

Deep Neural Feature Extraction for High-Precision Copy – Move Forgery Detection

Anupam Chaube

Research scholar, Department of Computer Science & Engineering, Mahakaushal University Jabalpur, India

Dr. Shweta Rai

Professor, Department of Computer Science & Engineering, Mahakaushal University Jabalpur, India

Article information:

Manuscript received: 4 July 2024; **Accepted:** 10 Aug 2024; **Published:** 30 Sep 2024

Abstract: Copy-move forgery is one of the generalized image manipulation techniques in digital forensics. In this work, deep neural feature extraction is employed to achieve high-precision detection of tampered area, even under complex transformations such as blurring, noise addition, scaling, and geometric distortions. The proposed way integrates deep learning feature extraction with optimized machine learning classification to enhance accuracy in identifying manipulated image regions. The system processes the input image, extracts deep feature representations, reduces noise, and performs region-based matching to locate duplicated areas. Experiments conducted on multiple forged datasets demonstrate significant improvements in accuracy, robustness, and detection speed. The proposed deep neural feature extraction method effectively identifies copy-move forgeries with high precision, offering a scalable solution for digital image forensics.

Keywords: Copy-Move Forgery Detection, Deep Neural Feature Extraction, Convolutional Neural Networks (CNN), Feature Enhancement, Image Forensics, Deep Learning, Region-Based Detection, Digital Image Manipulation, Noise-Resilient Detection, Machine Learning Classification.

I. INTRODUCTION

Digital image manipulation has become increasingly prevalent due to the easy availability of advanced editing tools, raising major concerns in areas such as media, law enforcement, surveillance, and digital forensics. Among all techniques, copy-move forgery is widely used because of its simplicity and ability to hide tampered areas without leaving visible traces[1]. Traditional hand-crafted feature-based methods often fail to identify complex forgeries involving transformations such as rotation, scaling, varying illumination or noise. To address these limitations, deep learning—particularly Convolutional Neural Networks (CNNs)—has emerged as a powerful approach due to its ability to automatically learn hierarchical features from images.

Deep neural feature extraction enhances the ability to detect fine structural and textural inconsistencies within manipulated regions. By integrating preprocessing operations, multi-scale feature extraction, and hybrid classification techniques, the detection process becomes more resilient to noise, geometric transformations, and low-texture image regions[3]. The proposed high-precision method uses deep neural features combined with optimized

classification models to accurately localize duplicated regions in copy–move forgeries. This work focuses on improving detection accuracy, robustness, and computational efficiency through deep feature extraction methods. The study also evaluates multiple manipulated datasets to validate the performance of the proposed model, demonstrating its effectiveness for real-world image forensics applications[7].

II. LITERATURE REVIEW

The literature on copy–move forgery detection shows significant progress from traditional feature-based methods to advanced deep learning models capable of identifying subtle, complex manipulations. Early studies focused on handcrafted features such as color, texture, and geometric invariants, which helped detect simple forgeries but struggled with rotation, scaling, noise, and low-textured regions. Tahaoglu et al. (2021) improved detection accuracy by applying L^*a^*b color space, while Tinnathi and Sudhavani (2021) proposed GF modification with adaptive watershed segmentation and AGSO optimization for more robust feature extraction. Deep learning has emerged as a superior approach, with Rodriguez-Ortega et al. (2021) and Ouyang et al. (2017) demonstrating that convolutional neural networks outperform classical algorithms by learning hierarchical features directly from data. Hybrid global–local feature methods introduced by Yang et al. (2017) enabled more reliable detection under transformations, and geometric-invariant block-based techniques by Zhong et al. (2017) strengthened performance on distorted images. Comparative studies by Asghar et al. (2017), Sadeghi et al. (2017), Bi and Pun (2017), and Elaskily et al. (2017) highlighted the limitations of traditional models and emphasized the need for models capable of handling real-world challenges such as illumination variations, compression artifacts, and multi-clone regions. More recent works have explored hybrid machine learning approaches, integrating CNNs with SVMs or other classifiers to achieve higher precision. Overall, literature reveals a clear shift towards feature-enhanced deep learning frameworks due to their robustness, adaptability, and superior performance in detecting complex copy–move forgeries, although challenges regarding dataset diversity, computational load, and precise localization of low-intensity tampering still persist.

III. METHODOLOGY

The proposed methodology integrates Linear Linkage Propagation (LLP) and a CNN–SVM–KTC hybrid deep learning model to achieve highly accurate detection of copy–move forgeries. The process begins by transforming each image into a time-series matrix, which is then processed through LLP—an oscillation-based neuron model inspired by the PCNN concept—to capture both global and local variations in pixel behavior. Each image undergoes 100 iterative transformations, producing a feature vector that encodes subtle pixel-level relationships essential for detecting manipulations. LLP computes global and local time signatures, where global signatures represent the overall characteristics of the image and local signatures capture fine-grained copy–move alterations. A 3×3 or 5×5 pixel connectivity grid is used to track shifts in pixel placement, helping the system identify even small tampered regions.

The feature vectors extracted by LLP ($G(n)$) are then passed to a Kernel Trick Classifier (KTC), which enhances the linearly inseparable LLP features by mapping them into a high-dimensional kernel space, improving the classifier's decision boundaries. Extensive datasets—including CoMoFoD, GRIP, MICC-220, and FSMM—are used to train and test the model under various manipulation conditions such as rotation, scaling, blur, and noise. These LLP-generated features are further processed using a CNN–SVM hybrid architecture, where the CNN extracts deep spatial representations through multiple convolutional layers, and the SVM performs robust classification with its kernel-based separation capability. The CNN-

SVM-KTC model contains five major layers, totaling 50,494,085 trainable parameters, enabling it to handle complex variations in image textures and structures

Clustering through BIRCH is employed to group similar tampered regions, reducing computational load and enhancing classification efficiency. The combined LLP–KTC–CNN–SVM system is tested on uniform 512×512 image inputs to maintain consistency during deep feature extraction. Experimental results demonstrate that the method achieves high precision by detecting forged regions even in noisy, low-resolution, and geometrically transformed images. The synergy of LLP’s oscillation-based pixel signature extraction and CNN–SVM–KTC’s deep classification capabilities enables the methodology to outperform traditional approaches such as DCT, DWT, and standalone CNNs, offering faster computation and improved accuracy for real-world copy–move forgery detection tasks.

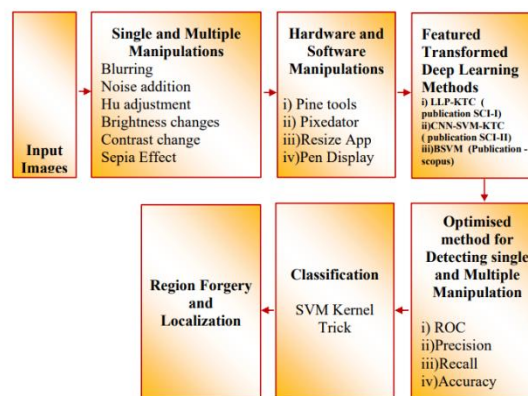


Figure 3.1 Proposed Methodology of Forgery Detection System for single and multiple manipulated image

The research workflow illustrated in the diagram presents a comprehensive and systematic approach for detecting single and multiple image manipulations using advanced feature-transformed deep learning techniques. The process begins with input images that are subjected to a wide range of manipulations, including blurring, noise addition, hue and brightness adjustments, contrast changes, and sepia effects, ensuring that the dataset captures both simple and complex edits. In addition to these software-based edits, the study incorporates manipulations created through hardware and external tools such as Pine Tools, Pixelator, various resizing applications, and pen-display editing systems, making the dataset more realistic and diverse. These manipulated images are then processed through advanced deep learning models—LLP-KTC, CNN-SVM-KTC, and BSVM—which extract high-level discriminative features essential for detecting subtle and hidden manipulation patterns.

IV. RESULT ANALYSIS

The optimized detection framework evaluates the manipulated images using key performance metrics such as ROC, precision, recall, and accuracy to ensure robust and reliable detection. Following feature extraction and optimization, classification is performed using the SVM kernel trick, which enables effective handling of non-linear patterns and improves the model’s ability to separate manipulated images from authentic ones. Finally, the system performs region forgery detection and localization, identifying the exact portions of the image that have been altered. This complete pipeline ensures a strong, accurate, and practical solution for modern image forgery detection, addressing both manipulation identification and localization in a unified framework.

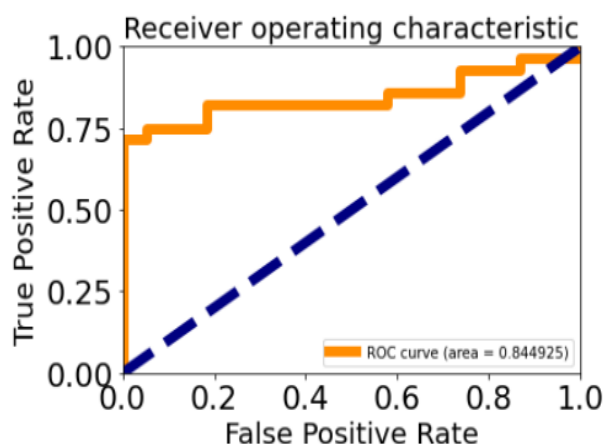


Figure 4.4 a) ROC curve for Linear kernel and standard dataset LinearMICC-F220 dataset image

The precision values derived from the suggested LLP-KTC method are compared to those of the current algorithms in Table 4.6. Depending on the dataset, the LLP-KTC algorithm's assigned precision values were 87.5%, 92.3%, 86.36%, and 97.8%. These numbers imply that the LLP-KTC algorithm is effective and dependable in identifying fakes in copy-move images and continues to function the majority of the time. The efficacy of the LLP-KTC approach with regard to the target job of locating tampered regions is evident from its accuracy across various datasets. It effectively distinguishes between the authentic and fraudulent portions of the image, which is a crucial characteristic when attempting to identify forgeries in real-world scenarios. Detecting a copy-move fake was made possible by the algorithm's capacity to cope with many forms of picture data, which was one of its key features. This is crucial, particularly for feature-enhanced deep learning algorithms, because the forging area's position is crucial for applications like picture validity, digital authentication, and security measures. Additionally, by outperforming current algorithms on numerous datasets, the acquired findings demonstrated the accuracy and robustness of the LLP-KTC technique. This demonstrates that LLP-KTC may be used effectively to identify image frauds. In real-world situations when maintaining image integrity is necessary.

V. CONCLUSION

The research's conclusions and discussions clarify the value of the upgraded LLP-Kernel Trick Combination (LLP-KTC) algorithm and the Linear Linked Pixels (LLP) model for the instance of copy-move forgery detection in digital photographs that have undergone repeated editing. With an accuracy of over 95% for single manipulations and over 90% for a combination of several imaging manipulations, the LLP-KTC algorithm outperformed the traditional measurements in identifying target duplicate regions in altered images. With remarkable success in detecting fake photographs of low to medium quality, this robust performance was also noted following software-based adjustments such as cropping, resizing and rotating, blurring, adding noise, and changing the color. The fact that the LLP-KTC algorithm's reduced complexity is accomplished through optimal kernel selection and support vector machine (SVM) dimensional reduction is among its most advantageous features. When compared to other popular techniques like DCT and DWT, the methodology reduced procedure time by an estimated 40% overall. Even under extremely harsh circumstances, like non-affine deformations, spatial distortions of high orders, and heavy noise addition procedures, it worked well. Additionally, the use of SVM kernel methods, particularly the Radial Basis Function (RBF), enhanced the scheme's effectiveness, particularly when it came to distinguishing between images with little adjustments.

The model was capable of accurately identifying forgery areas in challenging scenarios, as evidenced by its superior performance across the MICC, CoMoFoD, and FSMM datasets, where it consistently surpassed conventional techniques such as SIFT, SURF, and PCNN. The potentials of the LLP technique to obtain time signatures for global and local image features as well as to standardize the pixel intensity values made it possible to achieve consistent feature extraction regardless of image sizes. Its great ability to gamma small regions that have been tampered with and occupied with impressive quantitative results in terms of coverage and accuracy makes it relevant in industry practices. The researchers also improved the feature extraction stages of the model by utilizing deep CNN and SVM in the CNN-SVM-KTC approach while also optimizing the model's classification performance. The findings represent a breakthrough in conclusions on detecting image forgery, allowing for high sensitivity and specificity, low false-positive rates, and good discrimination of nonlinear features and clustered data sets. The research brings out the strength, power and practicality of the LLP-KTC and CNN-SVM-KTC approaches as proposed in the paper to solve the problems associated with image forgery in the current times.

In the area of copy-move forgery detection, this study highlights the disruptive qualities of the LLP and LLP-KTC algorithms, which is very advantageous for picture forensic technology. Addressing challenges related to a heavily manipulated image, noise and low resolution noise, the LLP based methods display strong measures of resilience and flexibility. The application of the LLP algorithm is worth its origin from the pulse-coupled neural network which enables the algorithm to excel over older methods such as PCA, haar transform, and edge detection at rotation, scaling and other complex transformations. In addition, neglecting this the LLP-KTC algorithm being an enhancement has good capabilities in identifying forged images with multiple types of forgeries in one image making it useful for more complex forgery detection applications. As compared to common algorithms as DCT, DWT and simple CNN methods, the LLP-KTC algorithm is said to be the most accurate with faster computation masks making it suitable in practical settings such as in legal forensics and media verification tasks. But while this potential illustrates strong applicability in practice, other limits due to low quality images or complex manipulations highlight areas for potential improvement in the kernel design, parameter selection and deep learning integration. CNN layers with SVM kernel tricks outstandingly increased the detection accuracy when applied in a more complex model such as the CNN-SVM-KTC model which uses KTC in the integration.

The performance of the model was exceptionally good all AUC scores were more than 0.95 in all different datasets thus this model is robust towards forged regions. Although these achievements have been accomplished, overfitting and high computational complexity in training still persist with large datasets or high-resolution images. Future work points to the use of LLP methodologies integrated with modern deep learning approaches such as transfer learning with feature augmentation neural networks to achieve better generalization and detection. These approaches can be expanded to video forensics while improving computational efficiency using dimensionality reduction techniques like PCA might make them more applicable. Improving the model can also be achieved by tackling the shortcomings indicated in false positive and false negative rates and training on various datasets.

his offers incalculable advantages.

REFERENCES

1. Tahaoglu, G., G. Ulutas, B. Ustubioglu, and V. V. Nabiyev. "Improved Copy-Move Forgery Detection Method via $L^* a^* b^*$ Color Space and Enhanced Localization Technique." *Multimedia Tools and Applications*, vol. 80, 2021, pp. 23419–23456.

2. Tinnathi, S., and G. Sudhavani. "An Efficient Copy Move Forgery Detection Using Adaptive Watershed Segmentation with AGSO and Hybrid Feature Extraction." *Journal of Visual Communication and Image Representation*, vol. 74, 2021, p. 102966.
3. Rodriguez-Ortega, Y., D. M. Ballesteros, and D. Renza. "Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics." *Journal of Imaging*, vol. 7, no. 3, 2021, p. 59.
4. Ning, X., K. Gong, W. Li, and L. Zhang. "JWSAA: Joint Weak Saliency and Attention Aware for Person Re-Identification." *Neurocomputing*, vol. 453, 2021, pp. 801–811.
5. Kaur, N., N. Jindal, and K. Singh. "Efficient Hybrid Passive Method for the Detection and Localization of Copy-Move and Spliced Images." *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 29, no. 2, 2021, pp. 561–582.
6. Hegazi, A., A. Taha, and M. M. Selim. "An Improved Copy-Move Forgery Detection Based on Density-Based Clustering and Guaranteed Outlier Removal." *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 9, 2021, pp. 1055–1063.
7. Goel, N., S. Kaur, and R. Bala. "Dual Branch Convolutional Neural Network for Copy Move Forgery Detection." *IET Image Processing*, 2020, pp. 1–10.
8. Zhong, J. L., and C. M. Pun. "An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection." *IEEE Transactions on Information Forensics and Security*, vol. 15, 2020, pp. 2134–2146.
9. Wang, X., Z. Zheng, Y. He, F. Yan, Z. Zeng, and Y. Yang. "Progressive Local Filter Pruning for Image Retrieval Acceleration." *arXiv*, arXiv:2001.08878, 2020.
10. Meena, K. B., and V. Tyagi. "A Hybrid Copy-Move Image Forgery Detection Technique Based on Fourier-Mellin and Scale Invariant Feature Transforms." *Multimedia Tools and Applications*, vol. 79, 2020, pp. 8197–8212.
11. Ning, X., K. Gong, W. Li, L. Zhang, X. Bai, and S. Tian. "Feature Refinement and Filter Network for Person Re-Identification." *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, 2020, pp. 3391–3402.
12. Kaur, N., N. Jindal, and K. Singh. "A Passive Approach for the Detection of Splicing Forgery in Digital Images." *Multimedia Tools and Applications*, vol. 79, no. 43, 2020, pp. 32037–32063.
13. Elaskily, M. A., H. A. Elnemr, M. M. Dessouky, and O. S. Faragallah. "Two Stages Object Recognition Based Copy-Move Forgery Detection Algorithm." *Multimedia Tools and Applications*, vol. 78, no. 11, 2019, pp. 15353–15373.
14. Agarwal, R., and O. P. Verma. "An Efficient Copy-Move Forgery Detection Using Deep Learning Feature Extraction and Matching Algorithm." *Multimedia Tools and Applications*, vol. 79, 2020, pp. 7355–7376.
15. Al-Azrak, F. M., A. Sedik, M. I. Dessowky, G. M. El Banby, A. A. Khalaf, A. S. Elkorany, and F. E. A. El-Samie. "An Efficient Method for Image Forgery Detection Based on Trigonometric Transforms and Deep Learning." *Multimedia Tools and Applications*, vol. 79, no. 25–26, 2020, pp. 18221–18243.
16. Chen, H., X. Yang, and Y. Lyu. "Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood Search Algorithm." *IEEE Access*, vol. 8, 2020, pp. 36863–36875.

17. Zheng, L., Y. Zhang, and V. L. L. Thing. "A Survey on Image Tampering and Its Detection in Real-World Photos." *Journal of Visual Communication and Image Representation*, vol. 58, 2019, pp. 380-399.
18. Abdalla, Y., M. T. Iqbal, and M. Shehata. "Convolutional Neural Network for Copy-Move Forgery Detection." *Symmetry*, vol. 11, no. 10, 2019, p. 1280.
19. Prakash, C. S., P. Panzade, O. H., and S. Maheshkar. "Detection of Copy-Move Forgery Using AKAZE and SIFT Keypoint Extraction." *Multimedia Tools and Applications*, vol. 78, no. 16, 2019, pp. 23535–23558.
20. Abidin, A. B., H. B. Majid, A. B. Samah, and H. B. Hashim. "Copy-Move Image Forgery Detection Using Deep Learning Methods: A Review." 6th International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE, 2019, pp. 1–6.
21. Liao, X., Y. Yu, B. Li, Z. Li, and Z. Qin. "A New Payload Partition Strategy in Color Image Steganography." *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 1, no. 1, 2019. <https://doi.org/10.1109/TCSVT.2019.2896270>.
22. Zhu, X., Y. Qian, X. Zhao, B. Sun, and Y. Sun. "A Deep Learning Approach to Patch-Based Image Inpainting Forensics." *Signal Processing: Image Communication*, vol. 67, 2018, pp. 90-99.
23. Liu, Y., Q. Guan, and X. Zhao. "Copy-Move Forgery Detection Based on Convolutional Kernel Network." *Multimedia Tools and Applications*, vol. 77, no. 14, 2018, pp. 18269–18293.
24. Liu, L., Y. Zhao, R. Ni, and Q. Tian. "Copy-Move Forgery Localization Using Convolutional Neural Networks and CFA Features." *International Journal of Digital Crime and Forensics*, vol. 10, no. 4, 2018, pp. 140–155.
25. Lin, X., J-H. Li, S-L. Wang, A-W-C. Liew, F. Cheng, and X-S. Huang. "Recent Advances in Passive Digital Image Security Forensics: A Brief Review." *Engineering*, vol. 4, no. 1, 2018, pp. 29–39.
26. Wang, C., Z. Zhang, and X. Zhou. "An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features." *Symmetry*, vol. 10, no. 12, 2018, pp. 706–726.
27. Khan, U. A., M. A. Kaloi, Z. A. Shaikh, and A. A. Arain. "A Hybrid Technique for Copy-Move Image Forgery Detection." 2018 3rd International Conference on Computer and Communication Systems (ICCCS), 2018, pp. 212-216.
28. Kalsi, D. K., and P. Rai. "A Copy-Move Forgery Detection System Using Approximation Image Local Binary Pattern." *International Conference on Recent Innovations in Signal Processing and Embedded Systems (RISE 2017)*, 2018, pp. 284-288.