International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 03 | Mar 2025 www.irjet.net p-ISSN: 2395-0072

Image Forgery Detection Techniques with a Focus on Copy-Move Forgery Problem Definition and MATLAB-Based Solutions

Miss. Apeksha P. Ingle[1], Dr. C.N. Deshmukh[2], Dr. D.T. Ingole[3]

[1]*(Mater of Engineering , Electronics & Telecommunication Engineering) Student, Prof .Ram Meghe Institute of Techonology & Research Badnera,*

[2]*Head of Department, Prof. Ram Meghe Institute of Techonology & Research Badnera,*

[3]*Principal, Takshashila Institute of Eengineering and Technology Darapur, Sant Gadge Baba Amravati University, Amravati, Maharashtra*

Abstract - *Digital image manipulation, specifically copy-move forgery, poses a significant challenge given the easy access to editing software. This research examines block-oriented (including DCT, PCA, DWT) and key point-oriented (such as SIFT, SURF) detection techniques, evaluates their shortcomings, and introduces a combined methodology integrating both approaches. MATLAB-based implementation is suggested to address computational complexity, localization accuracy, and robustness to geometric transformations. A MATLAB-based solution is recommended to tackle processing efficiency, detection precision, and resilience against geometric modifications.*

Key Words: *: Copy-move forgery, Digital copyright, Feature Extraction, Detection.*

1.INTRODUCTION

- **Context:** The proliferation of social platforms and image manipulation tools has made forgery identification crucial for legal, media, and investigative purposes.
- **Challenge:** Copy-move forgery, involving the duplication of content within an image, presents unique difficulties due to its subtle nature and subsequent modifications (like scaling, rotation, noise insertion).
- **Objective:** Create an effective, comprehensive detection system using MATLAB to address existing methodological limitations.

1.1 IMAGE FORGERY DETECTION TYPES

Authentication verification establishes image legitimacy. Various approaches have been developed to validate authentic images. These methods can be broadly classified into two main groups:

- Active techniques
- Passive techniques

This classification is based on whether the source image is available or not. Each approach can be further subdivided. The classification hierarchy is illustrated in figure 1.

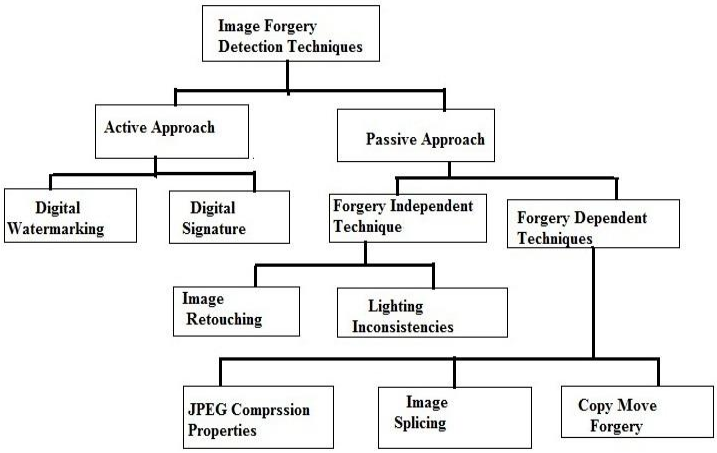

Fig. 1: Types of Image Forgery Detection

1.1.1 Active Forgery identification Techniques

Active forgery detection methodology requires pre-embedded or pre-extracted data. Digital Watermarking and digital signature techniques are commonly employed methods in the active detection approach.

1.1.2 Passive Forgery detection Techniques

Passive techniques, also known as blind methods, utilize only the image itself for authentication and integrity verification. This approach operates on the premise that even when visual tampering signs are absent, the manipulation may disrupt underlying statistical properties through noise inconsistencies, image blur effects, enhancement artefacts, copy-move forgery, and image inpainting operations.

Forgery dependent methodologies are designed to identify specific types of manipulations, such as splicing, which rely on the nature of alterations performed on the image. Forgery independent approaches detect manipulations that are not tied to specific fraud types but instead focus on traces left by processes like sharpening, blurring, and irregularities in lighting and shadow patterns.

1.2 GENERALIZED SCHEMA FOR IMAGE FORGERY IDENTIFICATION

Forgery identification in pictures is two step issue. The principle target of blind forgery detection technique stays to categorize a given picture as real or altered. A widely used schema of image forgery identification procedure, that comprises of the following steps:

1. **Image Pre-processing**: This initial phase involves various pre-processing operations on the target image, including filtering, enhancement, cropping, DCT coefficient modifications, and color space conversion from RGB to grayscale before proceeding with feature extraction. Algorithms may or may not incorporate this step based on specific computational requirements.

2. **Feature Extraction**: Feature selection for each class differentiates image sets across various classes while maintaining consistency within a specific chosen class. The selected feature set should ideally be compact to reduce computational complexity while maintaining significant distinction between classes.

3. **Selection of Classifier**: Based on the extracted feature set from the previous step, an appropriate classifier is either selected or designed. Larger training datasets typically result in enhanced classifier performance.

4. **Classification**: The fundamental aim of classification is to determine image authenticity. Common classifiers employed include Neural Networks, LDA, and SVM.

5. **Postprocessing**: Certain forgeries may require additional processing steps, such as identifying copied regions.

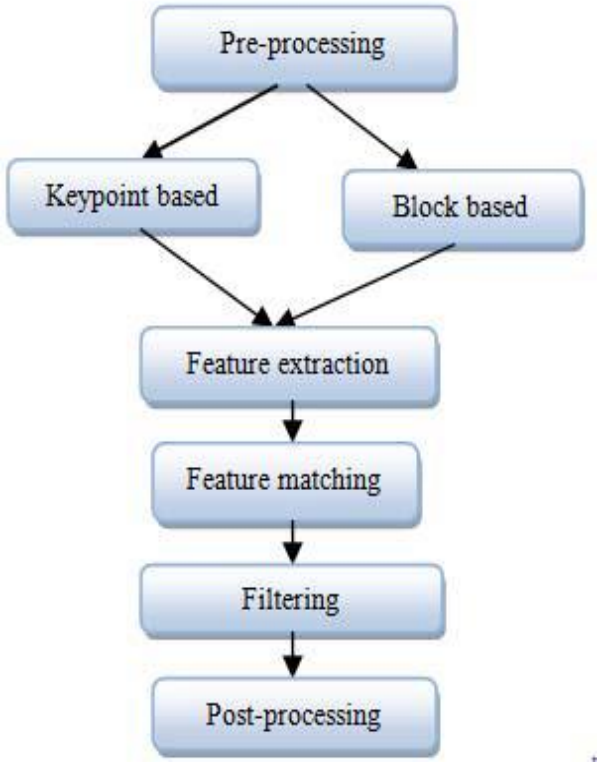

Fig. 2: Generalized schema for image forgery detection

2. Literature Review

Copy-Move fabrication discovery strategies can be arranged into two approaches:

1. Key point based methodologies.
2. Block based methodologies

Key point based approaches utilize scale and rotation invariant feature detection and description algorithms, primarily Speeded-up Robust Features (SURF) and Scale Invariant Feature Transform (SIFT).

Block based techniques employ various transformation methods including Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA), Singular Value Decomposition (SVD), and Discrete Cosine Transform (DCT).

The following table outlines the methodologies, key contributions, and inherent limitations of each referenced study, along with proposed solutions to address identified gaps:

Reference	Method	Contribution	Limitations
Fridrich et al. [4]	Block-based DCT + lexicographical sorting	Introduced efficient block matching via DCT coefficient sorting.	Fails for small duplicated regions; sensitive to geometric transformations.
Popescu & Farid [5]	PCA-based dimension reduction	Reduced computational cost using PCA for overlapping blocks.	Low accuracy for small block sizes (e.g., 32x32).
Li et al. [6]	DWT + SVD	Combined DWT for dimensionality reduction and SVD for robust feature extraction.	Limited robustness to rotation/scaling; high memory usage.
Bayram et al. [8]	Fourier-Mellin Transform (FMT)	Invariant to translation/scaling; robust to noise.	Computationally expensive; struggles with complex transformations.
Ryu et al. [9]	Zernike Moments	Rotation and blur invariance; localized tampered regions.	High computational cost; fails for scaled regions.
Bo et al. [10]	SURF-based key points	Efficient feature detection using Hessian matrix; robust to noise.	Poor localization accuracy; cannot delineate exact forged regions.
Amerini et al. [11]	SIFT-based detection	Detected geometrically transformed regions using SIFT.	High false positives; computationally intensive for large images.
Zhong & Xu [12]	Gaussian Pyramids	Used multi-scale decomposition for low-frequency analysis.	Limited to specific forgery types; poor recall rates.
Thajeel & Sulong [13]	Block-based + Hu Moments	Combined fixed-sized blocks with Hu moments for feature extraction.	Inefficient for high-resolution images; lacks robustness to post-processing.

Table -1: Contributions and Limitations

3. Problem Synthesis

In copy-move forgery detection, block-based and key-point-based algorithms emerge as the predominant methodological approaches. Fridrich et al. [4] presents a block-based methodology utilizing discrete cosine transform (DCT), where feature extraction involves quantized DCT coefficients from overlapping blocks. However, this approach demonstrates limited effectiveness in identifying small duplicated regions. Popescu et al. [5] implements Principal Component Analysis (PCA) to achieve dimensionality reduction during feature extraction. Subsequent methodologies incorporate DWT and SVD algorithms for image feature point extraction. The field has also witnessed the introduction of key-point-based techniques for forgery region identification. Scale Invariant Feature Transform (SIFT) enables key-point extraction, while Speeded Up Robust Features (SURF) focuses on identifying interest points rather than utilizing blocks for tampering detection. While these approaches successfully identify matching points, they fall short in precisely localizing forged image regions. Most block-based detection techniques, though utilizing identical algorithms, differ primarily in their feature extraction methodologies. These approaches consistently demonstrate suboptimal recall rates.

Key Challenges Identified:

1. **Computational Complexity:** Block-based approaches (e.g., DCT, PCA) demand extensive comparisons, while key point-based methods (e.g., SIFT, SURF) demonstrate poor scaling with increasing image dimensions.

2. **Geometric Transformations:** Existing methods struggle to detect duplicated regions modified through rotation, scaling, or blurring operations.

3. **Localization Precision:** Key point-based approaches identify matches but fail to delineate exact tampered region boundaries.

4. **Threshold Dependency:** The requirement for manual threshold adjustment (e.g., θ, R) restricts generalization across diverse datasets.

4. CONCLUSIONS

The widespread accessibility of digital image manipulation tools has transformed copy-move forgery detection into a crucial challenge for validating image authenticity. This comprehensive review examined block-based methodologies (incorporating DCT, PCA, DWT) and key point-based approaches (utilizing SIFT, SURF), evaluating their respective advantages and drawbacks. While block-based techniques demonstrate superior accuracy in identifying duplicated regions, their computational demands are substantial, and they exhibit vulnerability to geometric transformations. Conversely, key point-based approaches, though resilient to scaling and rotation manipulations, demonstrate limitations in precise boundary detection and efficiency with larger images. Analysis of current research reveals several persistent challenges: substantial computational requirements, vulnerability to post-processing modifications, and suboptimal localization precision. To overcome these limitations, this study proposes integrating block-based and key point-based

methodologies into a unified framework. This hybrid approach aims to capitalize on the complementary strengths of both techniques, enhancing resilience to geometric transformations while maintaining precise localization capabilities. MATLAB emerges as the optimal development environment, providing comprehensive tools for algorithm implementation, performance optimization, and validation, particularly in addressing computational efficiency and scalability concerns.

Subsequent research directions will concentrate on enhancing this hybrid framework, streamlining feature extraction and matching mechanisms, and conducting extensive validation across multiple datasets. Priority will be given to developing automated threshold selection processes, reducing manual calibration requirements and improving universal applicability. Successfully implementing these improvements could substantially advance forensic analysis, legal proceedings, and journalistic verification by delivering an efficient, dependable solution for identifying sophisticated forgeries. This research establishes groundwork for developing a robust, adaptable detection system, connecting theoretical advancements with practical implementation requirements.

REFERENCES

[1] G.K.Birajdar and V.H.Mankar,"Digital image forgery detection using passive techniques:A survey",Digital investigations,pp.226-245,2013.

[2] "A Review Paper on Digital Image Forgery Detection Techniques", Navpreet Kaur Gill, Ruhi Garg, Er.Amit Doegar, 8th ICCCNT 2017

[3] "*Image forgery detection for high resolution images using SIFT and RANSAC algorithm*", Gonapalli Ramu, S.B.G. Thilak Babu, Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017)

[4] Fridrich,D.Soukal and J.Luka,"Detection of copy-move forgery in digital images", in Digital Forensic Research Workshop,pp.6-8,2003..

[5] Popescu, A1in c., and Hany Farid, "Exposing digital forgeries by detecting duplicated image regions", Department of Computer Science, Dartmouth College, Technical Report. TR2004-515, August 2004.

[6] G. Li, Q. Wu, D. T u, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China, pp. 1750-1753, July 2-5, 2007.

[7] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast And Robust Forensics for Image Region duplication Forgery,"in Proceedings ofActa Automatica Sinica, Vol. 35, pp. 1488-1495, 2009

[8] S. Bayram, H. T aha Sencar and N. Memon, "An Efficient and Robust Method for Detecting Copy-Move Forgery,"in IEEE InternationalConference on Acoustics, Speech and Signal Processing, Taipei, pp. 1053-1056, 2009

[9] S. Ryu, M. Lee and H. Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," in Proceedings of InformationHiding Springer Berlin Heidelberg, pp. 1053-1056, 2009

[10] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image Copy-Move Forgery Detection Based on Surf,"in Proceedings of MultimediaInformation Networking and Security, International Conference On, pp.889-892, 2010

[11] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "An SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery,"in Proceedings of IEEE Transactions onInformation Forensics and Security, vol. 6, no. 3, pp. 1099-1110 Sept. 2011