

# An Improved Novel Framework for Image Forgery Detection Using CNN-LSTM Deep Learning Model

N. Swapna, Mohammed Noman Quadeer, Mohammed Mujtaba Hussain,  
Mirza Osama Baig

Department of Computer Science and Engineering, Vijay Rural Engineering College, Rochis Valley,  
Manikbhandar, Telangana, India

swapnanaralas@gmail.com, csebatch15nom@gmail.com

## ABSTRACT

In recent years, the popularity of capturing images has increased. The rapid advancement of technology has made effective image processing tools more accessible and making image forgery easier. Identifying real images from forged images has become an alarming obstacle. To detect image forgeries, numerous traditional techniques have been developed over time. Obtained efficiency and type of forgery and/or the image features. Image forgery detection uses different techniques depending on the detection requirements. This paper presents An Improved Novel Framework for Image Forgery Detection using a deep learning model based on CNN (Convolutional Neural Networks) and LSTM (Long Short-Term Memory). The described model uses CASIA.2.0 (Chinese Academy of Sciences, Institute of Automation), the database of image forgery, which contains a total of 12614 images, 5123 are Tempered Images, and the remaining 7491 are Genuine Images. In the image segmentation process, the K-means clustering model is utilised. Grey Level Co-occurrence Matrix (GLCM) features are then calculated to differentiate between the original and forged images. From the comparative results, the image forgery detection has performed better, achieving 98.5% Accuracy, 98% Precision, 97% Recall, and 97% Specificity, using the described CNN-LSTM Deep Learning Model, compared to other algorithms.

**Keywords:** *Image Forgery Detection, CNN (Convolutional Neural Networks), LSTM (Long Short-Term Memory), K-means clustering, Deep Learning.*

## I. Introduction

Digital content is the most popular form of communication because of its portability, ease of use, and information-rich nature [1]. A crucial piece of evidence of digital media technology has developed into such insurance claims, defence, Press, politics, and a few other important areas of legal cases [2].

The image has played an essential role in conveying information about effective carriers in technology. By using smartphones, a large number of advanced imaging devices, people take high-resolution digital images that are exchanged regularly through smartphones [3]. The images can be affected in ways that are not easily observable by performing different types of manipulations. Digital images have become increasingly important in various applications, where authenticity is essential. Verifying the authenticity and integrity of these images is essential [4]. As the creation of digitally forged images has increased, their use has become more frequent throughout society. Without offering any hint as to the update [5], the manipulations of the image's properties may add, delete, or alter them.

Digital image forgery involves altering a source image by adding noise or performing geometric transformations like rotation, resizing, or scaling without the owner's knowledge or consent.[6] There are two types of image forgeries: are two: copy-move and image splicing. Image Splicing: This technique involves a source image in which a portion of a donor image is copied to create the final forged image [7]. To build the final forged image, which uses a sequence of donor images [8]. Copy-Move: This forgery involves a single image where a portion is copied and pasted within the same image, altering the original content through digital manipulation. The frequent use of this is to conceal the other objects. There are no components from other images in the final forged image [9].

By employing several mechanisms, different images can be manipulated. Changes to the present object-level and Parts of the image can be handled effectively using splicing and copy-move techniques [10]. In general, by using image retouching techniques with different tools, images can be altered. However, according to the image content, the holes are filled using image inpainting; for instance, the image contrast can be enhanced. When a specific part of the image must be traced, colourisation might be a misjudgment; normally, colourisation changes based on likely colours in the image [11]. For all possible locations in the images that are impracticable to examine, Cloned zones are used; hence, they can be in any shape and at any location. Sometimes, a cloned zone is essential to rotate, build an impressive image, or stretch or resize sections of the image. For instance, when an image of an object is added to another image to match the other image's comparable height and width, the object will need to be resized.

In both cases, the primary purpose of image forgery is to spread misinformation by altering the original content [12]. Due to image forgery, misinformation spreads; for information exchange, an extremely credible source is the earlier images. The public trust in images will be affected [13]. The naked eye may or may not be visible or recognisable through the forging of images. Detection of image forgeries is essential to prevent the spreading of misinformation and restore public trust in visual content. Detecting image forgeries involves using various image processing techniques to examine the artefacts left behind during the forgery process.

Image forgery detection techniques focus on various artifacts within a forged image, like contrast, sensor noise, compression, illumination changes, and shadows. Convolutional Neural Networks (CNNs) have gained popularity for tasks like image object recognition, classification, and semantic segmentation. This paper introduces a hybrid CNN-LSTN classification model to detect image forgery from a dataset.

The structure of this paper is as follows: Section II presents the existing literature, while Section III explains the proposed Image forgery detection model. Section IV presents the resulting experiment, and Section V provides the paper's conclusion.

## **II. Literature Survey**

The copy-move forgery problem can be solved accurately; the method in [14] generates a novel ground-truth (GT) image. Using image classification and semantic segmentation techniques, the

novel GT image is generated. Creating a variety of ground truth (GT) images involves utilising state-of-the-art image classification techniques and deep neural network semantic segmentation. In the experiment, the result is confirmed by the existing GT net image, which serves as the basis for the performance comparison. In the F1 Score, the demonstrated maximum improvement was 0.4% and 0.2% for the GT decomp image of the proposed scheme. The proposed scheme demonstrated improvements, as evidenced by the GT decomp image.

In [15], depending on Polar Complex Exponential Transform (PCET) and Speeded-up Robust Feature (SURF), copy-move forgery detection (CMFD) is presented in this method. Initially, the image is divided into non-overlapping, irregular image blocks using superpixel segmentation. The second step is the extraction of PCET coefficients and key points, which are identified using SURF. A feature-matching algorithm is utilised to search for similar features. The experimental results, including attacks such as noise addition, blurring, JPEG compression, scaling, and rotation, indicate that the proposed method can withstand various types of distortion.

In [16], this paper proposes a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching. The integration approach of this method is block-based as well as key-point-based forgery detection. The extraction algorithm for the forgery region uses a replacement for traditional feature points: small superpixels, which are blocks of features. This method combines regions with similar local colour features into feature blocks, effectively merging neighbouring blocks.

Significantly outperforms the state-of-the-art method, demonstrating the proposed copy-move forgery detection method. In [17], the primary focus is on extracting, comparing, and evaluating a proposed scheme for detecting copy-move forgery in images.

The proposed scheme distinguishes itself from traditional methods by first segmenting the test image into semantically independent patches before keypoint extraction. The demonstration of the experimental results shows that the proposed scheme outperforms state-of-the-art methods on public databases. The proposed technique leverages deep learning to assess the compression quality of forged areas by leveraging transfer learning to simultaneously detect two types of image forgeries. This approach enhances the detection of digital image forgery [18]. Using the pretrained MobileNetV2 Model, the technique achieves a high detection accuracy rate of around 95% with fewer training parameters. This efficiency leads to faster training times. In [19], the proposed Signal Noise Separation (SNIS) network tackles the challenge of detecting post-processed image forgery. It leverages a parallel atrous convolutional architecture within a multi-scale feature-learning module to learn high-level global features from multiple perspectives. The prediction module classifies the type of tampering operation and predicts the tampered region. Extensive experiments demonstrate that SNIS is effective for forgery detection, robust against multi-post-processing attacks, and capable of detecting forged images without post-processing.

The [20] utilisation of full-resolution information is proposed by introducing a CNN-based image forgery detection framework, where the entire image is used to make decisions. Due to limited resources of memory and supervision of weak image-level, the framework is designed to

be trainable end-to-end. Thanks to gradient checking. Experiments on Image forensics datasets show that the proposed approach significantly outperforms all baselines and methods of reference, demonstrating its strong performance. The superior performance of the approach is extensively demonstrated in experiments. In [21], a novel robust training scheme is proposed. In the beginning, the baseline detector we

Designed and achieved the top rank in a recent certificate forgery detection competition. Next, by online social networks (OSNs), we are conducting a thorough analysis of the noise introduction and dividing it into two parts. Extensive experimental results, particularly in detecting OSN-transmitted forgeries, validate the superiority of the proposed scheme compared to various state-of-the-art competitors.

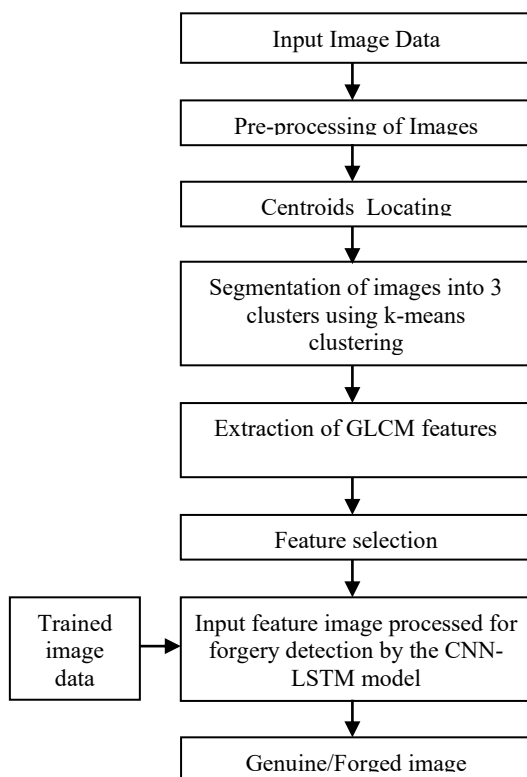
In [22], this approach, using the sensor pattern noise of the proposal, is a new approach for detecting image forgeries. It employs a suitable Markov random field prior to model the strong spatial dependencies of the source. Bayesian estimation, which is termed the Casting problem, and for each pixel, the decision making will be made jointly on the whole image. Large-scale experiments demonstrate that the proposed technique is successfully applicable to a wide range of practical situations. and the art of the present state is improved by a large proposed technique based on real forgeries and simulated shows. In [23], a new methodology is proposed that focuses on detecting localized LCA inconsistencies to identify forged image regions. The proposed statistical model detects image regions by capturing inconsistencies between global and local estimates of lateral chromatic aberration (LCA). It treats forgery detection as a hypothesis-testing problem and derives optimal detection statistics under certain conditions. The experiment shows that the estimation algorithm is proposing significantly, resulting in a reduction of estimated time without introducing additional errors. In [24], an end-to-end neural network based on residual refinement network (AR-Net) and adaptive attention is proposed. In particular, the adaptive attention mechanism fully captures context information and enriches feature representation by fusing position and channel attention features. Extensively experimenting with demonstration, which is the AR-Net, outperforming state-of-the-art algorithms, accurately locating pixel-level tampered and genuine regions. Additionally, on postprocessing operations the AR-Net have been high robustness, such as recompression, blur, JPEG, and noise.

In [25], an automatic computer-based system is required to be developed that can identify the originality of the input image. Image processing involves three main phases: pre-processing, feature extraction and foreground area detection using the extracted features. An inclusive survey of various image forgeries, their types and a comparison of various detection techniques are presented. Each method is also highlighted with its advantages and drawbacks. In [26], this is achieved by using the image's luminance channel and colour characteristics, which identifies the patterns for accurate forgery detection, combining deep features with handcrafted ones. The pre-trained ResNet-18 model known as ' ResFeats', creates a 512-D feature vector by processing Local binary feature maps through a convolution-based portion, especially from the last

layer. This fusion-based approach achieves an impressive 99.3% accuracy on benchmark datasets.

### III. Improved Novel Framework for Image Forgery Detection

The workflow of An Improved Novel Framework for Image Forgery Detection using a CNN-LSTM Deep Learning Model is illustrated in Figure 1. This paper used to contain a total of 12,614 images, Genuine Images are 7,491, and 5123 are the remaining Tempered Images, which are named as CASIA.2.0 image forgery database. 80% of the images are included in the training data, totalling 10091. The testing data comprises 20% of the images, and finally, the total is 2523.



**Figure 1:** Workflow of the Improved Novel Framework for Image Forgery Detection

Pre-processing an image involves multiple steps. First, noise is removed to clean the image data. Next, and the RGB image is converted to grayscale using standard color conversion. During this grayscale conversion and edge detection, the Canny method is often used. This ensures that image features are preserved while extracting details. Finally, additional de-noising sharpens the image.

When compared with other methods, centroids play a significant role in image analysis. They assist in identifying the most similar clusters, allowing for effective calculation of the Euclidean distance between them. Whereas, in order to calculate the Euclidean distance, the connection between centroids is utilised.

Within a database of images, each image has highly unique features that can be matched perfectly with similar feature. The Usage of k-means cluster where the image is segmenting into three distinct clusters. For quantizing vectors is a technique of K-means clustering. This method divides the image into k segments, each containing mutually exclusive data. One of the segmented images is selected based on its information. Each segment's features are calculated using the highest mean of the segment, and the Grey Level Co-occurrence Matrix (GLCM) is chosen. Using cross-validation, the comparison of the GLCM of the segmented image with the original image. Another array is generated by this comparison, which is then analysed to determine if the image has been morphed.

Among various image analysis methods, extracting GLCM features has consistently proven efficient. GLCM provides statistical measures for texture analysis in tabular form. This method considers the special relationships between pixel intensities in a grey level. In this paper, to analyse the differences between the digitally forged image and the original one, GLCM features are used.

Neighbourhood component analysis (NCA) is a dimensionality reduction technique that aims to select a subset of features to improve classification performance. In the context of GLCM features, NCA can be used to select the most informative features. The final feature selection result is a subset of the combined features, selected by the NCA optimisation as the most informative. These selected features are retained for further processing, such as classification for image forgery detection.

CNN-LSTM Deep Learning Model is hybrid classification algorithm used to detect forgeries in images. Here if an image is genuine or a forged we use this CNN-LSTM model in the proposed approach to determine. CNN develops a wide variety of images that may be used as input for the precision of the predicting models. Recurrent Neural Networks (RNN) are designed to process and retain information over multiple time steps. The specializing type of RNN is Long Short-Term Memory (LSTM). The tensor weight proportional is generated by LSTM which will the same of convolutions, which will generate convolutions in multiplication. The proposed LSTM has several convolution layers, including building blocks, an input layer, a classification layer, fully connected layers, and an output layer. In a copy-move forgery detection model LSTM is used in which advantageous of CNN is due to the effectiveness of CNN as a feature extracting strategy. This boosts the models of overall performance. Additionally, the CNN in turn can be achieving by exposed of it where the capacity of the CNN which is to learn a larger set of sample inputs which is may be enhanced. The training process can be repeated more often which provides better output results.

In the next step, performance of describes using of Detection of Image Forgery CNN-LSTM Deep Learning Model is analyzed by using the performance parameters as Accuracy, Precision, Recall and Specificity. If these parameters achieved greater percentage values then it declares that higher efficiency in detecting forged images.

#### **IV. Result Analysis**

In this section the description of the testing environment and training for the proposed approach and also explains the performance of described Improved Novel Framework for Image Forgery Detection using CNN-LSTM Deep Learning Model. In this paper CASIA.2.0 image forgery database is used where it contains a total images are 12,614 and 5123 are Tempered Images and remaining 7,491 are Genuine Images. Of this data for training 80% is used while for testing 20% reserved. Accuracy, Precision, Recall and Specificity are the performance parameters used for evaluation. For calculation of these parameters some predetermines are required and these are, True Negative (TN), True Positive (TP), False Positive (FP) and False Negative (FN).

Accuracy: Proportion of correctly classified instances, whether positive or negative. It is mathematically defined in below equation 1,

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (1)$$

Precision: Also known as the representing of the fraction of true positives among those classification as positives, positive predictive value. Precision has been expressed in (2).

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (2)$$

Recall measuring of how often a machine learning model correctly identifying true positive from all the actual positive samples in the dataset. It is expressed as shown in equation 3 below,

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (3)$$

Specificity: The true negatives rate, or Specificity is the proportion of negatives that are correct classification. This metric evaluates the model's ability to accurately identify actual negative cases has been expressed in (4).

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}} \quad (4)$$

TP (True Positive) Indicates instances of genuine image correctly classified as genuine image. TN (True Negative) classified as Indicates instances of forged image correctly classified as forged image. FP (False Positive) Indicates instances of genuine image incorrectly classified as forged image. FN (False Negative) Indicates instances of forged image incorrectly classified as genuine image.

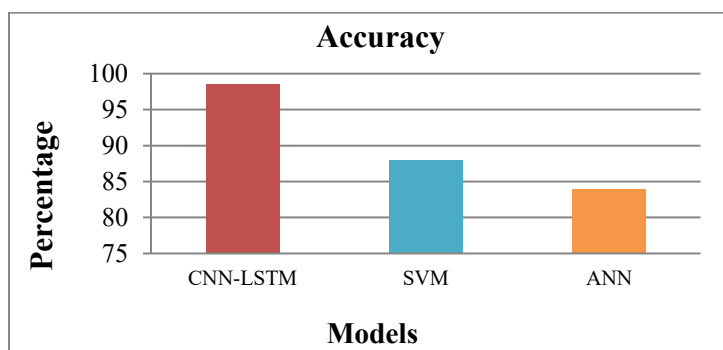
Described Improved Novel Framework for Image Forgery Detection using CNN-LSTM Deep Learning Model performance is comparing with Artificial Neural Network (ANN) and Image Forgery Detection using SVM (Support Vector Machine). This comparative analysis is represented in below Table 1 in terms of performance parameters.

**Table 1:** Comparative performance analysis

| Parameters | Image Forgery Detection model |
|------------|-------------------------------|
|------------|-------------------------------|

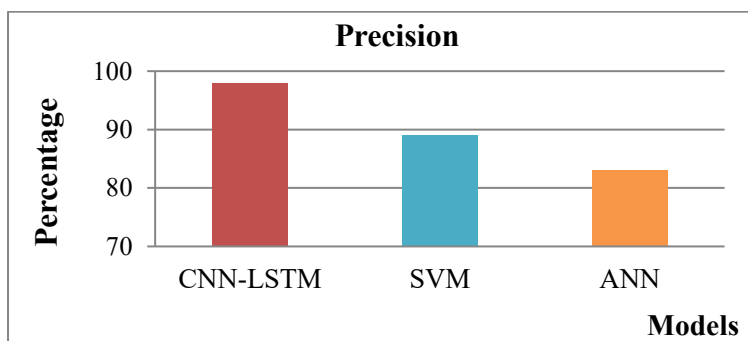
|             | <b>CNN-LSTM</b> | <b>SVM</b> | <b>ANN</b> |
|-------------|-----------------|------------|------------|
| Accuracy    | 98.5            | 88         | 84         |
| Precision   | 98              | 89         | 83         |
| Recall      | 97              | 87         | 84.5       |
| Specificity | 97              | 88         | 82         |

The graphical representation of Accuracy parameter for Image Forgery Detection using described CNN-LSTM model, SVM model and ANN model is represented in below Figure 2, in which the representation of X-axis is models and Y-axis denoting the percentage value. From result it is observed that, Accuracy of described CNN-LSTM model based Image Forgery Detection is high compared to other models.



**Figure 2:** Comparative accuracy analysis

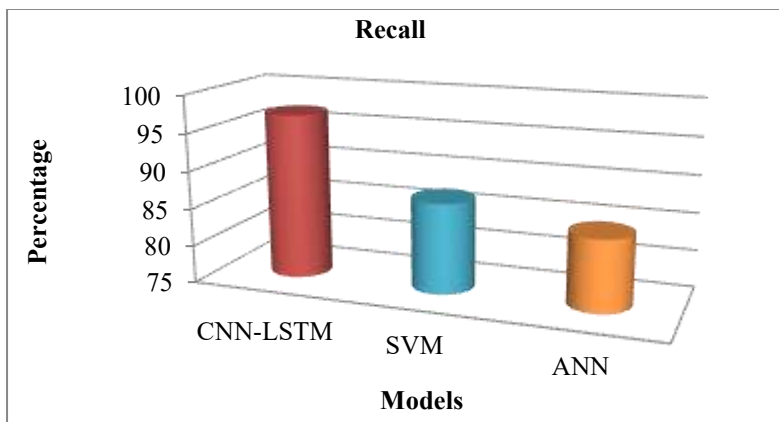
Comparative graphical analysis of Precision parameter is represented in below Figure 3 for Image Forgery Detection using described CNN-LSTM model, SVM model and ANN model. It states that, highest Precision value is achieved for described CNN-LSTM model. X-axis representation is models and Y-axis denotes percentage value.



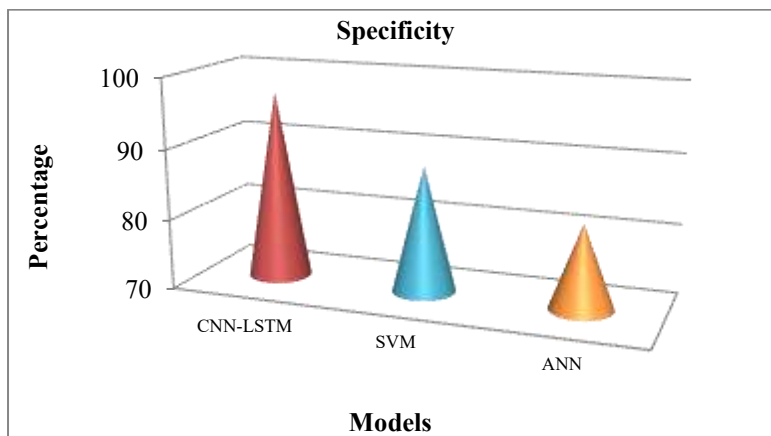
**Figure 3:** Comparative Precision analysis

Figure 4 presents the Recall parameter comparative analysis for three models based Image Forgery Detection, in which Y-axis denotes percentage and X-axis denotes models. CNN-LSTM model based Image Forgery Detection gains high percentage of Recall value. Specificity parameter comparative analysis is described in below Figure 5 for Image Forgery Detection

using described CNN-LSTM model, SVM model and ANN model. Specificity of described model is high compared to other models. Y-axis representation of the percentage value and X-axis representation is models.



**Figure 4:** Comparative Precision analysis



**Figure 5:** Comparative Specificity analysis

Therefore overall results states that, described Improved Novel Framework for using CNN-LSTM Deep Learning Model of Image Forgery Detection is more efficient in terms of all performance parameters. Obtained values for described model are Accuracy as 98.5%, Precision as 98%, Recall as 97% and Specificity as 97%.

## V. Conclusion

In this paper, An Improved Novel Framework for Image Forgery Detection using CNN-LSTM Deep Learning Model is described. The processing of genuine images which is distinguished from counterfeit ones is the evolving of a challenging challenge. The evolution of a challenging challenge is the genuine images process which is distinguishes from forged ones. CASIA.2.0 database of image forgery has using this paper where for image forgery detection process totally it contains images of 12,614. From this data, for training 80% is used, while for testing 20% is reserved. K-means clustering model is using in image segmentation process. In this paper, the

features of GLCM is calculating to study the difference of the digitally forged image and original image. Neighborhood component analysis (NCA) is a dimensionality reduction technique that aims to select a subset of features. CNN-LSTM Deep Learning Model is hybrid classification algorithm used to detect forgeries in images. Accuracy, Precision, Recall and Specificity are used performance parameters for evaluating the performance. Obtained values for described model are Accuracy as 98.5%, Precision as 98%, Recall as 97% and Specificity as 97%. Therefore overall results states that, described Improved Novel Framework for Image Forgery Detection using CNN-LSTM Deep Learning Model is more efficient in terms of all performance parameters.

## VI. References

- [1] S. Karnouskos, "Artificial Intelligence in Digital Media: The Era of Deepfakes," in *IEEE Transactions on Technology and Society*, vol. 1, no. 3, pp. 138-147, Sept. 2020, doi: 10.1109/TTS.2020.3001312.
- [2] H. Wang and W. Wu, "The Effects of Digital Technology Strategy Configurations on New Venture Performance," in *IEEE Transactions on Engineering Management*, vol. 71, pp. 5470-5486, 2024, doi: 10.1109/TEM.2024.3363625.
- [3] N. Le and F. Retraint, "An Improved Algorithm for Digital Image Authentication and Forgery Localization Using Demosaicing Artifacts," in *IEEE Access*, vol. 7, pp. 125038-125053, 2019, doi: 10.1109/ACCESS.2019.2938467.
- [4] E. A. Armas Vega, E. González Fernández, A. L. Sandoval Orozco and L. J. García Villalba, "Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression," in *IEEE Access*, vol. 8, pp. 11815-11823, 2020, doi: 10.1109/ACCESS.2020.2964516.
- [5] K. M. Hosny, A. M. Mortda, M. M. Fouda and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forgery," in *IEEE Access*, vol. 10, pp. 48622-48632, 2022, doi: 10.1109/ACCESS.2022.3172273
- [6] C. Chen, J. Ni, Z. Shen and Y. Q. Shi, "Blind Forensics of Successive Geometric Transformations in Digital Images Using Spectral Method: Theory and Applications," in *IEEE Transactions on Image Processing*, vol. 26, no. 6, pp. 2811-2824, June 2017, doi: 10.1109/TIP.2017.2682963.
- [7] Y. Rao, J. Ni and H. Zhao, "Deep Learning Local Descriptor for Image Splicing Detection and Localization," in *IEEE Access*, vol. 8, pp. 25611-25625, 2020, doi: 10.1109/ACCESS.2020.2970735.
- [8] Y. Zhang, G. Zhu, L. Wu, S. Kwong, H. Zhang and Y. Zhou, "Multi-Task SE-Network for Image Splicing Localization," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 7, pp. 4828-4840, July 2022, doi: 10.1109/TCSVT.2021.3123829
- [9] Y. Li and J. Zhou, "Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1307-1322, May 2019, doi: 10.1109/TIFS.2018.2876837.

- [10] J. -L. Zhong and C. -M. Pun, "An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2134-2146, 2020, doi: 10.1109/TIFS.2019.2957693.
- [11] I. Žeger, S. Grgic, J. Vuković and G. Šišul, "Grayscale Image Colorization Methods: Overview and Evaluation," in *IEEE Access*, vol. 9, pp. 113326-113346, 2021, doi: 10.1109/ACCESS.2021.3104515.
- [12] P. Kakar, N. Sudha and W. Ser, "Exposing Digital Image Forgeries by Detecting Discrepancies in Motion Blur," in *IEEE Transactions on Multimedia*, vol. 13, no. 3, pp. 443-452, June 2011, doi: 10.1109/TMM.2011.2121056.
- [13] Y. Guo, X. Cao, W. Zhang and R. Wang, "Fake Colorized Image Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 1932-1944, Aug. 2018, doi: 10.1109/TIFS.2018.2806926.
- [14] K. H. Rhee, "Generation of Novelty Ground Truth Image Using Image Classification and Semantic Segmentation for Copy-Move Forgery Detection," in *IEEE Access*, vol. 10, pp. 2783-2796, 2022, doi: 10.1109/ACCESS.2021.3136781.
- [15] C. Wang, Z. Zhang, Q. Li and X. Zhou, "An Image Copy-Move Forgery Detection Method Based on SURF and PCET," in *IEEE Access*, vol. 7, pp. 170032-170047, 2019, doi: 10.1109/ACCESS.2019.2955308.
- [16] C. -M. Pun, X. -C. Yuan and X. -L. Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1705-1716, Aug. 2015, doi: 10.1109/TIFS.2015.2423261.
- [17] J. Li, X. Li, B. Yang and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, March 2015, doi: 10.1109/TIFS.2014.2381872
- [18] A. H. Khalil, A. Z. Ghalwash, H. A. -G. Elsayed, G. I. Salama and H. A. Ghalwash, "Enhancing Digital Image Forgery Detection Using Transfer Learning," in *IEEE Access*, vol. 11, pp. 91583-91594, 2023, doi: 10.1109/ACCESS.2023.3307357.
- [19] Shanmuganathan, V., Yesudhas, H. R., Khan, M. S., Khari, M., & Gandomi, A. H. (2020). R-CNN and wavelet feature extraction for hand gesture recognition with EMG signals. *Neural Computing and Applications*, 32(21), 16723-16736.
- [20] F. Marra, D. Gragnaniello, L. Verdoliva and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," in *IEEE Access*, vol. 8, pp. 133488-133502, 2020, doi: 10.1109/ACCESS.2020.3009877.
- [21] H. Wu, J. Zhou, J. Tian, J. Liu and Y. Qiao, "Robust Image Forgery Detection Against Transmission Over Online Social Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 443-456, 2022, doi: 10.1109/TIFS.2022.3144878
- [22] G. Chierchia, G. Poggi, C. Sansone and L. Verdoliva, "A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 554-567, April 2014, doi: 10.1109/TIFS.2014.2302078

- [23] O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1762-1777, July 2018, doi: 10.1109/TIFS.2018.2799421
- [24] Y. Zhu, C. Chen, G. Yan, Y. Guo and Y. Dong, "AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6714-6723, Oct. 2020, doi: 10.1109/TII.2020.2982705.
- [25] K. H. Hingrajiya and R. K. Sheth, "Comparative Study of Digital Image Forgery Detection Techniques," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp. 83-86, doi: 10.1109/ICACITE51222.2021.9404748.
- [26] S. Walia, K. Kumar, M. Kumar and X. -Z. Gao, "Fusion of Handcrafted and Deep Features for Forgery Detection in Digital Images," in *IEEE Access*, vol. 9, pp. 99742-99755, 2021, doi: 10.1109/ACCESS.2021.3096240.