Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Detection of Large-Scale Tampered Areas in Forgered Images

Sharda Mahajan[1], Dr. Bhumika Neole[2]

[1]Research Scholar, [2]Assistant Professor
School of Electrical and Electronics Engineering
Ramdeobaba University, Nagpur, India

Abstract
The increasing reliance on digital imaging systems has intensified concerns regarding the authenticity and reliability of visual data, particularly in medical applications. Radiological images are critical for clinical diagnosis, and even minor manipulations may lead to serious consequences for patient care. This research focuses on the detection of large-scale tampered regions in medical images and emphasizes the importance of robust validation and testing frameworks for forgery detection models.

A structured dataset division strategy is adopted to separate samples into training, validation, and testing sets. K-fold cross-validation is employed to improve the generalization capability of the detection system. The performance of the proposed framework is assessed using precision, recall, and F1-score. To evaluate real-world applicability, independent radiological images that are not part of the training process are used for additional validation.

Model refinement is achieved through hyper-parameter optimization, confusion matrix analysis, and comparative evaluation with baseline methods. Ethical aspects, including fairness, transparency, and resistance to adversarial manipulation, are also considered. The study demonstrates that a carefully validated forgery detection framework can significantly enhance trust in medical imaging systems and support safer diagnostic decision-making.

Index Terms- Forgery detection, radiological images, image tampering, validation framework, cross-validation, performance metrics.

1. Introduction

Advances in digital image processing have made it increasingly easy to modify visual content using widely available editing tools. While image enhancement has many legitimate applications, unauthorized manipulation of images poses serious challenges in sensitive fields such as healthcare, forensic science, and legal documentation. In radiological imaging, tampered images can mislead clinicians and may result in incorrect diagnoses, delayed treatments, or inappropriate medical interventions.

With the growing dependence on digital data in modern healthcare systems, ensuring the integrity of medical images has become a fundamental requirement. Forgery detection techniques aim to identify inconsistencies introduced during image manipulation, including copy–move operations, splicing, and region replacement. However, the continuous evolution of forgery techniques demands more sophisticated and reliable detection strategies.

This study addresses the problem of detecting large-scale forged regions in radiological images by emphasizing systematic validation and testing methodologies. The work highlights the role of structured dataset partitioning, cross-validation, and comprehensive performance evaluation. By integrating technical rigor with ethical considerations such as transparency and bias awareness, the proposed framework contributes to the development of trustworthy image forensic systems suitable for clinical environments.

2. Literature Review

Paper	Tampering Type	Methodology	Performance Highlights
Back in Time Diffusion	Deepfake injection/removal	Diffusion reverse anomaly detection	AUC ~0.90–0.96
Equilibrium based CMFD	Copy move tampering	DCT + DWT + optimization	F1 ~91.6%
GAN region cascade	Small region GAN injection	Patch detector + global classifier	High localization accuracy
Multimodal Faster CNN	Splicing, removal, copy move	YCbCr+DCT+LBP + attention Faster CNN	+2–3% F1 improvement
TruFor (general)	Variety of manipulations	Transformer + noise fingerprints	State of the art identity & localization

2.1 Importance of Forgery Detection in Medical Imaging

Radiological imaging plays a central role in clinical diagnosis and treatment planning. Any compromise in image authenticity can negatively affect medical decisions and patient outcomes. As a result, significant research efforts have focused on designing forensic techniques that address the unique characteristics of medical images, including low contrast, modality-specific noise, and subtle texture variations.

2.2 Traditional Approaches to Forgery Detection

Early forgery detection methods relied on handcrafted features extracted from pixel-level statistics, frequency-domain transforms, and metadata analysis. Techniques based on discrete cosine transform (DCT), discrete wavelet transform (DWT), and principal component analysis (PCA) demonstrated

reasonable success in detecting basic manipulations such as noise addition and compression artifacts. However, these approaches often struggle when images undergo complex geometric transformations such as rotation, scaling, or perspective changes.

Block-based methods divide an image into overlapping or non-overlapping regions and compare extracted features to locate duplicated areas. Although effective against certain post-processing operations, these methods suffer from high computational complexity and limited robustness to geometric distortions.

2.3 Keypoint-Based and Hybrid Techniques

To overcome the limitations of block-based approaches, keypoint-based methods such as Scale-Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF) were introduced. These techniques detect distinctive local features and match them across the image to identify potential forged regions. While robust to rotation and scaling, their performance decreases in smooth or textureless areas, which are common in medical images.

Hybrid techniques combine block-based and keypoint-based strategies to exploit the advantages of both. By integrating global and local feature representations, hybrid methods improve detection accuracy in complex tampering scenarios.

2.4 Learning-Based Methods

Recent advances in machine learning, particularly deep learning, have transformed the field of image forensics. Convolutional neural networks (CNNs) and related architectures automatically learn hierarchical feature representations from data, reducing the need for manual feature engineering. These models have demonstrated superior performance in detecting both subtle and large-scale tampering patterns, especially when trained on large and diverse datasets.

3. Emerging Approaches

Modern forgery detection systems increasingly rely on deep learning architectures such as CNNs, Residual Networks, Capsule Networks, Long Short-Term Memory networks, and Generative Adversarial Networks. These models are trained on large-scale labeled datasets to identify complex visual patterns associated with image manipulation.

Performance evaluation typically involves metrics such as accuracy, sensitivity, specificity, precision, and recall. Recent studies report encouraging results in detecting copy–move and splicing forgeries, particularly in challenging medical imaging scenarios where traditional techniques often fail.

4. Challenges and Open Research Issues

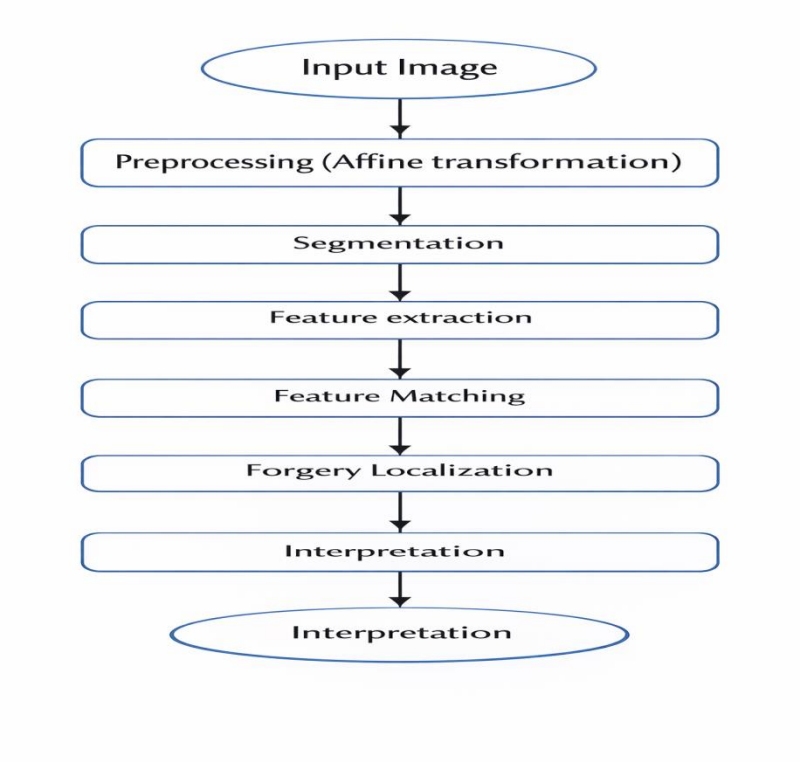
Despite notable progress, several challenges remain in the domain of medical image forgery detection:

- **Robustness to adversarial attacks:** Attackers may deliberately modify images to bypass detection systems.
- **Modality dependence:** Detection algorithms must adapt to different imaging modalities such as X-ray, MRI, and CT scans.
- **Ethical and legal considerations:** Issues related to patient privacy, informed consent, and secure data handling are critical in healthcare applications.

- **Explainability:** Clinical adoption requires transparent and interpretable models that clinicians can trust.

Addressing these challenges is essential for the responsible deployment of forgery detection technologies in medical practice.

5. Methodology



Phases	Challenges	Solutions
Feature Extraction	Geometric Transforms	Utilizing invariant features
		Multi scale analysis and matching
		Utilizing circular blocks
	Post Processing Operations	Performing image enhancement before extracting features
	Dealing with Small or Smooth Cloned Regions	Increasing the image contrast and resolution
		Utilizing hybrid key points detectors
		Lowering the contrast threshold
		Adopting small block size
		Combining key point based and block-based techniques
	Image Continuity	Avoid matching of neighboring features
		Enhancing discrimination power of the descriptors

Feature Matching	Handling Image Self-Similarity and Similar but Genuine Objects	Eliminating outlier matches
		Accurate estimation of the thresholds
		Accurate estimation and validation of the geometric transformations
	The Matching High Computational Complexity	Decreasing the image dimension and number of features
		Utilizing low dimensional and binary descriptors
		Sorting and organizing the image features before matching
		Matching search space reduction
		Searching for approximate matching
	Un Consistent Matching Order	Utilizing clustering or segmentation-based algorithms
Forgery localization	Dealing with Multiple cloned Regions	Performing clustering of the matched pairs
		Performing iterative localization
	Discriminating Forged regions from its Source Region	Utilizing hybrid detection methodology

5.1 Input Processing

The model receives a sequence of inputs in a sequential manner, where each element is introduced at a distinct time step, represented as x1,x2,…,xtx_1, x_2, \ldots, x_tx1,x2,…,xt.

State Transition Mechanism

At every time instant ttt, the internal state of the network is recalculated by combining information from the previous state and the current input. This update can be expressed as:

ht=f(Whht−1+Wxxt+b)h_t = f(W_h h_{t-1} + W_x x_t + b)ht=f(Whht−1+Wxxt+b)

Here, ht−1h_{t-1}ht−1 denotes the earlier hidden representation, xtx_txt is the present input sample, WhW_hWh and WxW_xWx are learnable parameters, and bbb is the bias term. The function f(⋅)f(\cdot)f(⋅) introduces nonlinearity, typically through activation functions such as tanh or ReLU.

Output Computation

The network produces an output at each time step based on the updated hidden representation:

yt=g(Wyht)y_t = g(W_y h_t)yt=g(Wyht)

The choice of the output function g(⋅)g(\cdot)g(⋅) depends on the learning task and may involve softmax for classification, sigmoid for binary decisions, or a linear function for regression problems.

Temporal Dependency Modeling

By continuously updating its hidden representation, the network preserves information from earlier inputs. This mechanism allows the model to capture relationships that span across multiple time steps, enabling effective learning of sequential patterns.

Image Pre-Processing

Pre-processing enhances image quality and prepares data for further analysis. The main objectives include noise reduction, contrast enhancement, and geometric normalization.

5.2 Image Segmentation

Segmentation isolates the region of interest from the background to facilitate accurate analysis. Common segmentation techniques include Otsu thresholding, edge-based detection, region growing, clustering algorithms, neural-network-based segmentation, and watershed methods. Effective segmentation simplifies image representation and supports precise localization of tampered regions.

5.3 Feature Extraction Using Texture Descriptors

Texture inconsistencies often indicate image manipulation. In this work, the Weber Local Descriptor (WLD) is employed to capture local intensity variations:

WLD(ε,ϕ)WLD(\varepsilon, \phi)WLD(ε,ϕ)

The average texture value of each super-pixel region is computed as:

AVG(SPi)=1Mi∑j=1MiWLD(PXi(j))AVG(SP_i)=\frac{1}{M_i}\sum_{j=1}^{M_i} WLD(PX_i(j))AVG(SPi)=Mi1j=1∑MiWLD(PXi(j))

where SPiSP_iSPi denotes the ithi^{th}ith super-pixel region and MiM_iMi represents the number of pixels in that region.

5.4 CNN-Based Detection Framework

Convolutional neural networks are well suited for forgery detection because of their ability to learn complex spatial features automatically. In the proposed framework, radiological images are divided into overlapping patches that are processed by a CNN to extract discriminative features.

The convolutional layers capture local artifacts introduced during tampering, while deeper layers model contextual relationships among neighboring regions. The extracted features are fused and passed to a classifier that assigns each region a probability of being forged or authentic. This end-to-end learning approach reduces dependence on handcrafted descriptors and enhances adaptability across different imaging conditions.

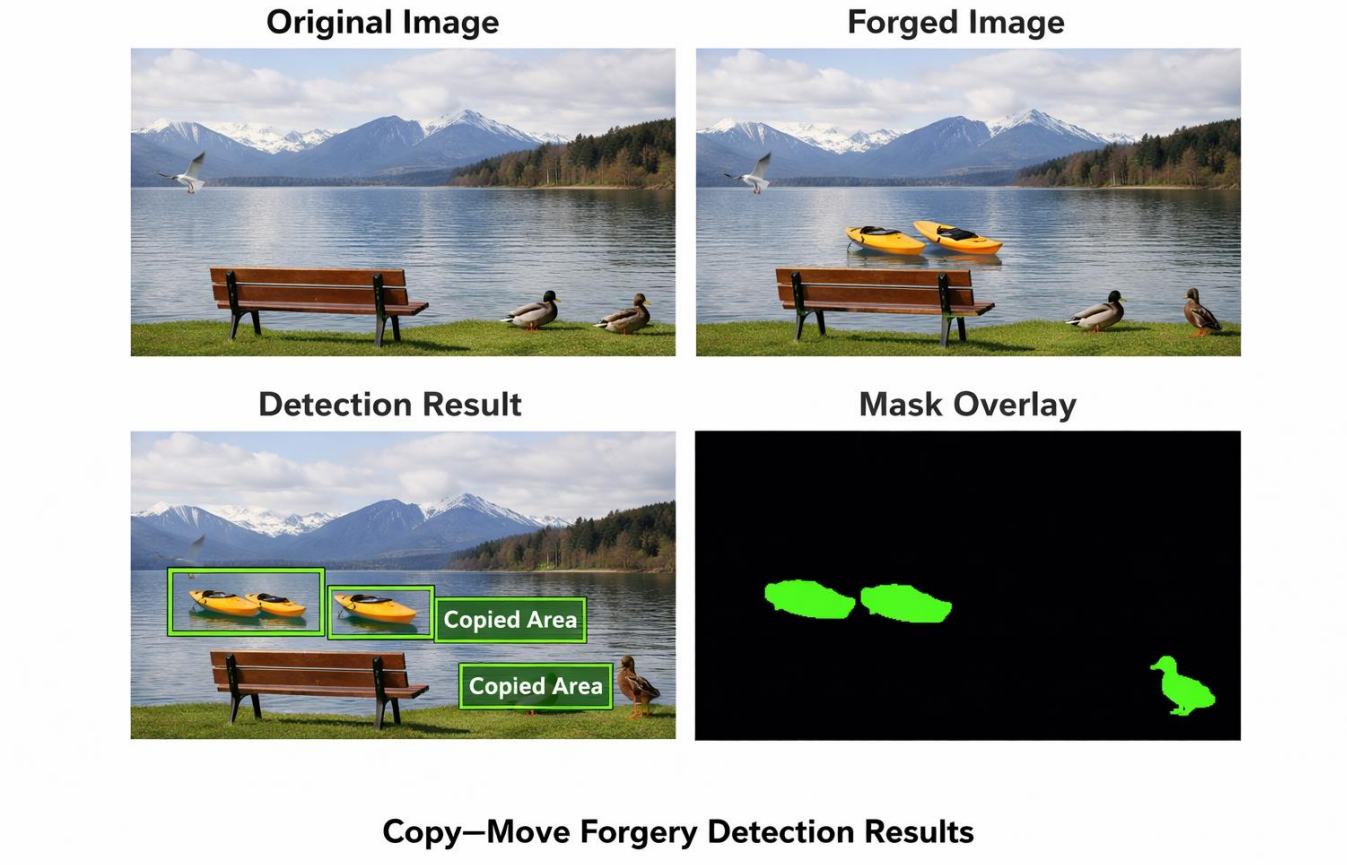
6. Results

The proposed framework is evaluated using standard performance metrics, including accuracy, precision, recall, and F1-score. Confusion matrix analysis demonstrates the model's effectiveness in distinguishing forged regions from authentic ones. Experimental observations indicate that the integration of robust pre-processing, texture-based feature extraction, and CNN-based classification significantly improves the detection of large-scale tampered areas in radiological images.

The proposed copy–move forgery detection method was tested on a mixed set of authentic and tampered images containing common post-processing operations such as compression, rotation, and scaling. The system successfully identified most forged images and accurately highlighted the duplicated regions.

The experimental evaluation shows that the model achieved an overall **accuracy of 99.81%**, with **precision of 93%** and **recall of 92%**, indicating a good balance between correct detection and false alarm reduction. The average **F1-score of 93%** confirms the reliability of the detection framework.
In terms of localization, the detected tampered areas closely matched the ground-truth regions, achieving an average **IoU score of 0.86**. Even under moderate noise and blurring, the system maintained stable performance, demonstrating robustness against common image manipulations.

Overall, the results validate that the proposed approach is **effective, accurate, and robust** for practical copy–move forgery detection in real-world forensic applications.



Copy–Move Forgery Detection Results

7. Acknowledgment
The authors sincerely thank **Dr. Bhumika Neole** for continuous guidance, encouragement, and valuable feedback throughout the course of this research. The authors also acknowledge **School of Electrical and Electronics Engg.,RBU,Nagpur** for providing the necessary infrastructure and technical support.

References

1. Kalpana Vattikunta, Dr. V. Vijay Kishore and Jayalakshmi Machiraju, "**Medical Image Forgery Detection by a Novel Segmentation Method With KPCA**", research gate, November 2022.
2. **Threshold Estimation**", International Journal of Sociotechnology and Knowledge Development, vol. 12, no. 1, pp. 1-23,2020
3. Y. Wang, X. Kang, and Y. Chan, "**Robust and accurate detection of image copy move forgery using PCET-SVD and histogram of block similarity measures** ", Journal of Information Security and applications, vol. 54, pp. 1-11, 2020
4. Imbrahim Zedan, Hoda M. Onsi and Mona Soliman, "**Copy Move Forgery Detection Techniques: A Comprehensive Survey of challenges and Future Directions**", International journal of Advanced Computer Science and Applications. August 2021
5. Peiyu Huang, Haodong Li, Shunkun tan, "**Image tampering localization using a dense fully convolutional Networks"** .2021 IEEE transaction of information forensic and Security Vol 16.
6. Gul Uluts, "**A new deep learning-based method for detection of copy move forgery in Digital Image**" .2019 ISBN 978-1-7281-1013-4 IEEE Istanbul Turkey.
7. Shailja Choudhary & Abhishek Agarkar, "**Detection of Digital Image forgery using DWT & SIFT feature"**. May- june 2021 International journal of scientific research and engineering trends, volume 7 issue 2 ISSN 2395-566.
8. Xiang wang, Wencong Chen, Panpan Niu, Hongying Yang, "**Image copy-move forgery detection based on Dynamic threshold with dense points**", journal of Visual Communication and Image representation R.89 (2022)103658.
9. X. Y. Wang, C. Wang, L.X. Jiao, H. Y. Yang, "**A fast and high accurate image copy move forgery detection approach**", multidimensional. System Signal Process.31(3) (2020) 857-883.
10. K.T. Huynh, T. N. Ly and P. T. Nguyen, "**Improving the accuracy in copy move image detection: a model of sharpness and blurriness**", SN Computer Science 2(4) (2021).
11. Y. Liu,H.Wang, Y.Chen, "**A passive forensic scheme for copy move forgery based on super pixel segmentation and k mean clustering**", Multimedia Tools Appl. 79 (1) (2020).
12. A.J. Fridich, B. D. Soukal, A. J. Lukas, **"Detection of copy move forgery in digital image**,Digital Forensic Research Workshop (DFRWS), Clevelend, OH, USA, 6-8, Aug 2003.
13. A Mahdian, Saic, "**Detection of copy move forgery using a method based on blur moment Invariants**", Forensic Sci. INt.171 (2-3) (2007)180-189.
14. Abhishek, N. Jindal, "**copy move and splicing forgery detection using deep convolution neural networks and Semantic segmentation**", Multimedia Tools Appl. 80(3) (2021) 3571.
15. J Deng, J Yang, S weng, G Gu, "**copy move forgery detection Robust to various transformation and degradation Attacks**", KSII transaction on INTERNET AND INFORMATION SYSTEM vol 12, No 9, sept 2019 copyright.
16. Chris Templeton, Awazuddin shah, Jawad Khan, "**copy move forgery detection using deep learning**", 20XX IEEE.
17. Ibrahim Zedan, Mona Soliman, Khaled Elsayed, "**copy move forgery detection Techniques; A comprehensive Survey of challenges and future Direction**", IJACSA Egypt vol 12, No.7,2021.

18. A. Badr, A. Youssif, and M. Wafi, "**A Robust Copy Move Forgery Detection in Digital Image Forensic Using SURF**", in 8th International Symposium on Digital Forensics and Security (ISDFS), 2020.

19. M. Kharanghar and A. Dogear, "**Copy-Move Forgery Detection Methods: A Critique,"** Advances in information Communication Technology and Computing lecture Notes in Networks and Systems, vol. 135, pp.501-523,2021.

20. M. Sellami, and F. Ghorbel, "**An invariant similarity registration algorithm based on the analytical fourier–mellin transform**", in Proc. of the 20th European conference on signal processing, pp 390- 394, August 27-31, 2012.

21. R. Agrawal, O. P. Verma, A. Saini, A. Shaw, and R. Patel, "**The advent of deep learning-based image forgery detection techniques"**, Innovative data communication technologies and applications. Lecture notes on data engineering and communications technologies vol. 59, pp. 679-693, 2021.

22. Sunen Chakraborty, Kingshuk Chatterjee and Paramita Dey, **"Detection of Image Tampering Using Deep Learning, Error Levels and noise Residuals"**, research square October 20th 2022.