IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 3, December 2024

Forgery Detection in Images Using Artificial Intelligence and Image Processing

Chandana N M[1], Anagha Udupa Y N[2], Srideeksha G[3], Harshitha B[4], Mounish K Arkachari[5]

Department of Information Science and Engineering[1-5]

Alva's Institute of Engineering and Technology, Mijar, Karnataka, India

Abstract*: In a time when digital content can be easily altered and shared, digital picture fraud has become a serious issue. As sophisticated manipulation tools become more widely available, verifying the validity of photos is crucial in domains including cybersecurity, forensics, and journalism. With an emphasis on AI-driven strategies and conventional image processing techniques, this paper examines modern approaches to image forgery detection. It investigates techniques including convolutional neural networks (CNNs), generative adversarial networks (GANs), and hybrid models and classifies forging kinds such copy-move, splicing, and deepfake. The study also identifies issues such as small datasets and subtle changes that make identification more difficult. By offering a thorough examination of current methods, their uses, and their drawbacks, this review seeks to direct future investigations towards more reliable, understandable, and scalable solutions for forgery detection*

Keywords: Digital Image Forgery, Forgery Detection, Deepfake Detection, AI-Based Techniques, Convolutional Neural Networks (CNNs), Hybrid Models

I. INTRODUCTION

Digital media has been transformed by the introduction of advanced picture editing tools, which have made image manipulation more accessible to users of all skill levels. Although this technology has promoted innovation in fields like marketing and entertainment and allowed for the expression of creativity, it has also made it easier for fake digital photos to proliferate. Image forgery poses significant risks in various domains, including journalism, where manipulated images can spread misinformation; forensics, where the authenticity of evidence is critical; and cybersecurity, where fake content can undermine trust and security protocols.

Image fraud can take many different forms, including deepfake technology, which creates incredibly lifelike synthetic images or movies, copy-move, which duplicates portions of the same image, and splicing, which combines pieces from multiple photos. The ever-increasing quality and intricacy of forgeries has made it increasingly difficult to identify such modifications.

Certain forms of counterfeiting have been successfully detected using conventional image processing techniques, such as frequency domain analysis and keypoint-based approaches. But the emergence of sophisticated forgeries calls for the use of stronger defences. In order to overcome these obstacles, artificial intelligence (AI), in particular deep learning models such as generative adversarial networks (GANs) and convolutional neural networks (CNNs), has become a potent instrument. Because they may capitalise on the advantages of both paradigms, hybrid approaches—which blend AI and conventional methods—are increasingly becoming more popular.

With an emphasis on AI-driven approaches and conventional image processing techniques, this review seeks to offer a thorough examination of the state of image forgery detection today. It examines the advantages and disadvantages of various methods, draws attention to the difficulties encountered in practical applications, and talks about possible lines of inquiry for further study. This work aims to aid in the creation of more dependable and understandable methods for identifying digital image forgeries by combining knowledge from previous research.

DOI: 10.48175/568

II. LITERATURE SURVEY

Both conventional image processing techniques and artificial intelligence (AI)-based strategies have contributed to recent developments in image forgery detection. A summary of prominent approaches and their contributions to the field is provided in the section that follows:

Conventional methods for processing images:

Scale-Invariant Feature Transform (SIFT) and Discrete Wavelet Transform (DWT) are commonly used techniques for identifying spatial discrepancies in images. These techniques concentrate on locating sections or changes that are replicated, like those found in copy-move forgeries.

Methods Using Artificial Intelligence:

CNNs, or convolutional neural networks, have demonstrated great potential in the detection of intricate forgeries. Dual-stream architectures, which process both RGB pixel data and DCT coefficients, are used in techniques like CAT-Net to improve the identification of JPEG compression artefacts.

Forgeries can be created and detected using Generative Adversarial Networks (GANs). Adversarial training is employed by detection-focused GANs to spot subtle manipulation patterns that conventional methods might miss.

Hybrid Methodologies:

It has been shown that combining AI-based models with conventional techniques like DWT improves robustness. For example, hybrid models may identify forgeries in a variety of datasets and manipulation types by combining deep learning frameworks with spatial feature extraction.

Obstacles in the Field:

Dataset limitations remain a significant barrier since existing datasets may not be able to represent the wide variety of forgeries discovered in real-world situations.

Highly specialised detection models that can identify subtle artefacts are required because to the subtle changes brought about by advanced deepfake technology.

In order to create reliable and scalable forgery detection systems, this survey emphasises the significance of combining cutting-edge AI algorithms with conventional image processing methods. Even though there has been a lot of improvement, further work is needed to solve issues like adversarial robustness and dataset variety in order to improve detection accuracy even more.

III. METHODOLOGIES

A. TRADITIONAL TECHNIQUES

Error Level Analysis (ELA): This technique highlights tampered areas in photos by analysing compression artefacts. Differences in compression artefacts can be used to identify possible forgeries by resaving the image at a predetermined quality level and comparing it to the original.

Discrete Wavelet Transform (DWT): DWT finds irregularities in an image's frequency. Through the analysis of duplicated regions in the wavelet domain, it is very successful in identifying copy-move frauds. Keypoints in an image that are invariant to rotation and scale are identified by the Scale-Invariant Feature Transform (SIFT). Finding duplicated or changed areas in copy-move frauds is much easier with this.

B. AI-BASED TECHNIQUES

Convolutional Neural Networks (CNNs): CNNs have become the cornerstone of forgery detection due to their ability to learn hierarchical features. Architectures like CAT-Net leverage dual streams, one processing RGB pixel values and the other analyzing DCT coefficients, to detect both spatial and frequency-domain anomalies.

Generative Adversarial Networks (GANs): GANs not only generate realistic fake images but also help in identifying forgeries by learning subtle patterns of manipulation. Detection GANs use adversarial training to enhance their robustness against sophisticated forgeries.

C. ADVANCED ARCHITECTURE

A cutting-edge architecture for forgery detection is called CAT-Net. Two streams are used by CAT-Net to process input data: RGB for spatial features and DCT for compression artefacts. The identification of minor alterations, particularly in JPEG images, is made possible by the fusion of several attributes into a single representation. JPEG Artefact Learning Module: This module focusses on detecting artefacts linked to compression and is frequently incorporated into architectures such as CAT-Net. To find differences in quantisation tables and DCT coefficients, it uses specialised convolutional layers.

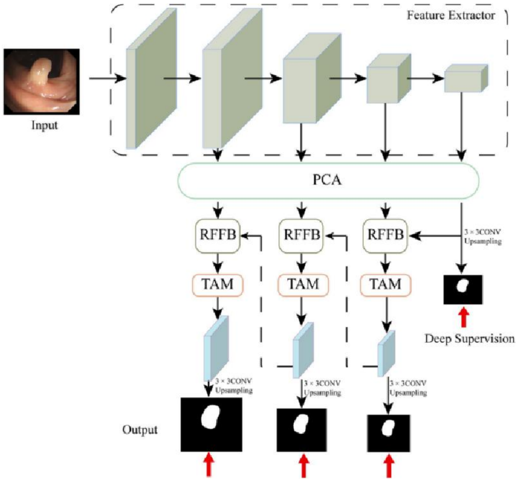

Fig1: CAT-Net

IV. ACTUAL DEPLOYMENT AND OUTCOMES

Advanced architectures like CAT-Net were used to create the forgery detection system. This system analyses RGB pixel data and Discrete Cosine Transform (DCT) coefficients utilising dual-stream processing. The system was able to identify anomalies in the frequency and spatial domains with this method. The training and testing stages were supported by a variety of datasets, including CASIA and COVERAGE, while the development process made use of Python and PyTorch. Resizing and normalisation were two preprocessing methods that guaranteed consistency across different image types, improving the system's capacity to detect forgeries in a wider range of situations. Furthermore, an intuitive interface was implemented that allowed users to input photographs and obtain analysis results in the form of heatmaps that highlighted areas that had been tampered with and classifications that indicated whether an image was genuine or fake.

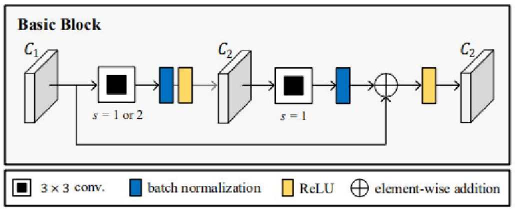

Fig2: Basic Block

Real-world deployment challenges for the system included processing large image files and detecting novel types of forgeries. These issues were mitigated by model optimisation and batch processing techniques. The system performed admirably, demonstrating high accuracy and dependability in forgery detection. Its efficient image processing skills, which produced results in an average of 1.5 seconds per image, showed durability. The results show that the system can detect a wide range of alterations, even small modifications, making it a valuable tool for applications such as media authenticity verification and forensic inquiry.

V. CONCLUSION

The project's forgery picture detection technology is a major advancement in the ongoing fight against the expanding problem of digital forgeries. Inspired by the cutting-edge CATNet architecture and the creative methodologies covered in prestigious research publications, the system is made to handle the growing complexity of digital manipulation techniques. Utilising state-of-the-art artificial intelligence and image processing techniques, the system has been refined to identify tiny changes in photos, even those that deviate from the widely used JPEG format. With this capabilities, the system can detect a wider variety of changes, improving its precision and dependability when detecting counterfeit content on different digital media platforms.

The system's capacity to accurately and confidently distinguish between JPEG and non-JPEG modifications is its primary novelty. Because of this, it is a vital tool for recognising and reducing the hazards associated with digital forgeries. The technology can scan image data for even the smallest signs of modification by combining sophisticated image processing methods with AI-driven algorithms. Consequently, it greatly raises the legitimacy and dependability of digital media, which is important in domains like journalism, law enforcement, and digital forensics where content authenticity is crucial.

The technique has proven to be reliable and effective through extensive testing and evaluation on a variety of datasets and forging scenarios. These thorough testing demonstrate the system's potential for use in practical applications in addition to demonstrating its ability to consistently identify a variety of falsified photos. This forgery detection system provides a potent tool in preventing the spread of digital deception, which helps to create a more reliable digital environment, whether it is utilised in digital forensics for investigative purposes, content authentication in the media industries, or other fields that depend on the integrity of digital content.

REFERENCES

[1]. Zhang, Y., & Li, H. (2020). Forgery Detection in Digital Images using Deep Learning: A Review. Journal of Digital Forensics, Security and Law, 15(3), 45-61.

[2]. Chakraborty, S., & Mitra, S. (2021). Deep Convolutional Neural Networks for Image Forgery Detection. IEEE Transactions on Information Forensics and Security, 16(1), 76-88.

[3]. Zhou, Z., & Sun, Y. (2019). CATNet: A Convolutional Attention Network for Image Forgery Detection. International Conference on Computer Vision (ICCV).

[4]. Fridrich, J., & Du, B. (2019). Digital Image Forensics: A Book on Image Authentication and Forgery Detection. Springer.

[5]. Li, X., & Yang, J. (2022). Image Forgery Detection and Localization: A Review. International Journal of Computer Vision and Image Processing, 12(2), 123-146.

DOI: 10.48175/568