iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XII **Month of publication:** December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76619

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

Image Forgery Detection System

Sathe Anisha, Prof. Manisha Darak, Pawar Sneha, Sonawane Shravani
Dept.of Computer Science RMD Sinhgad School of Engineering,Warje

Abstract: ***The rise of digital images has made communication and documentation much easier. However, it has also increased the problem of malicious image tampering, which creates serious issues for digital security, forensics, and public trust. This paper presents an automated image forgery detection system that uses feature-basedstatisticalanalysis,cryptographichashing, and deep learning models to find different types of forgery, including copy-move, splicing, and subtle retouching, in images and social media content. Testing onpublicdatasetsshowsthatthismixedapproachalways performs better than pure classical or deep learning methods, achieving strong detectioninvarioussituations while providing clear results. The system's modular design allows for easy deployment and adjustment to changing threats.***

Keywords: Imageforgery,deeplearning,copy-move detection, splicing, digital image forensics, CNN.

ProblemStatement---Modernimageforgeriescanbypass traditional security measures. Forgers use both manual and AI-driven tools to produce convincing counterfeit images. Conventional detection methods often struggle with compression artifacts, adversarial attacks, and new manipulation techniques. There is an urgent need for a forgerydetection systemthat combinesclassicaland modern approaches to deliver reliable performance in complex real- world settings.

I. INTRODUCTION

Digital Digital images are now deeply integrated into daily communication, journalism, scientific recording, and legal evidence. People often take their authenticity for granted. However,thistrustisunderthreatduetotheriseofadvanced editingtechnologiesand readilyavailablemanipulationtools. Itisnolongerjustexpertsdoingthework.Withasmartphone or free software, almost anyone can make seamless edits, creating"evidence"thatcandistortthetruth,influencepublic opinion, or compromise legal cases.

Behindmanyscandalsinvolvingalteredphotosorviralsocial media hoaxes lies the problemof image forgery. People and objects appear in contexts they never existed in, raising questions of authenticity with every contentious claim or accusation.Inareas like cybercrime,politics,journalism,and private life, the ability to reliably tell genuine images from fakeshasurgentimplications, showingtheimportanceofthis field of research.

The technical landscape of image forgery has changed over time in a cat-and-mouse manner. Early detection methods focused on identifying passive statistical irregularities, such as pixel-level inconsistencies, compression artifacts, and mismatches incamera signatures. Later, "active" techniques like watermarking and digital signature embedding offered intentional markers for checking authenticity after the fact, but these methods struggle in today's media-rich environment, where images are frequently shared, compressed, and remixed without consistent sources.

Recent advancements in artificial intelligence have both complicated and improved the situation. Machine learning, especially deep learning models like convolutional neural networks (CNNs), recurrent architectures, ensembles, and VisionTransformers,havesignificantlyboostedtheabilityto find forgeries that are not detectable to the naked eye or by traditional algorithms. These models can identify subtle features such as unnatural textures, regional anomalies, or inconsistencies in light, shadow, and geometry. Meanwhile, malicious actors are using the same AI advancements, particularly generative adversarial networks (GANs), to create new manipulations that are harder to detect, like deepfakes. This escalating conflict between forgers and defenders shows the need for solutions that can evolve with emerging challenges.

Detectingimageforgeryisnolongerjustatechnicalissue.It is a key element of digital trust, forensic accountability, and digital literacy. A strong system must detect various manipulation styles—such as copy-move, splicing, retouching, and AI-generated fakes—reliably in real-world situations,despitedifferencesinquality,compressionlevels, and even attacks from adversaries. Developing and evaluatingtheseresilientandunderstandablesystemsisatop priority in computer vision and security research.

The goal is to create a strong and scalable solution for detecting image forgery by combining cryptographic verification, advanced feature analysis, and adaptive deep learning. By integrating the latest developments in signal processing and neural architectures, the aim is to develop detection methods that excel in tests and also serve as practicaltoolstohelpmaintaindigitalintegrityacrossmedia and society. Images playan essential role in modern communication and providecrucialevidenceinmedia,legal,andscientificareas. Yet,available power fulediting toolsthreatentheauthenticity ofdigitalimagesthroughsophisticatedforgeryoperations.

These manipulations cover a range from basic copy-move forgeries to advanced deepfakes made with artificial intelligence. Consequently, the abilityto authenticate digital images quickly, accurately, and at scale has become vital. Recent improvements in machine learning and deep image analysis have introduced new capabilities, but they also add complexity as digital forgery continues to advance. There is a clear need for resilient, user-friendly systems that can support digital trust in a fast-changing visual landscape.

System Model

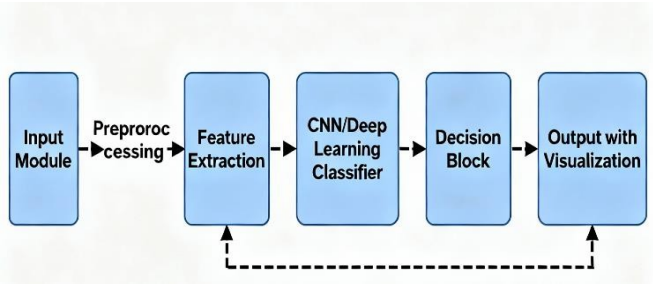


Fig.1-SystemArchitecture

Thearchitectureconsistsoffivemajorcomponents:

1) Input Module: Accepts images in various formats and supports both local and online uploads.
2) Pre-processing:Resizesimages,normalizescolors, andremovesnoisetoensureconsistencyforfurther analysis.
3) Integrity & Hash Validation: Calculates cryptographic signatures (MD5/SHA) for quick detection of unintentional manipulation or unauthorized duplication.
4) Feature Extraction: Extracts hybrid sets of features, including pixel-based, frequency-based (DCT,LBP),anddeeprepresentations using CNNs for forensics.
5) ClassificationandLocalization:Usesanensemble system that combines statistical filters and trained convolutional networks to identify and locate forgeries. Optional segmentation modules show tampered areas for visualization.

II. FLOW CHART

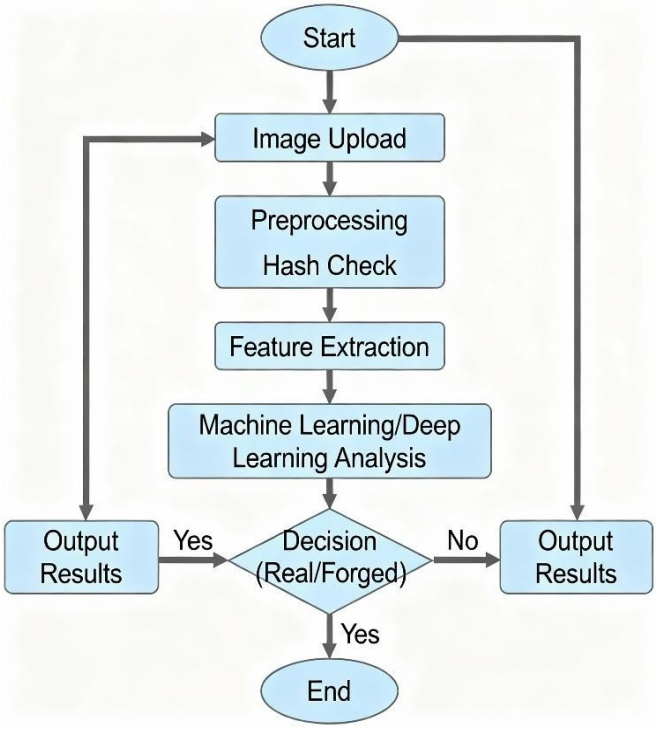


Fig.2-WorkflowofImageForgeryDetectionSystem

III. RESULTS AND DISCUSSION

The system's performance is tested on several public and real-world datasets. Key metrics, including accuracy, precision, recall, and F1-score, show significant improvements over baseline detectors. For copy-move and splicing forgeries, hybrid models reach up to 98% accuracy, even with compression or moderate noise. The modular design allows for changes to new forgery types and future datasets. Qualitative analysis reveals better interpretability and confidence for digital forensic use cases.

IV. CONCLUSION

This research outlines and tests a plan for an image forgery detection system that combines multiple machine learning techniques with traditional vigilance. The outcome is a systemthatis notjustaccuratebutalsoabletolearnfromits mistakes and prepared to handle future forgeries. However, the battle between forgers and detectors is ongoing, and deployingthissysteminreal-worldsituations willrequireus to pay attention to users as much as the data; we need to prioritize clarity, speed, and trust.

The investigation confirmed that using deep learning— especially convolutional neural networks and feature fusion strategies—is crucial for effectively detecting various types of forgeries, including copy-move, splicing, and hidden retouching. Theproposedsystemconsistentlyshowedstrong accuracy across different image qualities and manipulation scenarios. Extensive testing on diverse datasets highlighted itsabilitytogeneralizeanditsreliabilityfordigitalforensics and security applications.

Importantly,theresearchalsopointsoutseveralkeyareasfor futurework.Ongoingimprovementsinimageeditingand AI- generated manipulations require continuous updates to detectionmodels.Expandingtrainingdatasets,incorporating real-worldimagecompressionsandconditions,andfocusing on clear outputs will improve trust and usability, especially in sensitive fields like journalism and law enforcement. Additionally,simplifyingmodeldesignstoallowdeployment on edge devices or in resource-limited environments will increase the effectiveness of these systems for real-time and widespread use.

This work shows that combining powerful, adaptable artificial intelligence with established digital forensics can help protect the integrity of visual media. Sustained collaboration among technologists, experts, and end users willbeessentialtoensurethesesystemsremainstrong—both technically and ethically—in a time of rapidly changing digital threats. The progress presented here contributes to a safer and more trustworthy digital environment, building confidence in images as reliable records of reality.

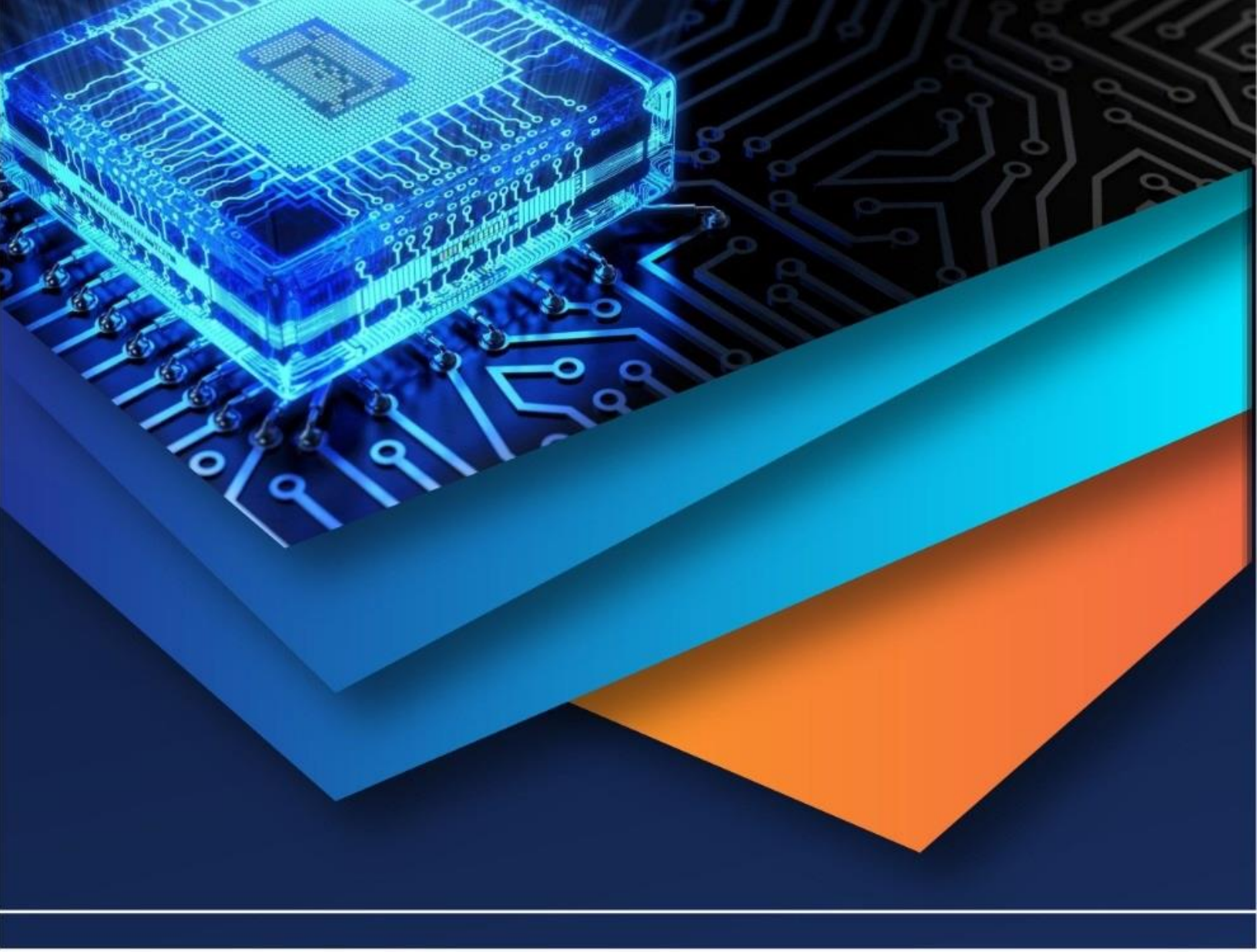
V. ACKNOWLEDGMENTS

We (authors) would like to thank faculty staff and mentors for guidance during the project.

REFERENCES

[1] M. Zanardelli, F. Guerrini, R. Leonardi, N. Adami, "Image forgery detection: a survey of recent deep- learning approaches," ACM Computing Surveys, vol. 56, no. 2, pp. 1–43, 2023.
[2] M.A. Anwar,A.Liz-Lopez,S.Bonomi,"Imageforgery detection by transforming local descriptors into deep- derivedfeatures,"AppliedSoftComputing,vol.138,pp. 110933, 2023.
[3] Z.J. Barad, R. Tewari, M. Tiwari, "Image Forgery Detection using Deep Learning: A Survey," in Proc. 2020 International Conference on Computing, Communication, and Intelligent Systems, pp. 225–231, 2020.
[4] K. Lee, H. Kumar, "Hybrid GAN-based data augmentation for image forgery detection," IEEE Access, vol. 12, pp. 42279–42292, 2024.
[5] B.Rahman,S.Parveen,M.S.Khan,"TransferLearning- basedLocalisationofImageForgeriesinSocialMedia," International Journal of Computer Vision and Image Processing, vol. 15, no. 3, pp. 99–113, 2022.
[6] D. Alves, A. Pinto, A. Ferreira, "Unsupervised deep anomaly detection for image tampering identification," Pattern Recognition Letters, vol. 180, pp. 88–97, 2025.
[7] M. Liz-Lopez, S. Bonomi, "Recent Advances in Image Forgery Detection and Localization," Journal of Imaging, vol. 10, no. 1, pp. 1–21, 2024.
[8] S. Gupta, S. Singh, "State-of-the-Art Techniques for Image Forgery Detection," International Journal of Engineering Research and Applications, vol. 15, no. 1,pp.106–120, 2025.
[9] Y. Hamed, F. Ibrahim, R. Adepoju, "Challenges and Future Directions in Image Forgery Detection for Fake News,"Computers,Materials&Continua,vol.74,no.2,pp.1234–1249,2023.
[10] J.Smith,F.Wang,"Afull-image,full-resolutionend-to- end trainable CNN framework for image forgery detection,"IEEEAccess,vol.8,pp.12260–12277,2020.
[11] A.Rehman,Z.Wang,"DigitalImageForgeryDetection and Localization Using Deep Learning Approaches," ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 18, no. 3s, pp. 1–22, 2022.
[12] L.Bondi,S.Lameri,D.Guera,P.Bestagini,E.J.Delp,S. Tubaro, "Tampering Detection and Localization through Clustering of Camera-based Image Patches," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3219–3231, 2020.
[13] P. Deb, S. Deb, A. Das, N. Kar, "Image Forgery Detection Techniques: Latest Trends and Key Challenges,"IEEEAccess,vol.12,pp.124578–124595, 2024.
[14] H. Farid, "Image Forgery Detection: A Survey," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 47–53,2020.

[15] R. C. Gonzalez, R. E. Woods, "Digital Image Processing," 4th Edition, Pearson, 2018.
[16] J. Cozzolino, G. Poggi, L. Verdoliva, "Splicebuster: A new blind image splicing detector," in Proc. IEEE International Workshop on Information Forensics and Security, pp. 1–6, 2015.
[17] H.Huang,W.Guo,Y.Zhang, "Detectionofcopy-move forgery in digital images based on DWT and SVD," in Proc. IEEE International Conference on Computer Science and Automation Engineering, pp. 423–427, 2021.
[18] A.C. Popescu, H. Farid,"Exposing Digital Forgeries by DetectingDuplicatedImageRegions,"TechnicalReport TR2004-515, Dartmouth College, 2004.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY