

A Hybrid CNN-LBPNET Approach for Improving Duplicate Image Detection

Prathi Naveena*, Sandeep Kumar Dash

National Institute of Technology Mizoram,
India

{dt21cs002, sandeep.cse}@nitmz.ac.in

Abstract. The explosive growth and popularity of social media networks like Instagram, Facebook, etc., have intensely influenced the surge in visual data in recent years. Digital image-altering tools have made manipulation of images easier but their identification more difficult; this has created serious problems in multimedia forensics and content verification, as they anticipate the potential misuse of these images to provoke crowds and disseminate false information. The copy-move forgery method is often used to change or hide visual information by copying and moving parts of images within the same image. The lighting, color distribution, noise, and imaging circumstances of the original and duplicated portions are quite similar, making it difficult to detect this type of alteration, and it is essential to verify the authenticity of an image before adding it to these sites. This study proposes a hybrid CNN-LBPNET model that combines Local Binary Pattern (LBP) texture representation with neural feature learning to identify image-level copy-move forgeries. It makes use of RGB images to maintain structural and spatial information, and it transforms grayscale images into LBP texture maps to emphasize local intensity shifts and micro-texture variations. This integration creates a consistent input for the network, enabling it to effectively learn forensic cues based on texture and complementing spatial information. The proposed system accurately recognized copy-move forgeries at the image level when applied to the MICC-F220 dataset. The CNN-LBPNET addresses and improves upon the constraints of utilizing merely CNNs or manually created features for detecting forged images by combining acquired spatial characteristics with explicit texture descriptors. By enhancing digital evidence verification, social media image authenticity, document integrity evaluation, and multimedia forensic investigations, the model's robust detection abilities reduce the emergence of forged images as original.

Keywords. CNN-LBPNET, copy-move forgery detection, local binary pattern, MICC-F220, image-level classification, digital image forensics.

1 Introduction

With the increasing use of digital media, image forgery has become a significant concern. Image forgery refers to altering or manipulating an image in a way that changes its meaning or context. The digital realm is teeming with a wide range of visuals, enriching online encounters while presenting obstacles to content moderation systems, search engines, and copyright enforcement.

Traditional image duplicate identification approaches like hash-based algorithms often fail because of errors caused by distortions, transformations, and lighting. As a result, it becomes challenging to differentiate between authentic and forged images, which can lead to severe consequences in various fields, including law enforcement, journalism, and forensics.

Convolutional Neural Networks (CNNs) are among the most promising methods that have been suggested for detecting image forgeries. Due to their ability to recognize intricate features and patterns in pictures, CNNs have proven very effective at spotting fake images. A new approach for detecting image forgery through the use of the CNN is presented in this work.

The proposed method involves training a neural network [4] to analyze different image features like color, texture, and edges to detect manipulation.

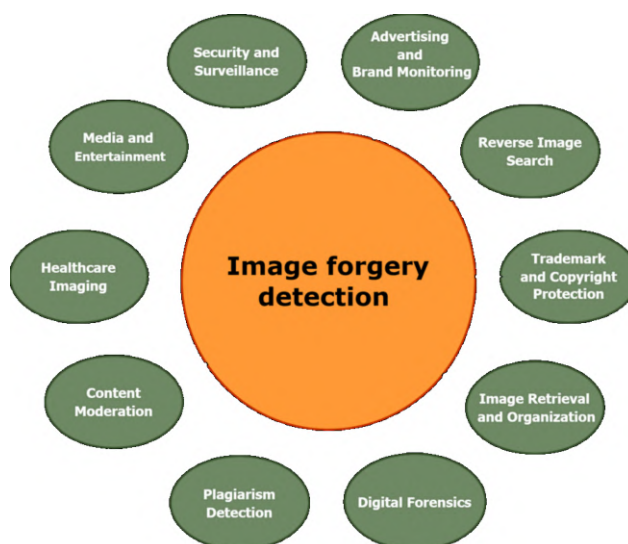


Fig. 1. Applications of image forgery detection

The neural network is trained using a large dataset [11] of authentic and forged images, enabling it to identify manipulated images accurately. The proposed method has several advantages over existing approaches. It is highly accurate and can detect various types of image forgery, including copy-move, splicing, and retouching [2]. It is efficient and can process images in real-time, making it suitable for forensic analysis and online image verification applications. It is based on Local Binary Pattern (LBP), a robust feature descriptor that captures local image information effectively. The method is effective computationally, making it appropriate for real-time use.

This work proposes a new method that uses Convolutional Neural Networks to identify image manipulation. The importance of CNN in improving picture forgery detection is highlighted, and future research areas are proposed in this work. This work advances image forgery detection by providing a cutting-edge approach.

An improved model for image duplicate identification is suggested in this study by combining the advantages of Convolutional Neural Networks with local binary pattern recognition. A practical method for detecting duplicate photos is proposed as a hybrid approach that integrates LBP descriptors with CNN. This approach can detect both local and

large patterns. This all-encompassing method is suggested to address the challenging problem of image forgery.

Deep learning has dramatically enhanced computer vision applications, particularly with the advent of Convolutional Neural Networks, which are incredibly effective for tasks involving images. However, Local Binary Patterns (LBPs) are great at catching picture details and texture, whereas Convolutional Neural Networks could miss more nuanced local patterns. More integration of these techniques still needs to be done.

Evaluation metrics are crucial to gauge how well picture forgery detection models are performing [30]. Precision, recall, F1-score, ROC curve, and area under the curve (AUC) are frequently used measures [1]. The precision ratio is the sum of all-natural and predicted positives. Recall is the proportion of actual positives to all real positives. The harmonic mean of recall and accuracy is known as the F1-score. A ROC curve is a graph of the actual positive rate versus the false positive rate at various classification levels. The area under the ROC curve is known as AUC.

Each metric has its advantages and disadvantages. Precision and recall are helpful when the number of false positives and false negatives is essential.

The F1-score is useful when a trade-off between accuracy and recall is required. The ROC curve and AUC are helpful when the classifier is required to perform well across all thresholds. The most suitable metric for different types of image forgery detection tasks depends on the specific requirements of the task. For example, precision and recall may be more critical in forensic applications [30], while the ROC curve and AUC may be more suitable for general image-tampering detection tasks.

In recent years, there has been significant progress in image forgery detection. Several research studies have been carried out to improve detection accuracy and develop more robust models. Utilizing deep learning algorithms [27, 7] such as Convolutional Neural Networks and Recurrent Neural Networks (RNNs), is one of the newest developments in this area [17]. These algorithms have shown promising results in detecting various image forgeries, including copy-move [3], splicing [2], and removal. Additionally, transfer learning and adversarial training have been explored to improve the model's generalization and robustness to adversarial attacks. Another area of research in image forgery detection is the development of multi-modal and multi-task models.

These models combine information from multiple sources, such as visual, spatial, and temporal features, to enhance detection performance. Furthermore, integrating other data modalities, such as audio and metadata, has also been explored to develop more comprehensive detection frameworks. Future research in image forgery detection will likely focus on creating more efficient and reliable models that can handle large-scale datasets and complex image manipulations. Developing explainable and interpretable models that can provide insights into the detection process is also an area of growing interest.

Figure 1 displays the wide range of applications for image forgery detection. In forensic investigation, image forgery detection [26, 13, 12, 16] can help investigators determine the authenticity of a photograph or video and identify any alterations made to the original image. It can be beneficial in criminal investigations where evidence integrity is crucial. Content authentication and image forgery

detection can verify the authenticity of images used in marketing, advertising, and journalism. It can help prevent the spread of fake news and misinformation and protect the reputation of companies and individuals. In social media analysis, image forgery detection is used to identify manipulated images, such as deep fakes, and prevent the spread of harmful content [25, 19, 6, 36]. However, implementing image forgery detection can be challenging. One of the biggest challenges is the sheer volume of daily images and videos being shared online. Another challenge is the constantly evolving techniques forgers use to create convincing fakes. Additionally, image forgery detection algorithms can sometimes produce false positives or negatives, leading to incorrect conclusions. Despite these challenges, the potential benefits of image forgery detection make it a valuable tool in various applications.

2 Literature Review

This bibliometric analysis concludes by illuminating the current state of research concerning detecting forged images. The results underscore the increasing significance of devising efficacious methodologies to counteract image forgery in the era of digitalization. Research in the field of visual forensics can benefit greatly from this study because it identifies important issues, prominent authors, and prominent publications in the field. By reviewing numerous academic databases, it becomes clear that image forgery detection has witnessed substantial study and advancements. The present article includes a complete analysis of recent trends by focusing on 2010-2024 documents in the Scopus database. Vosviewer is an application that facilitates the visualization and analysis of co-authorship networks among members of a scientific community [34].

Its interactive interface allows users to discern prominent researchers, clusters of collaboration, and emergent trends. Out of 5162 Scopus keywords analyzed using Vosviewer, 427 satisfied the predetermined requirements for bibliometric keywords. Overlay and density visualization of keywords are shown in Figures 2 and 3 using the Vosviewer tool.

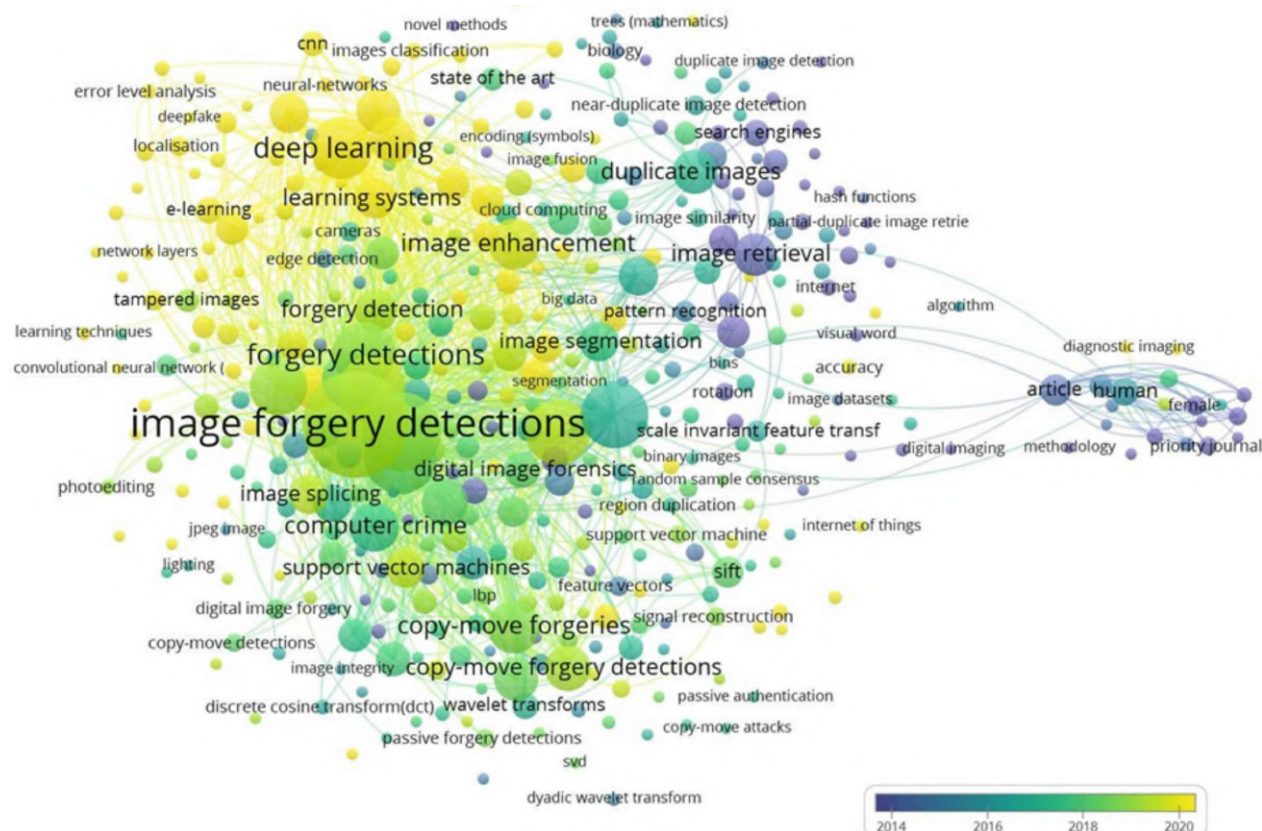


Fig. 2. Overlay Visualization of Keywords

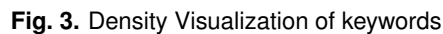
Most keywords were "image forgery detection" and "duplicate images" related to Adobe Photoshop and photo editing programs. This section examines recent research that has utilized CNN techniques for distinguishing between authentic and manipulated images. In 2016, C.N. Bharti et al. [5] found that forged image detection has become essential due to image alteration technologies. There are two types of forgery detection methods: copy move and splicing. These methods may assist in detecting potential attacks that include blurring and noise. This overview introduces techniques, the basic flow, and comparative studies that include parameters, merits, and demerits.

In 2020, Ankita Bansal et al. [7] addressed the difficulties and methods of picture copy-move forgery detection in 2020. The proliferation of simple image-altering software has made it

nearly impossible to tell if an image has been altered. Duplicating and pasting a part of an image is a common alteration technique. The paper offers an in-depth examination and evaluation of different detection techniques for copy-move forgery, emphasizing the strengths and weaknesses of each approach.

This initiative attempts to improve image-tamper identification. Sophisticated photo editing techniques include merging numerous photographs, while essential tools enable users to change hue, saturation, and composition and add effects like age compositing and image cloning [18].

In 2019, P. B. Shailaja Rani et al. [28] discussed image fraud methods to create realistic-looking computer images. According to the study, false images are more challenging to identify than real ones.



In 2019, H. Guan et al. [14] Using a large dataset consisting of more than 176,000 high-provenance photos, 11,000 videos, 100,000 altered photographs, 4,000 altered videos, 35 million online images, and 300,000 video snippets, this article offers a standard for digital Media Forensics Challenge assessments. The study includes descriptions of the architecture and infrastructure, as well as previous evaluation outcomes, and discussions of the goals, difficulties, and methods for creating evaluation datasets. This study stresses the significance of utilizing

This work introduces an innovative approach for detecting image duplicates using a Hybrid CNN-LBPNET architecture. This design integrates CNN with local binary pattern recognition to extract detailed information.

Table 1. Comparative analysis of techniques used for detection of forgery

S.No.	Authors	Year	Technique Used	Main Findings	Remarks
1	M. Sabeena et al.,[29]	2024	CBAM Network	Accurately pinpoint the tampered region and is robust to post-processing operations such as rotation, scaling, and JPEG recompression	Detection of spliced images remains a challenge
2	Tyagi et al.,[32]	2023	MiniNet	To efficiently identify fake photos with low computational cost, a Convolutional Neural Network based approach is employed	CNNs have proven to be effective in identifying tampering in diverse manifestations and also efficient in video segmentation
3	Kumar et al.,[22]	2023	Non-overlapping block level pixel comparison technique	The structure similarity index metric is utilized for the purpose of classifying images as either authentic or compromised	Enhanced detection of rotated patches in fake photos is within the algorithm's capabilities
4	Koul et al.,[20]	2022	CNN based framework with feature extraction and classification	To accurately identify copy-move forgery	Locating manipulated image regions is being accomplished with the help of state-of-the-art deep learning algorithms such as RCNN
5	Sri CG, Bano S et al.,[31]	2021	ELA based CNN	A lossless picture compression error level analysis is used to detect counterfeiting	Estimating images without prior resizing is facilitated by ELA
6	Lu M, Niu S et al.,[24]	2020	An LSTM-CNN based detection method	An LSTM-CNN based detection method for the elimination of objects introduced by exemplar-based image inpainting	Accuracy and prediction have improved in the model
7	Castillo Camacho et al.,[8]	2020	Forensic image processing using CNN	A multi scale approach to efficiently evaluating strongly correlated noise in JPEG-compressed images	Intended to fix the data mismatch between training and testing, the study centres on picture forensics and the detection of realistic and malicious image forgeries
8	RS Zhang et al.,[35]	2020	CNN-Self coding module	Photo realistic computer-generated visuals and photographic photographs are contrasted throughout the text	Detecting recolored picture tampering is difficult
9	He P et al.,[15]	2020	AD-CNN	An attention-based dual-branch Convolutional Neural Network Using convolutional layers that use multi scale kernel sizes, AD-CNN pairs two identical shallow CNN branches	To improve the output features, an attention-based fusion model is used, after which three fully-connected layers are added
10	Diallo, B. et al.,[10]	2020	CNN-based camera model identification for forged image detection	The robustness of image tampering detection for compression	Handling compressed Images for discriminant features extraction is a challenge

The research further analyzes the learned feature representations, draws attention to the model's interpretability, and discovers critical discriminative characteristics. Furthermore, the investigation provides a viable answer with potential real-world

applications in several fields. Recent advances in computer vision have improved image analysis and recognition. Combining Convolutional Neural Networks and Local Binary Patterns in a hybrid model is one promising strategy. This novel

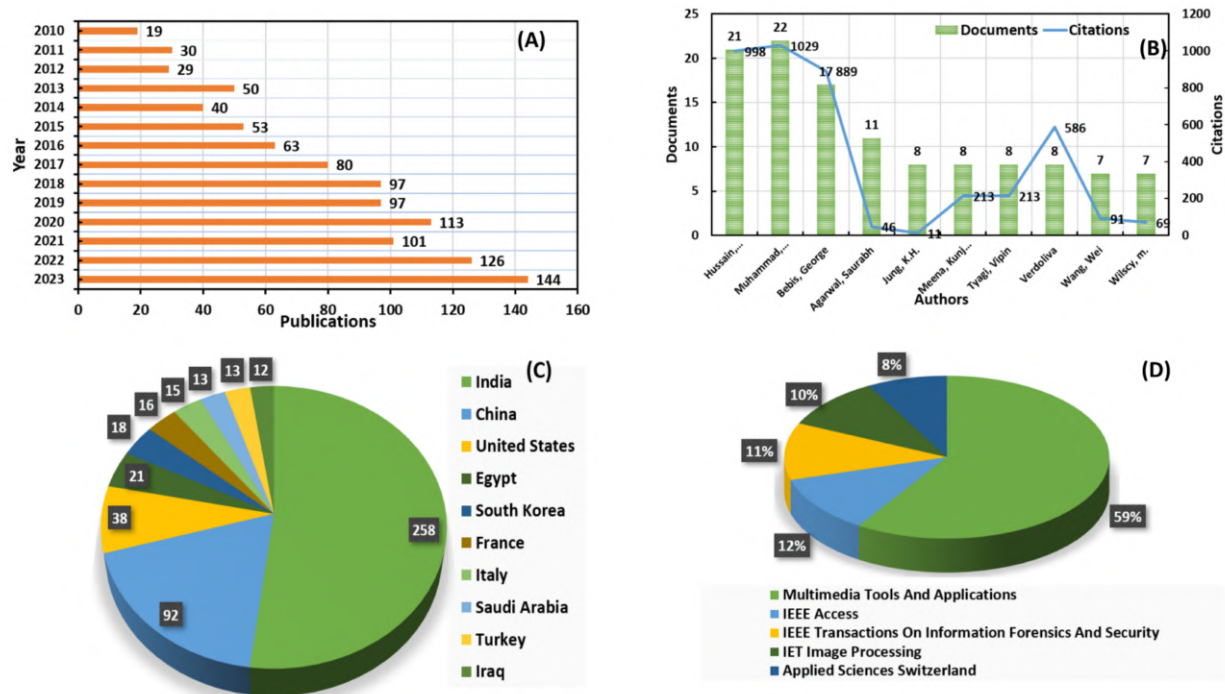


Fig. 4. An Examination of the Dynamic Landscape of Image Forgery Detection via Prominent Scholars, Innovative Journals, Worldwide Outlooks, and Progressive Developments (A). List of active journals over the period of last ten years, (B). Top ten active authors with publications and citation count, (C). Top 10 active countries research on forged images, (D) The top five journals with most published articles in the field of image forgery detection

approach uses CNNs and LBPs to improve image analysis.

The CNN-LBPNET hybrid method is mainly used for image duplicate detection. Digital material is growing exponentially, making content monitoring and copyright enforcement crucial.

The global feature extraction of CNNs and the local pattern analysis of LBPs allow this hybrid model to identify visually comparable images more accurately and reliably. It is essential to manage massive image databases and enforce copyright laws.

The hybrid method also works well in other areas of computer vision. Combining CNNs with LBPs improves feature extraction, resulting in more accurate and dependable facial recognition systems used in biometrics and face recognition. Medical imaging and material science require texture analysis, in which the hybrid model

can capture hierarchical characteristics and local texture patterns.

The model is now highly skilled at identifying complex image textures. The hybrid model harnesses the power of both global and local data, making it ideal for object recognition and classification tasks. Convolutional Neural Networks (CNNs) are great at learning object hierarchies, and LBPs improve the model's pattern recognition capabilities in very localized areas. This robust method can deal with changes in the look of objects well.

Along with its use in medical image analysis, gesture recognition, video analysis, quality assessment in image and video processing, remote sensing, and satellite image analysis, the CNN-LBP hybrid technique has many more potential uses. Utilizing a mix of CNNs and LBPs yields more trustworthy outcomes across these fields.

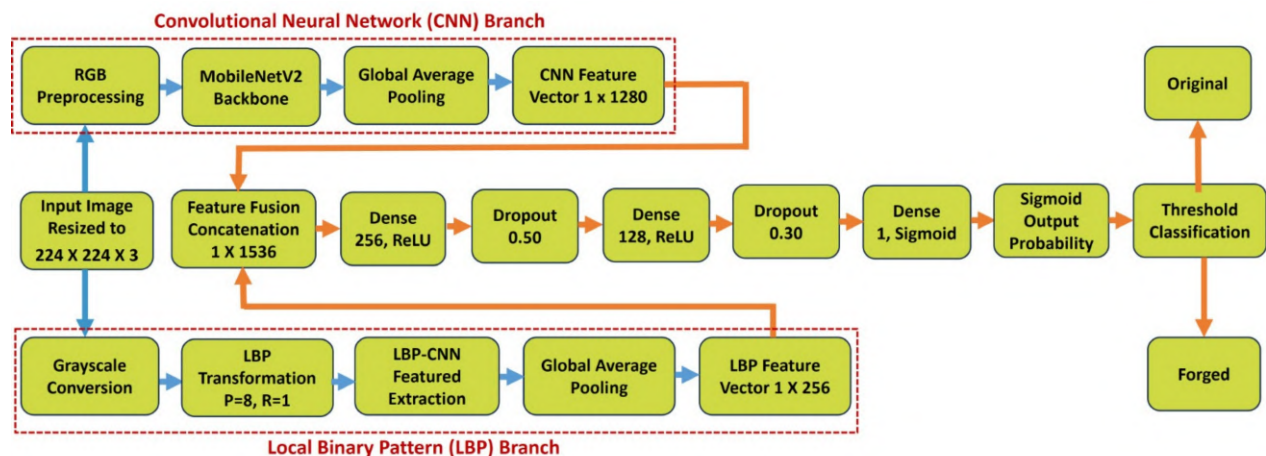


Fig. 5. CNN-LBPNET Process Architecture

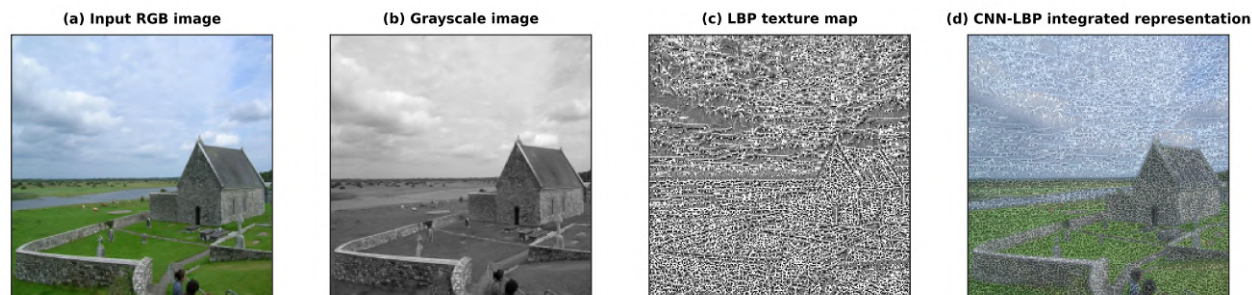
3 Proposed Methodology

To tackle the challenges of copy-move forgery, the proposed approach provides a new CNN-LBPNET framework for image-level forgery detection. Forgeries of this kind can produce structural and textural irregularities that aren't always easy to see, particularly when resized, blended, or compressed areas are placed against comparable backdrops. Conventional approaches, such as Local Binary Pattern (LBP) descriptors, Support Vector Machines (SVMs), and Complement Naive Bayes (CNB), have their limitations when it comes to complex forgery cases. SVM's efficacy is dependent on feature quality and tuning. Complement Naive Bayes simplifies visual feature correlations, and LBP captures local texture but fails to comprehend broader spatial relationships. However, while Convolutional Neural Networks (CNNs) trained independently are excellent at learning hierarchies in space, they could miss important information in the local texture. To improve the identification of subtle modifications in fabricated images, the CNN-LBPNET system attempts to fill these inconsistencies. In order to circumvent these restrictions, the hybrid CNN-LBPNET integrates spatial and texture data into a unified input representation. It keeps the image's visual structure with the help of the RGB component and emphasizes local intensity

variations and micro-textures with the help of the LBP component. The model is able to capture a more detailed representation than CNN or LBP could obtain on their own because of this combination. In the end, the system is able to differentiate between authentic and fake images by acting as a compact classifier at the image level.

To ensure consistency across datasets, the first step in developing CNN-LBPNET is to resize input images to a consistent dimension. By converting the image to grayscale, texture analysis can be performed via Local Binary Pattern (LBP) extraction, while the RGB image is kept for its intricate spatial information, such as color and structure. Even though the visual appearance is unaltered, this method is able to detect minute changes in texture that could be signs of copy-move operation.

The model takes advantage of the spatial information in the RGB channels and the textural insights in the LBP channels by integrating the two sets of representations. By utilizing both visual structure and local texture cues, the CNN is able to train more efficiently. Integrated representations are processed by CNN-LBPNET convolutional layers, which extract important spatial-texture information, and finally by a classification head that decides if an image is original or fake. This novel architecture improves the model's capacity to detect manipulation-related discrepancies by



The RGB image provides spatial information, while the LBP map provides local texture information for CNN-LBP integration.

Fig. 6. CNN-LBPNET Preprocessing and Integration Workflow

combining adaptive spatial representation from CNN learning with explicit texture sensitivity from LBP. Finally, it achieves better results than conventional classifiers and single-feature approaches for image-level classification.

The architecture of the Hybrid CNN-LBPNET model for detecting image forgeries is shown in Figure 5. There are two parts to the model that extract features. One part uses a convolutional neural network (CNN) to process a scaled RGB image with a MobileNetV2 backbone. After global average pooling, the outcome is a spatial feature vector with 1280 dimensions.

After the image is gray scaled and pooled, the LBP branch conducts a local binary pattern transformation ($P=8$, $R=1$), making the texture representation 256 dimensions. Through the use of fully connected layers activated by ReLU and dropout regularization, the model processes a 1536-dimensional representation that is created by merging two feature vectors.

By using a sigmoid output layer, the likelihood of a classification as either original or forged is potentially determined. By combining LBP-based handcrafted texture features with CNN-derived semantic representation, this architecture enables the classifier to learn both structural and local features that are crucial for detecting image forgeries. The MICC-F220 dataset [23], which contains 220 images distributed evenly between original and faked versions, was used to extensively test the proposed CNN-LBPNET model. Both a fixed decision threshold of 0.5 and a validation-optimized threshold were used to

evaluate the model's performance in a 5-fold StratifiedKFold cross-validation setting.

Prioritizing the fixed threshold for evaluation was based on its capacity to consistently and reproducibly make decisions across all test folds, assuring reliable outcomes. The proposed model showed impressive efficacy in this study and its strength in identifying forged images was particularly noticeable.

Figure 6 shows the CNN-LBPNET model preprocessing and feature integration process. The visualization depicts the input preprocessing step of the CNN-LBPNET framework, emphasizing the hybrid strategy of using both RGB and LBP components. While the RGB component records important color and spatial characteristics, the LBP component is tuned toward local texture variations, which are vital for spotting discrepancies that could be caused by image modifications. The CNN-LBPNET's feature extraction and classification layers are then trained on this integrated representation, allowing the system to detect if an image is original or fake.

4 Experimental Setup and Results

Experiments were conducted using the MICC-F220 dataset for image-level forgery detection. The recommended specifications for the experiment system include 8 GB of RAM and an Intel Core 2 Duo processor or later. Software requirements are Python 3.6, TensorFlow 1.15, and NumPy 1.14.0. Examined the outcomes of the experiments concerning different factors to draw

inferences. Using True Positive Rate (TPR) and False Positive Rate (FPR), True Negative Rate (TNR), and False Negative Rate (FNR) measures [21], the detection performance of manipulated images was measured in the research work. Table 2 shows the results of the proposed model:

- True Positive (TP): A true positive (TP) is a hit. This is the percentage of test profiles successfully classified as belonging to the relevant class; it measures the proportion of appropriately identified positives.
- True Negative (TN): This metric indicates the percentage of correctly identified negatives.
- False Positive (FP): A type-I error known as a false positive (FP) is the same as a false alarm.
- False Negative (FN): A type II error, often known as a false negative (FN), is the same as a miss.
- True Negative Rate: TNR, or specificity/selectivity, is a metric that measures the accuracy of correctly identifying actual negatives in a given scenario:

$$TNR = TN / (TN + FP). \quad (1)$$

- True Positive Rate or Hit Rate: The proportion of correctly classified forged photos is compared to the number of forged images:

$$TPR = TP / (TP + FN). \quad (2)$$

- False Positive Rate: Type I error, or incorrect negative identification, refers to the percentage of true negatives incorrectly classified:

$$FPR = FP / (TN + FP). \quad (3)$$

- False Negative Rate: The miss rate is a statistic that measures the proportion of true positives that are false negatives or Type II errors:

$$FNR = FN / (FN + TP). \quad (4)$$

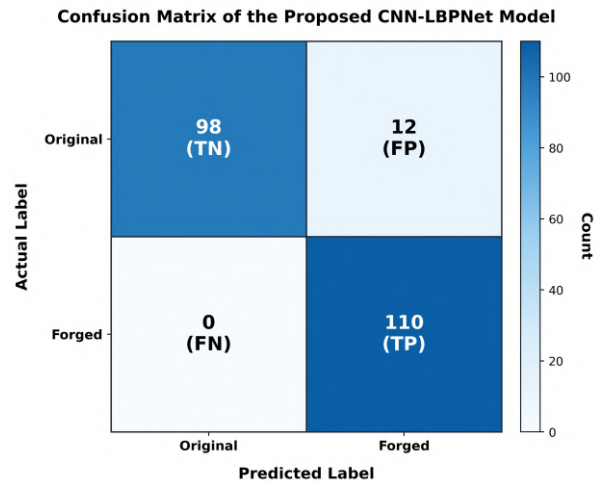


Fig. 7. Confusion Matrix of the proposed model

- Accuracy: Prediction accuracy is defined as the proportion of correct predictions (positive and negative) relative to the total number of forecasts. Detection accuracy is an essential measure for assessing the effectiveness of a proposed method:

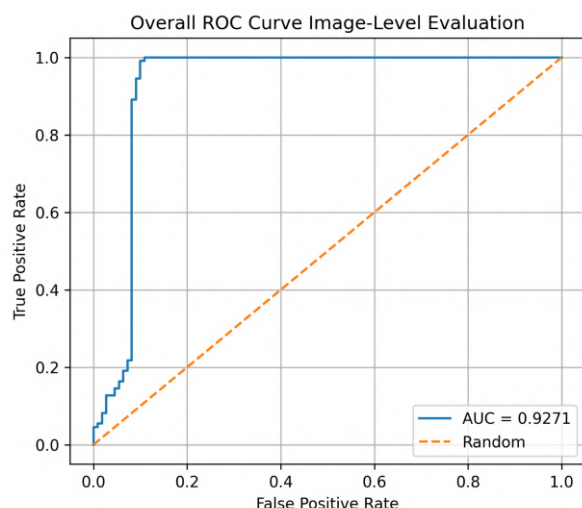
$$ACCURACY = (TP + TN) / (TP + FN + FP + FN). \quad (5)$$

The CNN-LBPNET model achieved a total accuracy of 94.55% on the MICC-F220 dataset, demonstrating impressive effectiveness in identifying image forgery. It achieved an impressive 208 out of 220 test image classifications across five folds with a fixed threshold of 0.5, boasting a true positive rate of 100% and a false negative rate of 0%. Subsequently, all modified images were correctly detected, demonstrating the model's accurate nature and recommending its possible use in real-world security measures. With a true negative rate of 89.09%, the model displayed notable efficacy in image classification, correctly identifying the majority of original images.

Nevertheless, it appears that some original images were incorrectly identified as fake, with a false positive rate of 10.91%. The combination of convolutional neural network (CNN) spatial characteristics with local binary pattern (LBP) texture features offered a strong and efficient method for distinguishing between authentic and

Table 2. Testing the proposed method on MICC-F220 yielded the following results

Dataset	TPR%	FPR%	FNR%	TNR%	Accuracy
MICCF220	100	10.91	0	89.09	94.55

**Fig. 8.** ROC-AUC of the proposed model

forged images, with an F1-Score of 94.83% and a ROC-AUC of 92.71%.

Figures 7 and 8 represent the confusion matrix and ROC-AUC of the proposed model, respectively. The confusion matrix demonstrates the potency of the proposed approach, proving its important capability to identify forged images. It successfully recognized all of the 110 forged images, indicating superior sensitivity and zero false negatives. Though it accurately identified 98 original images, it incorrectly classified 12 as forged. This suggests a strategic focus on minimizing the chances of overlooking manipulated images, which is crucial for effective forgery detection. The lack of false negatives emphasizes the model's practicality, while the false positives point to areas that could be improved by changing the threshold, incorporating more texture descriptors, or growing the validation dataset.

The CNN-LBPNET model performed proficiently in detecting image forgeries, according to the results analyzed from tests conducted on the MICC-F220 dataset. Despite the need to proceed

with caution when comparing the model to existing approaches partly due to differences in evaluation and preprocessing techniques, the model's 94.55% accuracy is significant.

It successfully identified all manipulated images, with an impeccable true positive rate of 100% and a false negative rate of 0%. Emphasizing the model's potential to improve forgery detection capabilities, this reliability is critical for situations where failing to notice altered images might have catastrophic implications. Combining convolutional neural network (CNN) spatial data with local basis function (LBP) texture descriptors yields a strong representation without requiring a complex architecture by bringing together semantic and local texture intelligence.

The results confirm that this feature fusion approach is successful and well-suited for identifying image forgery, even though there was a false positive rate of 10.91%, which means that some legitimate photos were mistakenly recognized as forged images.

Table 3 represents the comparative analysis of proposed model with existing methods. This study compares the efficiency of a different technique for detecting image forgery with that of more traditional methods by analyzing the MICC-F220 dataset. This assessment places an emphasis on precision and pertinent measures, recognizing that previous research has used different dataset handling, preprocessing, feature extraction, classifier design, and validation techniques, so a more indicative performance analysis is required instead of conventional exploratory replicated data.

5 Conclusions

The study demonstrates CNN-LBPNET, a hybrid model for image-level forgery detection. The model efficiently captures both structural content and local texture variations by combining handcrafted

Table 3. Comparative analysis of the proposed CNN-LBPNET model and existing methods for detecting image forgeries

Dataset	Technique	Year	TPR%	FPR%
MICC-F220	SLIC-SIFT-Hu-HOG [33]	2022	99.10	7.20
MICC-F220	SIFT-DBSCAN-EL [9]	2024	96.00	-
MICC-F220	DBSCAN [37]	2025	90.91	10.91
MICC-F220	SIFT-BIRCH [37]	2025	99.09	15.45
MICC-F220	Proposed CNN-LBPNET	Proposed	100.00	10.91

Note: "-" indicates that corresponding value is not reported.

texture descriptors with deep spatial representations. Single-feature approaches may miss tiny inconsistencies that are frequently present in modified photos, but this novel fusion approach improves their detection. Furthermore, applying an image-level cross-validation process ensures a fair assessment of the model's performance on both genuine and forged samples, leading to more reliable forgery detection methods. To classify binary forgeries, the research indicates that a combination of convolutional neural network (CNN) feature learning and linear regression (LBP) texture analysis works well. This model is excellent for first forensic screening since it is so effective at detecting fake photos. It needs additional improvement before it can be utilized safely in key forensic scenarios, though, because it has issues involving misclassifying some real images. Improving specificity without compromising the model's ability to recognize altered content is crucial.

Further improvement is necessary to raise specificity and decrease false alarms in order to make the proposed framework more effective. To evaluate the framework's potential to generalize across various manipulation types, compression levels, and picture capture methods, future studies should test it on larger and more diverse forensic datasets.

Furthermore, the method can progress from image-level categorization to pixel-level localization, identifying exact regions that have been altered. Enhancing the framework's resilience, interpretability, and practical utility in digital forensic investigations can be achieved by using adaptive threshold calibration, false-positive-aware optimization, and interpretable artificial intelligence visualization techniques.

References

1. **Ahmed, I. T., Hammad, B. T., Jamil, N. (2021).** A comparative analysis of image copy-move forgery detection algorithms based on hand and machine-crafted features. *Indones. J. Electr. Eng. Comput. Sci.*, Vol. 22, No. 2, pp. 1177–1190. DOI: 10.11591/ijeecs.v22.i2.pp1177-1190.
2. **Arun, A. (2015).** Image forgery and its detection: a survey. *International Conference on Innovations in Information*. DOI: 10.1109/ICIIECS.2015.7193253.
3. **Bansal, A., Atri, A. (2020).** Study of copy-move forgery detection techniques in images. *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, IEEE, pp. 630–635. DOI: 10.1109/ICRITO48877.2020.9197801.
4. **Barad, Z. J., Goswami, M. M. (2020).** Image forgery detection using deep learning: a survey. *2020 6th international conference on advanced computing and communication systems (ICACCS)*, IEEE, pp. 571–576. DOI: 10.1109/ICACCS48705.2020.9074408.
5. **Bharti, C. N., Tandel, P. (2016).** A survey of image forgery detection techniques. *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, IEEE, pp. 877–881. DOI: 10.1109/WiSPNET.2016.7566257.
6. **Brock, A., Donahue, J., Simonyan, K. (2018).** Large scale gan training for high fidelity natural image synthesis.

- arXiv preprint arXiv:1809.11096. DOI: <https://doi.org/10.48550/arXiv.1809.11096>.
7. **Castillo Camacho, I., Wang, K. (2021).** A comprehensive review of deep-learning-based methods for image forensics. *Journal of imaging*, Vol. 7, No. 4, pp. 69. DOI: <https://doi.org/10.3390/jimaging7040069>.
 8. **Castillo Camacho, I., Wang, K. (2021).** Data-dependent scaling of cnn's first layer for improved image manipulation detection. *Digital Forensics and Watermarking: 19th International Workshop, IWDW 2020, Melbourne, VIC, Australia, November 25–27, 2020, Revised Selected Papers 19*, Springer, pp. 208–223. DOI: https://doi.org/10.1007/978-3-030-69449-4_16.
 9. **Dabhole, S. D., Rajput, G., et al. (2024).** Copy-move image forgery detection and classification using sift and dbSCAN approaches. *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, pp. 1–7. DOI: [10.1109/ICCCNT61001.2024.10724022](https://doi.org/10.1109/ICCCNT61001.2024.10724022).
 10. **Diallo, B., Urruty, T., Bourdon, P., Fernandez-Maloigne, C. (2019).** Improving robustness of image tampering detection for compression. *MultiMedia Modeling: 25th International Conference, MMM 2019, Thessaloniki, Greece, January 8–11, 2019, Proceedings, Part I 25*, Springer, pp. 387–398. DOI: https://doi.org/10.1007/978-3-030-05710-7_32.
 11. **Farid, H. (2008).** Digital image forensics. *Scientific American*, Vol. 298, No. 6, pp. 66–71. DOI: [10.1109/MSP.2008.931078](https://doi.org/10.1109/MSP.2008.931078).
 12. **Farid, H. (2009).** Image forgery detection. *IEEE Signal processing magazine*, Vol. 26, No. 2, pp. 16–25. DOI: [10.1109/MSP.2008.931079](https://doi.org/10.1109/MSP.2008.931079).
 13. **Gill, N. K., Garg, R., Doegar, E. A. (2017).** A review paper on digital image forgery detection techniques. *2017 8th international conference on computing, communication and networking technologies (ICCCNT)*, IEEE, pp. 1–7. DOI: [10.1109/ICCCNT.2017.8203904](https://doi.org/10.1109/ICCCNT.2017.8203904).
 14. **Guan, H., Kozak, M., Robertson, E., Lee, Y., Yates, A. N., Delgado, A., Zhou, D., Kheyrkhah, T., Smith, J., Fiscus, J. (2019).** Mfc datasets: Large-scale benchmark datasets for media forensic challenge evaluation. *2019 IEEE Winter Applications of Computer Vision Workshops (WACVW)*, IEEE, pp. 63–72. DOI: [10.1109/WACVW.2019.00018](https://doi.org/10.1109/WACVW.2019.00018).
 15. **He, P., Li, H., Wang, H., Zhang, R. (2020).** Detection of computer graphics using attention-based dual-branch convolutional neural network from fused color components. *Sensors*, Vol. 20, No. 17, pp. 4743. DOI: <https://doi.org/10.3390/s20174743>.
 16. **Hingrajiya, K. H., Sheth, R. K. (2021).** Comparative study of digital image forgery detection techniques. *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, IEEE, pp. 83–86. DOI: [10.1109/ICACITE51222.2021.9404748](https://doi.org/10.1109/ICACITE51222.2021.9404748).
 17. **Huynh, T. K., Huynh, K. V., Le-Tien, T., Nguyen, S. C. (2015).** A survey on image forgery detection techniques. *The 2015 IEEE RIVF International Conference on Computing & Communication Technologies-Research, Innovation, and Vision for Future (RIVF)*, IEEE, pp. 71–76. DOI: [10.1109/RIVF.2015.7049877](https://doi.org/10.1109/RIVF.2015.7049877).
 18. **Jiang, L., Li, R., Wu, W., Qian, C., Loy, C. C. (2020).** Deepforensics-1.0: A large-scale dataset for real-world face forgery detection. *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 2889–2898. DOI: [10.1109/CVPR42600.2020.00296](https://doi.org/10.1109/CVPR42600.2020.00296).
 19. **Karras, T., Aila, T., Laine, S., Lehtinen, J. (2017).** Progressive growing of gans for improved quality, stability, and variation. *arXiv preprint arXiv:1710.10196*. DOI: <https://doi.org/10.48550/arXiv.1710.10196>.
 20. **Koul, S., Kumar, M., Khurana, S. S., Mushtaq, F., Kumar, K. (2022).** An efficient approach for copy-move image forgery detection using convolution neural

- network. *Multimedia Tools and Applications*, Vol. 81, No. 8, pp. 11259–11277. DOI: <https://doi.org/10.1007/s11042-022-11974-5>.
21. **Koul, S., Kumar, M., Khurana, S. S., Mushtaq, F., Kumar, K. (2022).** An efficient approach for copy-move image forgery detection using convolution neural network. *Multimedia Tools and Applications*, Vol. 81, No. 8, pp. 11259–11277. DOI: <https://doi.org/10.1007/s11042-022-11974-5>.
 22. **Kumar, S., Gupta, S. K., Gupta, U., Agarwal, M. (2023).** Non-overlapping block-level difference-based image forgery detection and localization (nb-localization). *The Visual Computer*, Vol. 39, No. 12, pp. 6029–6040. DOI: <https://doi.org/10.1007/s00371-022-02710-z>.
 23. **Kuznetsov, O., Frontoni, E., Romeo, L., Rosati, R. (2024).** Enhancing copy-move forgery detection through a novel cnn architecture and comprehensive dataset analysis. *Multimedia Tools and Applications*, pp. 1–35. DOI: <https://doi.org/10.1007/s11042-023-17964-5>.
 24. **Lu, M., Niu, S. (2020).** A detection approach using lstm-cnn for object removal caused by exemplar-based image inpainting. *Electronics*, Vol. 9, No. 5, pp. 858. DOI: <https://doi.org/10.3390/electronics9050858>.
 25. **Majumder, M. T. H., Alim Al Islam, A. B. M. (2018).** A tale of a deep learning approach to image forgery detection. 2018 5th International Conference on Networking, Systems and Security (NSysS), pp. 1–9. DOI: 10.1109/NSysS.2018.8631389.
 26. **Manjunatha, S., Patil, M. M. (2017).** A survey on image forgery detection techniques. *Digital Image Processing*, Vol. 9, No. 5, pp. 103–108. DOI: DIP052017003.
 27. **Pham, N. T., Park, C.-S. (2023).** Toward deep-learning-based methods in image forgery detection: A survey. *IEEE Access*, Vol. 11, pp. 11224–11237. DOI: 10.1109/ACCESS.2023.3241837.
 28. **Rani, P. S., Kumar, A. (2019).** Digital image forgery detection techniques: A comprehensive review. 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, pp. 959–963. DOI: 10.1109/ICECA.2019.8822064.
 29. **Sabeena, M., Abraham, L. (2024).** Convolutional block attention based network for copy-move image forgery detection. *Multimedia Tools and Applications*, Vol. 83, No. 1, pp. 2383–2405. DOI: <https://doi.org/10.1007/s11042-023-15649-7>.
 30. **Shwetha, B., Sathyanarayana, S. (2017).** Digital image forgery detection techniques: a survey. *ACCENTS Transactions on Information Security*, Vol. 2, No. 5, pp. 22–31. DOI: 10.19101/TIS.2017.25003.
 31. **Sri, C. G., Bano, S., Deepika, T., Kola, N., Pranathi, Y. L. (2021).** Deep neural networks based error level analysis for lossless image compression based forgery detection. 2021 International Conference on Intelligent Technologies (CONIT), IEEE, pp. 1–8. DOI: 10.1109/CONIT51480.2021.9498357.
 32. **Tyagi, S., Yadav, D. (2023).** Mininet: a concise cnn for image forgery detection. *Evolving Systems*, Vol. 14, No. 3, pp. 545–556. DOI: <https://doi.org/10.1007/s12530-022-09446-0>.
 33. **Ye, W., Zeng, Q., Peng, Y., Liu, Y., Chang, C.-C. (2022).** A two-stage detection method of copy-move forgery based on parallel feature fusion. *Eurasip Journal on wireless communications and networking*, Vol. 2022, No. 1, pp. 30. DOI: <https://doi.org/10.1186/s13638-022-02112-8>.
 34. **Yu, Y., Li, Y., Zhang, Z., Gu, Z., Zhong, H., Zha, Q., Yang, L., Zhu, C., Chen, E. (2020).** A bibliometric analysis using vosviewer of publications on covid-19. *Annals of translational medicine*, Vol. 8, No. 13. DOI: 10.21037/atm-20-4235.
 35. **Zhang, R.-S., Quan, W.-Z., Fan, L.-B., Hu, L.-M., Yan, D.-M. (2020).** Distinguishing computer-generated images from natural images using channel and pixel correlation. *Journal of Computer Science and*

Technology, Vol. 35, pp. 592–602. DOI: <https://doi.org/10.1007/s11390-020-0216-9>.

- 36. Zhu, J.-Y., Park, T., Isola, P., Efros, A. A. (2017).** Unpaired image-to-image translation using cycle-consistent adversarial networks. Proceedings of the IEEE international conference on computer vision, pp. 2223–2232.

- 37. Zhuang, Z. (2025).** Copy-move image forgery detection and classification using sift and birch approaches. ITM Web of Conferences, EDP Sciences, Vol. 78, pp. 02018. DOI: <https://doi.org/10.1051/itmconf/20257802018>.

Article received on 29/04/2026; accepted on 27/05/2026.

**Corresponding author is Prathi Naveena.*