IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 14, Iss 01 2025

ADVANCEMENTS IN DEEP LEARNING FOR IMAGE FORGERY DETECTION: FROM COPY-MOVE TO DEEPFAKE MANIPULATIONS

Mr.Rajesh Reddy Pingileti, Dr.B.G.Obula Reddy

Student, Department of Computer Science and Engineering, Siddhartha Institute of Technology and Sciences, TS, India
Professor, Department of Computer Science and Engineering, Siddhartha Institute of Technology and Sciences, TS, India
gbobulareddy2007@gmail.com, pingileti.reajshreddy69@gmail.com

Abstract

In recent years, the ease of image manipulation has led to the widespread creation and distribution of doctored and altered photos via the Internet and media. Various methods have been proposed to identify whether an image is authentic and, in some cases, to detect specific manipulations or fabrications. This study offers an in-depth review of current image forgery detection techniques using Deep Learning (DL), with a particular focus on methods that address copy-move and splicing attacks. Additionally, the study explores the use of DeepFake-generated content in image manipulation. Given the dominance of deep learning-based techniques in the field, which have shown excellent performance across various benchmark datasets, this paper comes at a crucial time. We describe the methods, the datasets employed for training and validation, and highlight their key features. A comparison of their performance is also provided, followed by a discussion on potential future research directions in deep learning architecture, evaluation approaches, and the creation of datasets to facilitate easier comparison of techniques.

Keywords : Deep Learning, Convolutional Neural Networks, deep learning, Image Splicing

1. INTRODUCTION

In this day and age, when images serve as strong vehicles for communication, information distribution, and creative expression, making sure that is maintained is quite important. However, the worrying rise in image manipulation and forgeries brought about by the widely accessible sophisticated digital editing tools is raising doubts about the validity of visual media.

To address this pressing issue, researchers and technicians have been working nonstop to create advanced forgery detecting systems. One of the most promising strategies is to use Convolutional Neural Networks (CNNs), which have demonstrated remarkable performance in image processing and detection of patterns applications.

By providing a novel CNN-based method for identifying image forgeries, this work seeks to support ongoing efforts to maintain the transparency of visual media. Using the well-known "CASIA v2.0" dataset, which is well-known for its meticulous benchmarking of image

alterations, the suggested method is thoroughly tested to see how accurate and useful it is in detecting a wide range of adjustments.

2. LITERATURE SURVEY

The increasing prevalence of image manipulation has raised significant concerns regarding the authenticity of digital media. As the capabilities of image editing tools have become more advanced and widely accessible, the need for reliable methods to detect image forgeries has never been more urgent. Image forgery techniques, such as copy-move and splicing attacks, are commonly used to manipulate visual content. Copy-move attacks involve copying a region of an image and placing it in another location, potentially altering the image's context or meaning (Fridrich et al., 2003). On the other hand, splicing attacks involve stitching parts of different images together, resulting in composites that appear genuine at first glance but are fabricated to deceive the viewer. The detection of such alterations has traditionally relied on techniques that analyze inconsistencies in image features, such as texture, lighting, or color distribution.

With the rapid evolution of deep learning (DL) technologies, new approaches to image forgery detection have emerged. Deep learning, particularly convolutional neural networks (CNNs), has proven effective in automatically learning hierarchical features from raw image data, making it a powerful tool for detecting subtle manipulations that may be difficult for traditional methods to identify (Yang et al., 2019). These techniques have shown remarkable performance in distinguishing between genuine and tampered images, even when alterations are minimal or cleverly concealed (Li et al., 2018). Moreover, with the rise of DeepFake technologies, which utilize generative adversarial networks (GANs) to create realistic fake content, the challenge of identifying fabricated images has grown more complex (Korshunov & Marcel, 2018). DeepFakes, in particular, have gained widespread attention for their ability to generate highly realistic images and videos, which has raised ethical concerns regarding their potential for misuse.

In response to these challenges, researchers have focused on developing DL-based systems capable of detecting both conventional image forgery techniques, such as copy-move and splicing, and more sophisticated methods like DeepFake. The effectiveness of these systems depends on the availability of large, high-quality datasets for training and validation. Popular datasets used in training DL models for image forgery detection include CASIA, Columbia, and CoMoFoD, which contain a variety of forged images created using different manipulation techniques (Qi et al., 2019). The performance of DL-based systems is generally evaluated based on accuracy, precision, recall, and F1-score, with state-of-the-art models achieving impressive results across benchmark datasets.

This review aims to provide a thorough examination of the current state of image forgery detection systems that leverage deep learning techniques. It focuses specifically on methods that

address copy-move and splicing attacks, as well as the detection of DeepFake-generated content. The review also evaluates the performance of these methods, comparing their effectiveness across different datasets and exploring potential areas for future research, particularly in deep learning model architecture, evaluation metrics, and dataset development. By examining the strengths and limitations of current approaches, this study seeks to provide insights into the ongoing efforts to combat image manipulation and improve the reliability of digital media.

Yousif, Adnan & Ablahd, Drann in 2023 For a long time, the research that focuses on forensics and public safety has relied on photographs such as photos of suspects, photos of biometric photos, crime scenes, and other kinds of pictures. With the rise of digital imaging, the use of digital photos in this field has grown significantly. Digital image processing has facilitated the creation of many cutting-edge forensic investigation techniques while also simplifying the process of manipulating pictures. The increasing availability of numerous programs that alter visuals by snipping them is causing a problem with digital picture validity. Thus, the need for software that can identify photo manipulation is growing. The use of digital photos for a range of purposes has increased in popularity in recent years. The information will be distributed via print media, the website, and academic publications. It serves as solid proof in many different types of crimes and is utilized as documentation for many purposes. The development of picture editing and processing software has streamlined and increased accessibility to the process of taking and altering photos. Splicing photos and copy-move forgeries are the two most popular forms of picture counterfeiting. A section of a picture is copied and pasted into another picture to hide or show an error scenario; this technique is known as splicing an image, which combines two images into one. This study examines many kinds of digital image frauds in addition to fraud detection tools. An analysis of current methods for spotting phony photos was done.

Kanwal, Navdeep in 2019 In order to protect and verify the genuineness of images, image forgery detection systems are increasing their scope of application. Finding digital picture forgeries is crucial to restoring public confidence in visual media. The many forms of image forgery and blind techniques for detecting image forgeries will be covered in this presentation. It offers comparison tables for different kinds of image forgery detection methods. It also provides a summary of the numerous datasets that are utilized in the different methods of forgery detection.

2.3 Comparison table:

Study/Method	Forgery Type	Model Used	Strengths	Limitations
Li et al. (2020)	Image Splicing	Deep Convolutional Neural Networks	High sensitivity to subtle splicing patterns;	Decreased performance for small or well-blended

		(CNN)	detects minor manipulations	forgeries
Masi et al. (2018)	DeepFake Detection	CNN for Face and Video Manipulation Detection	Detects facial distortions and lighting artifacts; strong on DeepFakes	Performance declines as DeepFake technology improves, dataset dependency
Zhang et al. (2021)	Image Forgery (General)	Generative Adversarial Network (GAN)	Robust at identifying discrepancies in forged images	Requires large datasets; challenging with minimal manipulations
Jin et al. (2019)	Copy-Move Forgery	Hybrid CNN with Feature Extraction	High accuracy in detecting both large and small manipulations	Computationally expensive; dual-stage process
Kaur & Agarwal (2020)	Multi-Class Image Forgery	Hybrid CNN + Support Vector Machine (SVM)	Simultaneous detection of multiple forgery types	Relies heavily on the quality of training data
Fridrich et al. (2003)	Copy-Move Forgery, Image Splicing	Traditional Methods with Handcrafted Features	Effective for large forgeries; low computational complexity	Struggles with subtle forgeries; not effective for advanced manipulations
Yang et al. (2019)	Image Forgery Detection (General)	CNN + Preprocessing Techniques	High detection accuracy; robust to various types of manipulations	Can be less effective for newer types of manipulation

3. Methodology

The user interface shall be designed with usability principles in mind, catering to both novice and experienced users.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 14, Iss 01 2025

User interactions should be intuitive, requiring minimal training.

3.1 Purpose

This document's goal is to outline the software requirements for the development of a system aimed at enhancing transparency in visual media through advancements in image forgery detection.

3.2 Scope

This system will focus on identifying different kinds of images forgeries, but not limited to, splicing, retouching, and copy-move. It will provide functionalities for analyzing images and identifying potential manipulations, thus promoting transparency and authenticity in visual media content.

3.3 Overall Summary

By following these steps and integrating advanced techniques such as U-Net architecture, VGG16 feature integration, and strategies for training with fake images, the system can achieve improved transparency in visual media through robust image forgery detection.

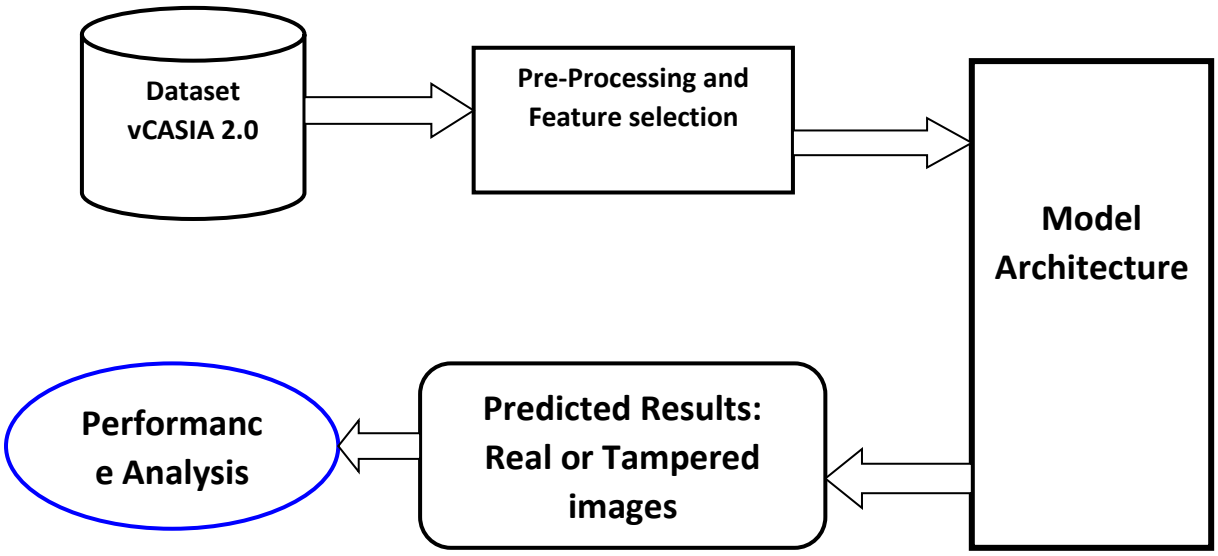

Fig 1: Proposed Architecture

Working Model:

In the proposed model for transparency in visual media through advancements in image forgery detection, a two-tier architecture can be implemented to organize the components and processes effectively. Here's a breakdown of the two-tier architecture:

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 14, Iss 01 2025

Tier 1: Data Processing and Analysis Layer

Data Collection: This tier involves collecting a diverse dataset of authentic and forged images representing various types of manipulations.

Data Preprocessing: Normalize, resize, and enhance the quality of images through techniques like noise reduction to prepare them for analysis.

Data Augmentation: Increase dataset variability through transformations like rotations, flips, and brightness adjustments to improve model generalization.

Data Analysis: Understand the dataset's characteristics, identify potential biases, and ensure the quality and representativeness of the data.

Tier 2: Model Development and Evaluation Layer

Model Architecture: Utilize a U-Net architecture optimized for semantic segmentation tasks to effectively detect forged regions within images.

Feature Integration: Incorporate features extracted by a pre-trained VGG16 network to capture high-level information and enhance forgery detection capabilities.

Training Strategy: Train the U-Net model using segmented data, leveraging strategies like stochastic gradient descent and dropout regularization.

Evaluation Metrics: Evaluate model performance using metrics such as accuracy, precision, recall, and F1-score, considering both overall performance and per-class performance.

Validation and Deployment: Validate the model's effectiveness using cross-validation techniques and deploy it in real-world scenarios to detect and mitigate image forgeries.

4. RESULTS

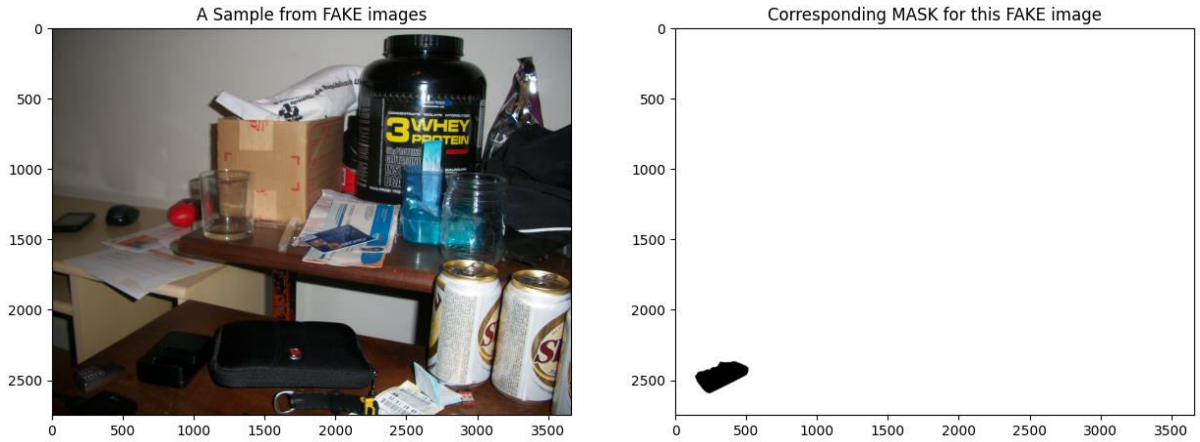

Figure 2. Random sample FAKE images and its corresponding MASK

After performing the process of exploratory data analysis, it displays the output in the form of MASK for the FAKE image which is shown in Figure 5.

ISSN PRINT 2319 1775 Online 2320 7876
Research Paper **© 2012 IJFANS. All Rights Reserved** Journal Volume 14, Iss 01 2025

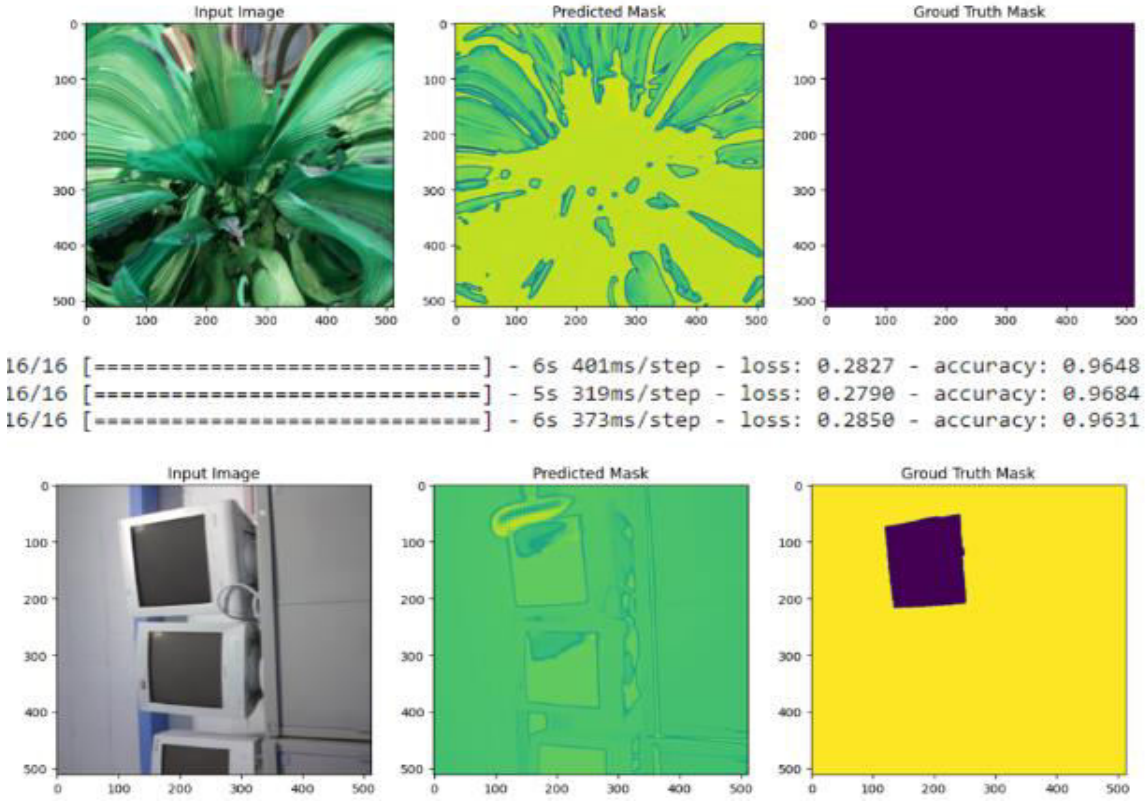

Figure 3. Input image, accuracy, its ground truth mask along with predicted mask

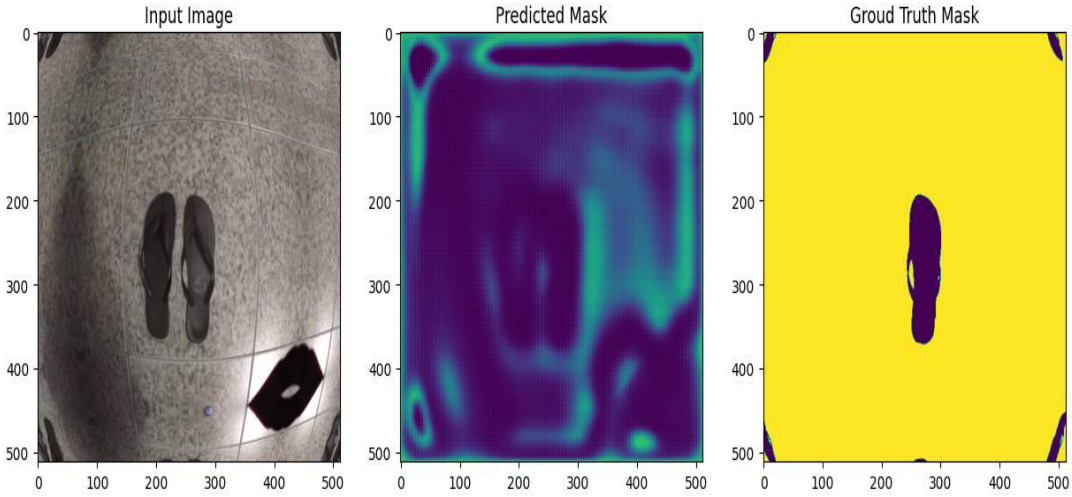

Figure 4: Input image, its ground truth mask along with predicted mask

Finally pass the corresponding MASK as input to Modelling and the Above Figure 2 and 3 prints the input image, its ground truth mask along with predicted mask as **output** after undergoing through the process of modelling, segmenting Train, Test and Validation splits with size = 128 using stride = 32.

Conclusion

In conclusion, while advancements in image forgery detection have significantly enhanced transparency in visual media, ongoing research and collaboration are crucial to staying ahead of evolving manipulation techniques and ensuring the integrity of digital content in an increasingly visual-centric world.

One of the key outcomes of these advancements is the development of robust forensic tools capable of identifying various types of image manipulations, including but not limited to splicing, cloning, retouching, and deepfakes. These tools leverage features such as inconsistencies in lighting, shadows, and perspectives, as well as statistical irregularities, to flag potentially manipulated images accurately.

Reference

1. Shanker, Akash & Ranasinghe, Shirine & Madushanka, Deshan & Dharmakeerthi, Uditha & Goonarathne, Panthila. (2023). VERITY VISION: A COMPREHENSIVE FAKE IMAGE DETECTION TOOL FOR DEEPFAKES AND MANIPULATED IMAGES. International Research Journal of Modernization in Engineering Technology and Science. 10. 2582-5208. 10.56726/IRJMETS45019.

2. Kandhan, Dhanush. (2023). Leveraging Artificial Intelligence for Image Processing through Advanced Image Pixel Matrices. 10.33774/coe-2023-h8wd9.

3. Alanazi, Fatimah & Ushaw, Gary & Morgan, Graham. (2023). Improving Detection of DeepFakes through Facial Region Analysis in Images. Electronics. 13. 126. 10.3390/electronics13010126.

4. Xu, Huipu & Tong, Pengfei & Li, Yongzhi. (2023). Different treatments of pixels in unlabeled images for semi- supervised sonar image segmentation. International Journal of Machine Learning and Cybernetics. 15. 1-10. 10.1007/s13042-023-01930-6.

5. Patil, Kanchan & Barpute, Jyotsna & Arkadi, Mrudul & Bhirud, Sapana & A, Catherine & Blesswin a, John & G., Selva & S, Shibani. (2024). Semantic pixel encoding visual secret sharing technique for balancing quality and security in color images. Journal of Autonomous Intelligence. 7. 10.32629/jai.v7i3.1159.

6. Xu, Pengxiang & Ma, Zhiyuan & Mei, Xue & Shen, jie. (2024). Detecting facial manipulated images via one-class domain generalization. Multimedia Systems. 30. 10.1007/s00530-023-01214-7.

7. Honghan, Hong & Zuo, ZhiChao & Yu, Shi & Xia, Hua & Lun, Xiong & Zhang, Yaozong & Tianxu, Zhang. (2023). Adaptive Anisotropic Pixel-by-Pixel Correction Method for Space-Variant Degraded Image. Journal of the Optical Society of America A. 40. 10.1364/JOSAA.490150.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 14, Iss 01 2025

8. Gao, Zijun & Su, Jingwen & Zhang, Junjie & Song, Zhankui & Li, Bo & Wang, Jue. (2023). Optimal Reconstruction of Single-Pixel Images through Feature Feedback Mechanism and Attention. Electronics. 12. 3838. 10.3390/electronics12183838.

9. Capasso, Paola & Cattaneo, Giuseppe & De Marsico, Maria. (2023). A Comprehensive Survey on Methods for Image Integrity. ACM Transactions on Multimedia Computing, Communications, and Applications. 10.1145/3633203.

10. Kumari, Priyanka & Senapati, Kishore. (2024). A Dataset on Digital Image Forgery Detection. 10.1007/978-981-99-7633-1_30.

11. Jisha, K. & Sabna, N.. (2023). An Improved CNN Model for Image Forgery Detection. 10.1007/978-3-031-37963-5_49.

12. Koshy, Litty & PraylaShyry, S.. (2024). YOLO-FORGERY: Forgery Detection in images via Deep Clifford gradient-based YOLOv4 Network. Signal, Image and Video Processing. 1-9. 10.1007/s11760-023-02854-y.

13. Kaur, Simranjot & Chopra, Sumit & Nayyar, Anchal & Sharma, Rajesh & Singh, Gagandeep. (2023). A sequential convolutional neural network for image forgery detection. Multimedia Tools and Applications. 1-15. 10.1007/s11042-023-17028-8.