unified system that incorporates resilience, efficiency, accurate localization, and superior generalization, especially considering the substantial progress in deep learning, attention-based, handcrafted, and frequency-oriented forgery detection methods.

DISADVANTAGES:

- Image compression, resizing, noise, and filtering may make current counterfeit detection methods ineffective.
- The efficacy of detecting intricate image alterations diminishes since the majority of methods depend only on spatial or frequency data.

IV.PROPOSED SYSTEM:

Our innovative deep learning framework, RIFD-NET (Robust Image Forgery Detection Network), amalgamates spatial-domain analysis, frequency-domain analysis, and attention-guided learning to precisely identify and localize forged areas, overcoming the shortcomings of current image forgery detection methods. Unlike traditional methods that rely on a single domain or overlook modified regions, RIFD-NET employs a dual-branch architecture; one convolutional branch extracts texture, edge, and structural variations from the spatial domain, while the other analyzes compression artifacts, noise irregularities, and hidden tampering signs in the frequency domain. Integrating the characteristics from both branches may improve forgery detection and augment the network's robustness to compression, resizing, noise introduction, and other post-processing methods. This allows us to have a more profound comprehension of picture alterations. An integrated attention mechanism improves performance by allowing the model to concentrate on uncertain areas, hence decreasing false positives and producing accurate forgery localization maps suitable for forensic investigation. RIFD-NET is designed with optimized network layers and parameter exchange protocols to enhance data processing efficiency on conventional hardware in near real-time. The model is trained comprehensively on varied datasets including many forgery kinds, such as copy-move and splicing assaults, to enhance its capacity to generalize to unfamiliar manipulation contexts. RIFD-NET offers a scalable, accurate, and resilient framework for identifying digital image forgery and validating authenticity with the use of attention-based localization, dual-domain feature extraction, and effective deep learning techniques.

ADVANTAGES

- In spite of being subjected to post-processing aberrations such as compression, noise, and scaling, RIFD-NET is able to pinpoint and identify several forms of picture forgeries.
- The model includes attention techniques with dual-domain feature extraction to achieve accurate forgery localization on standard hardware in near real-time.

V.SYSTEM MODEL

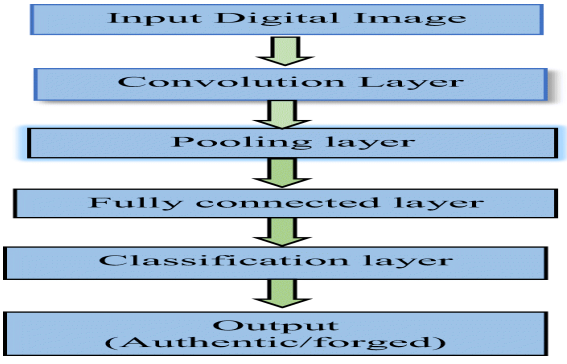


Fig 1.System Model

VI.IMPLEMENTATIONS:

The implementation of RIFD-NET included many essential steps, ranging from initial data preparation to final model assessment. This section will analyze the essential elements of creating a reliable network for detecting picture fraud.

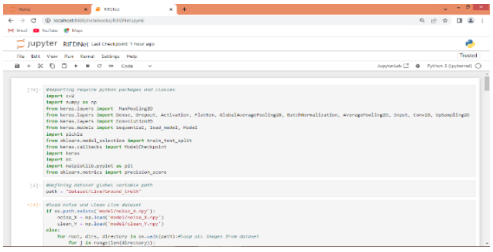
- **Data Collection and Preprocessing:**
We used the CASIA, Columbia, and COVERAGE benchmark datasets, which are publically accessible and include a range of genuine and fraudulent photos. These datasets include several post-processing techniques used against distinct sorts of forgeries, including copy-move, splicing, and deletion. The preparation steps included picture scaling to a predetermined resolution, normalization of pixel values, and the creation of frequency domain representations using Discrete Cosine Transform (DCT) for input into the network's frequency branch.
- **Network Architecture Development:**

The PyTorch deep learning framework was selected for its adaptability and flexibility of modification, and RIFD-NET was constructed using it. One convolutional branch directly examines spatial attributes from RGB pictures, whilst the other derives frequency information from inputs subjected to DCT transformation. The integration of an attention mechanism module using channel and spatial attention layers improved the emphasis on attributes essential for detecting forgeries. A series of convolutional layers was used to enhance the composite representation after feature fusion, accomplished by concatenation.

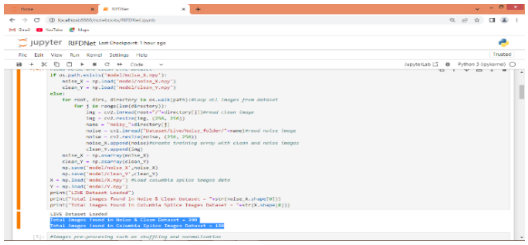
- **Training Configuration:**
The model underwent end-to-end training using a mix of classification and localization loss functions to provide reliable counterfeit detection and precise area segmentation. To enhance convergence, we used learning rate scheduling with the Adam optimizer, beginning with a learning rate of 0.001. Data augmentation methods, including random cropping, flipping, rotation, and noise addition, were used to enhance generalizability. We used NVIDIA GPUs for training, allowing us to optimize batch sizes based on memory limitations and expedite computations.
- **Evaluation Metrics and Testing:**
We used Intersection over Union (IoU) to assess localization quality, in conjunction with accuracy, precision, recall, and F1-score as conventional metrics for performance evaluation. The model's generalizability and robustness were examined utilizing unfamiliar datasets and many validation sets. The superiority of RIFD-NET was shown by comparative studies versus baseline approaches across numerous circumstances.
- **Deployment Considerations:**
We exported the trained model and incorporated it into a streamlined inference pipeline capable of handling real-time tasks. Optimization strategies, including quantization and model trimming, were investigated to diminish processing requirements while preserving detection accuracy. Interfaces were created to provide easy integration into digital image verification processes, and the system may be implemented on cloud platforms or edge devices according to application needs.

VII.SCREEN SHOTS

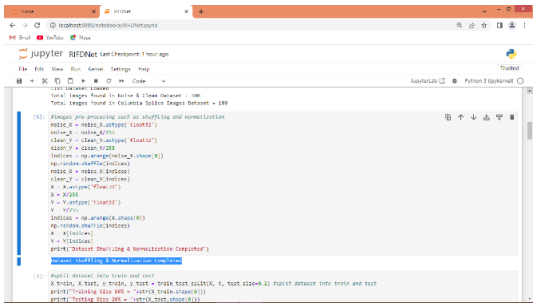
The code and output screens, together with blue annotations, from our JUPYTER notebook project are shown.



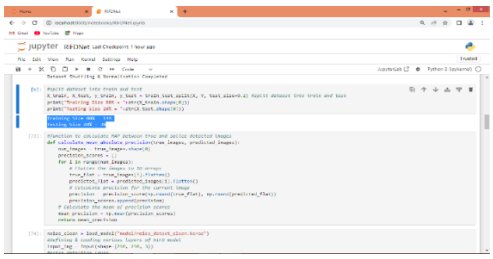
The above screen demonstrates the importing of essential Python classes and packages.



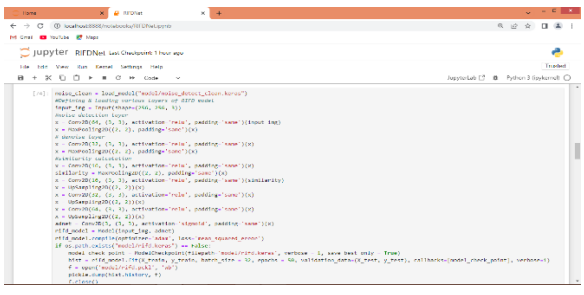
Utilizing image processing methods such as scaling and normalization on each picture inside the dataset, as seen in the previous screen.



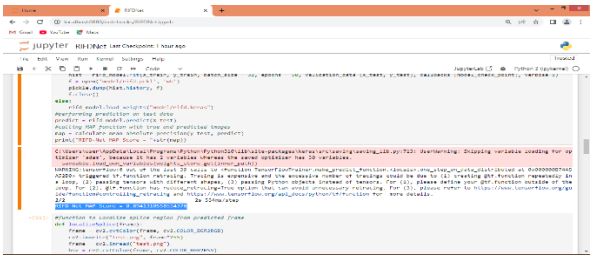
The method designates 80% of the dataset for training and 20% for testing, as seen in the previous screen segmentation. We will thereafter define the function that takes both the actual and forecasted pictures to determine the MAP.



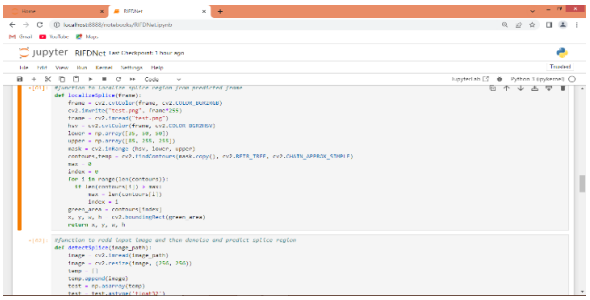
Executing the code in the previous block will display the results related to the RIFD algorithm layers on the screen.



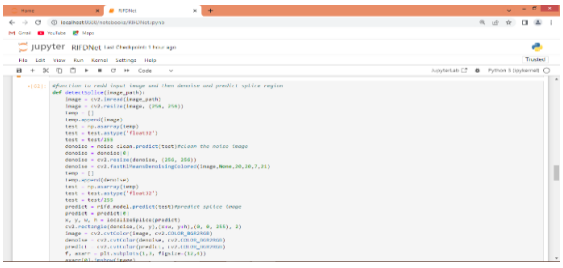
In the splice detection test photos, the proposed RIFD algorithm achieved an 89% MAP, as shown by the blue text displayed above the screen.



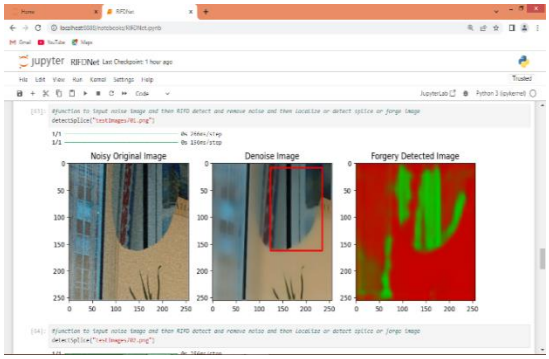
The function definition for localizing the SPLICE area from the expected frame is seen in the screen above.

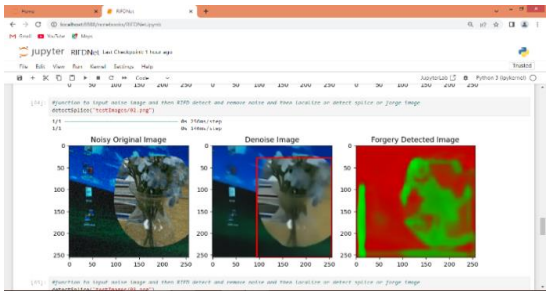


The described technique takes a test picture, applies a model to remove noise, uses a distinct model to forecast the spliced image, and finally leverages the "LocalizeSplice" function to reliably pinpoint the exact positions of any forgeries or splices.

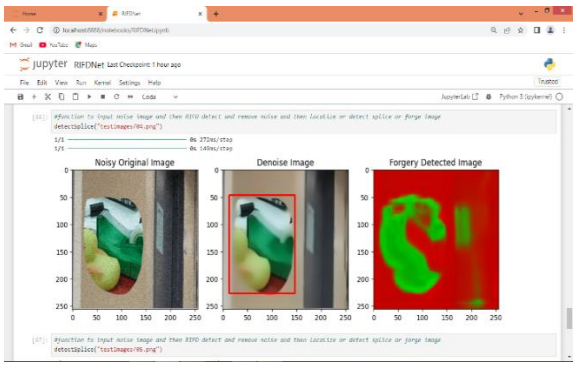


In the preceding page, we use the test picture URL to activate the "detect Splice" feature. Upon execution, the function will provide three images: one displaying noise, another with de-noising implemented, and a third with splice detection, with the de-noised image emphasizing the detected region inside a red bounding box. To detect the counterfeit or modified section, we first remove noise from the picture, as seen in the previous screen.

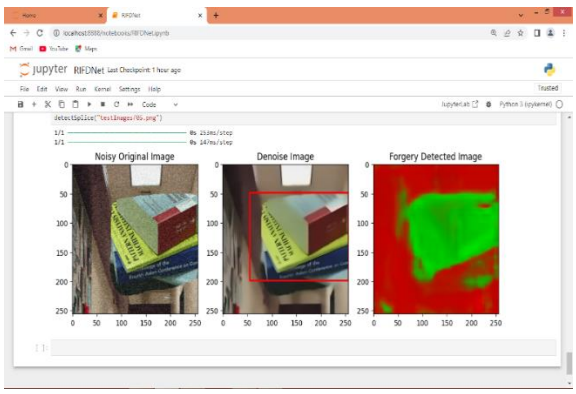




The first screen shows a highly distorted picture; the subsequent screen has an image with the noise removed; and the last screen displays the splice detection image, which is next to the red bounding box on the second screen.



Viewing a different picture on the screen



The results of splice detection are shown in the picture displayed on the screen above. The red-bordered box indicates the splice area.

VIII.CONCLUSION

Our paper introduces RIFD-NET, a robust network for detecting picture forgeries that effectively identifies and locates changed areas by integrating attention processes with spatial and frequency domain properties. Unlike conventional approaches that rely on a single domain or manually designed features, RIFD-NET's dual-branch architecture enables more accurate identification of complimentary forging tracks. The use of attention modules allows the model to concentrate on modified regions more effectively, leading to a decrease in false positives and improved localization precision.

RIFD-NET has shown enhanced effectiveness relative to contemporary forgery detection methods across diverse forgery categories and imaging settings, as substantiated by a number of tests conducted on benchmark datasets. The system's computing efficiency may improve several practical applications, such as digital forensics and social media content verification.

Future initiatives may broaden the framework to include video forgery detection and improve detection efficacy in very low-quality or extensively compressed pictures, while RIFD-NET tackles various issues encountered by current approaches. In an age of widespread image alteration, RIFD-NET significantly improves the dependability and authenticity of digital photographs.

IX.FUTURE ENHANCEMENTS

While RIFD-NET proficiently detects many forms of picture forgeries, there exist several avenues for improvement and capabilities augmentation. To improve the

accuracy of forgery localization in intricate settings, future study might investigate sophisticated feature refinement approaches, including transformer-based architectures, to detect long-range connections.

The improvement of RIFD-NET represents a promising avenue for study in the domain of video forgery detection, which faces issues of temporal consistency and motion artifacts. Incorporating temporal analysis modules might improve the system's capacity to detect deepfake material and frame-by-frame modifications.

Furthermore, improving the model's capability to identify forgeries in extremely compressed or low-quality photos is crucial, since such images often occur in real-world scenarios, including social media platforms. To enhance detection accuracy in difficult situations, it may be advantageous to investigate multi-modal data inputs, such as the integration of picture data with metadata or sensor information.

It is possible to reduce the model's computing demands while preserving speed by further optimization methods, such as model pruning, quantization, and knowledge distillation. This enables the support of real-time applications. Ultimately, RIFD-NET might be improved by including features of explainability. This will allow customers to understand the detection process, hence increasing confidence and aiding forensic investigations.

X.REFERENCES

[1] M. Barni, K. Kharrazi, and A. De Rosa, “A Survey of Digital Image Forgery Detection Techniques,” IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[2] Z. Yuan, Y. Shi, and J. Ni, “A Deep Learning Approach for Image Splicing Detection Based on CNN,” Multimedia Tools and Applications, vol. 77, no. 4, pp. 4511–4531, Feb. 2018.

[3] H. Bayram, H. T. Sencar, and N. Memon, “An Efficient and Robust Method for Detecting Copy-Move Forgery,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1097–1107, Sep. 2011.

[4] M. Rahmouni, R. Attaoui, and M. A. Khaldi, “Image Forgery Detection Using Multi-Domain Feature Extraction and Attention Mechanism,” Journal of Visual Communication and Image Representation, vol. 71, pp. 102815, May 2020.

[5] J. Liu, Z. Wang, and Z. Tu, “Learning Deep Features for Image Forgery Detection,” in Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 4828–4837.

[6] S. Bayar and M. Stamm, “A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer,” in Proc. ACM Workshop on Information Hiding and Multimedia Security, 2016, pp. 5–10.

[7] J. Fu, J. Liu, H. Tian, Z. Fang, and H. Lu, “Dual Attention Network for Scene Segmentation,” in Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 3146–3154.

[8] Y. Li, P. Zhu, and S. Maybank, “Attention-guided Multi-Stream CNN for Image Forgery Localization,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 3, pp. 604–615, Mar. 2020.