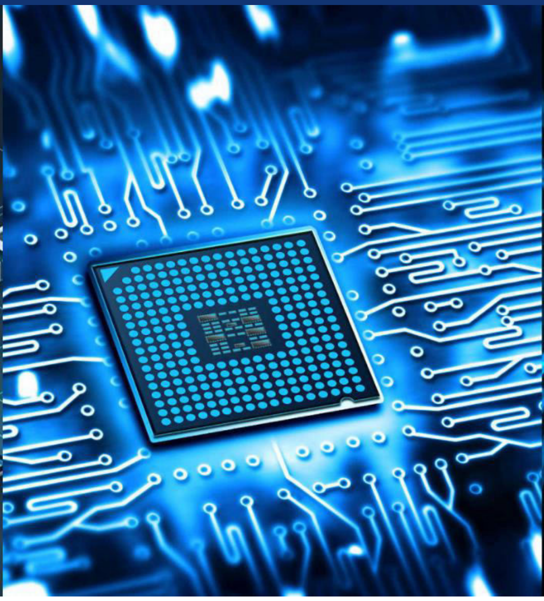
IJIRCCE

ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.625

Volume 13, Issue 1, January 2025

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Deep Copy Net: Copy-Move Forgery Detection Using Hierarchical U-Net and Densely Connected Convolutional Features

Ajay Prakash B V[1], Kushal M V[2], Aditya G[3], Chirag J[4], Shreyas DC[5], Yash SK[6]

Professor and Head, Dept. of AIML, Dr. Ambedkar Institute of Technology, Karnataka, India[1]

Assistant Professor, Dept. of AIML, Dr. Ambedkar Institute of Technology, Karnataka, India[2]

UG Student, Dept. of ISE, Dr. Ambedkar Institute of Technology, Karnataka, India[3,4,5,6]

ABSTRACT: This paper introduces a method employing Convolutional Neural Networks (CNNs) and U-Net to identify manipulated areas within digital images, aiming to address growing concerns regarding image authenticity. Leveraging CNNs' capability to extract complex features from images, the model learns distinctive patterns encompassing both local and global characteristics indicative of tampering. A diverse dataset comprising various forgery types (e.g., copy-move and splicing) is utilized to train and assess the CNN model's performance. Enhancing the model's resilience, pre-processing techniques like noise reduction, resizing, and augmentation are implemented. To prevent overfitting and boost generalization, novel loss functions and regularization techniques are integrated. The experimental analysis showcases the CNN and U-Net model's proficiency in accurately identifying manipulated regions across different types of manipulations, exhibiting high precision and recall rates. These results highlight the model's potential for practical use in image forensics, contributing significantly to preserving content integrity in an era marked by rampant digital alterations.

KEYWORDS: CNN -Convolutional Neural Network ,GAN -Generative Adversarial Network, CMFD- Copy-Move Forgery Detection, SVM- Support Vector Machine, PiL- Pillow SRM Steganalysis Rich Model

I. INTRODUCTION

Detecting manipulations in digital images has become a critical concern due to the increasing sophistication of editing tools that challenge the reliability and authenticity of visual content. This project focuses on the implementation of a Convolutional Neural Network (CNN) based method to identify and locate manipulated regions within digital images accurately. Due to the easy accessibility of image and video editing software, various forms of manipulations, such as copy-move, splicing, and retouching have emerged, posing threats to maintaining the credibility of visual content. Convolutional Neural Network (CNN) offers promise in this regard due to its ability to learn complex patterns and features, resulting in it being a good solution for detecting image forgeries. In order to improve the performance of the CNN model various preprocessing techniques are employed. These techniques include reducing noise, resizing images and using augmentation methods. Additionally innovative approaches such, as incorporating loss functions and regularization techniques are implemented to prevent overfitting and enhance the model’s adaptability. The main objective of this project is to contribute to the advancement of image forensics by introducing a methodology based on CNNs. This methodology aims to detect and locate forged regions within images. By doing it seeks to strengthen trust and credibility in media by safeguarding against falsified or misleading visual content. Through the use of techniques this project aims to address the challenges posed by image manipulation and provide a solution for ensuring the integrity and authenticity of visual information.

The process of alterting images by transmitting of false digital information is known to be image forgery and subset of image processing.The rapid growth of technology is becoming a threat for the growth of concern of maintaining the original(pristine) (see figure1) and image forgeried (see figure2).So,it’s a very societal step taken for the well being purpose of the people and society.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This is a step which we need to take as a group and as an individual so that it becomes successful. Image forgery detection, despite significant advancements, faces numerous problems and challenges due to the rapidly evolving techniques in image manipulation and the diverse application scenarios.

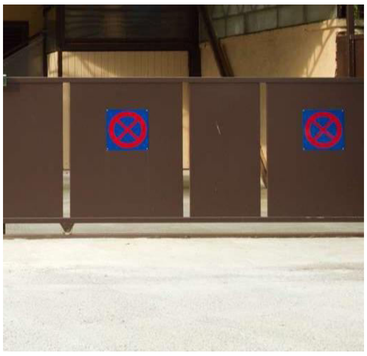


Figure1: Original Image

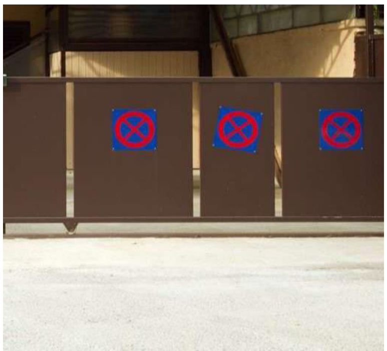


Figure2: Forgery Image

These challenges can be broadly categorized into the following:
Generative Models (e.g., GANs): Modern generative models can produce highly realistic fake images that are extremely difficult to distinguish from authentic ones. GAN-generated content often lacks visible artifacts, challenging traditional and even some deep learning-based methods.

- DeepFake Detection: Detecting manipulated videos and images created using DeepFake technology remains a significant hurdle, with detection accuracies often lagging behind other types of forgeries.
- Bias and Representation: Many datasets are biased, either towards specific types of manipulations or certain image categories, which affects the generalizability of detection models.
- Quality and Diversity: Variations in image resolution, compression, and noise levels within datasets make it challenging to train robust models.
- Scarcity of Standardized Datasets: The lack of widely accepted benchmark datasets with diverse and high-quality manipulations limits comprehensive evaluation and comparison of detection algorithms.
- Adversarial Attacks: Sophisticated attackers may intentionally craft images to fool detection systems, exploiting vulnerabilities in algorithms.
- Minimal Edits: Subtle alterations, like retouching or small-scale splicing, can bypass many detection systems, especially those reliant on large-scale statistical inconsistencies.
- Multiple Manipulations: Combining multiple forgery techniques (e.g., splicing with retouching) complicates detection and feature extraction.
- Semantic Manipulations: Some alterations change the meaning of the image without leaving detectable traces, making detection harder.
- Speed and Scalability: Real-time detection for high-resolution images or videos requires significant computational resources and optimization, which can be challenging in practical applications.

II. RELATED WORK

The study of image forgery detection spans a wide range of techniques, from traditional forensic approaches to modern deep learning methods. Traditional methods rely on analyzing statistical inconsistencies, noise variations, and compression artifacts, which are passive techniques, while active methods involve mechanisms like digital signatures, watermarking, and cryptographic tools. Understanding manipulation techniques such as copy-move forgery, splicing, and retouching is essential for developing reliable detection algorithms. the literature on image forgery detection is diverse, spanning traditional forensics techniques to cutting-edge deep learning methods the documentation and license of dataset are available in kaggle and comofod website[1].

A Deep Learning based approach to detect image forgery is presented by N. P. Nethravathi et al [2] .In particular, it compares performances of CNNs along with pre-trained model in detail. Deep learning techniques in image forgery as CNN model gives 99.87% accuracy and correct detection of invisible images is 99%. However, the VGG-16 gives only an accuracy of 97.93%, and a validation rate of 75.87%. M. Zanardelli et al. [3]. scrutinized modern methods for detecting image manipulation, specifically in identifying copy- move, splicing, and DeepFake alterations. A detection method showcased exceptional performance by nearly perfect accuracy across standard datasets for identifying copied regions and their original sources. Splicing detection achieved an accuracy of 85% on the CASIA2 dataset, accurately pinpointing forged regions. However, in DeepFake detection, no single method emerged as dominant across benchmark datasets, with accuracies averaging around 65%. An innovative method for detecting image forgeries using Convolutional Neural Network (CNN) was introduced by SS. Ali et al. [4]. This approach focuses on identifying tampering by exploiting the differences in image compression between original and altered segments. By analyzing the variations in recompressed images, the model distinguishes manipulated areas from genuine ones, effectively detecting both copy-move and splicing types of image tampering. Extensive evaluation on the CASIA2 [26] image forgery database showcases the effectiveness of the proposed CNN-based technique. Portrayal of prevalent forms of image forgeries like retouching, copy-move forgery, and image splicing facilitated by easily accessible editing software is shown by J. Ega et al. [5]. in this research. Through vivid examples, it illuminates these forgery types, underlining their extensive presence and implications in societal platforms and media. The study further highlights the pervasive use of fake images for malicious intent, including political manipulation and false representation, underscoring their relevance in contemporary society. This limitation could impact its applicability in the swiftly advancing landscape of digital forensics.

N. K. Rathore et al. [6] makes use of the Improved Relevance Vector Machine (IRVM), for detecting image forgery, specifically focusing on Copy-Move Forgery Detection (CMFD). The study addresses the challenges prevalent in existing methods related to feature extraction, computational time, and accuracy. This investigation must cover various types of image manipulations and ensure efficiency, especially when dealing with large datasets. Prevalent forms of manipulation like copy-move, resampling, splicing, and JPEG compression, all capable of altering or concealing information in satellite images are introduced by A. Kuznetsov [7]. To tackle the challenge of splicing, the study employs convolutional neural networks (CNNs), specifically a VGG-16-inspired architecture. With convolutional and fully connected layers, augmented by dropout layers to mitigate overfitting, the proposed CNN architecture demonstrates robustness in detecting distortions, achieving an impressive accuracy of 97.8% (for fine-tuned) and 96.4% (for zero-stage trained) on the CASIA dataset, surpassing existing methods. Sabeena and Dr. Lizy Abraham[8] they both have conducted a significant research focusing on methods to analyse and identify tampered images. C. D. Kaur and N. Kanwal [9] implementations on gradcam for mask creation to enhance the establishment of datasets. M. D. Ansari, S. P. Ghrera, and V. Tyagi [10] has determined various procedures for the classification based on forgery score.

III. METHODOLOGY

Data Exploration :Phase 1

Begin by importing fundamental Python libraries for tasks such as data exploration, manipulation, and model development. Within the dataset, there are three distinct folders: Tp: This directory comprises of tampered images. To initiate the analysis, the main focus will be on fake images housed in the 'Tp' folder. As this directory also contains miscellaneous files, only those files with the extensions '.jpg' or '.png' will be specifically read and considered There are a total of 8000 fake images in the dataset as s, each associated with a corresponding mask image stored in the 'CASIA 2' folder, indicating the tampered regions. However, it’s important to note that this mask information is not needed in the phase 1.

Data Preprocessing:

The approach involves conducting an error level analysis on the input image and feeding the resulting a simple convolutional neural network (CNN) trained to discern between fake and authentic images.Using Grad-cam for evaluation of mask and finding error level analysis is a method for detecting manipulated images by capturing them at a specific quality level and subsequently calculating the variation from the compression level. When an image is initially saved as a JPEG, it undergoes compression. Most editing software, such as Adobe Photoshop, GIMP, and Adobe

Lightroom, supports JPEG compression operations. If the image is then modified using editing software, it is compressed once again.

Data Exploration :Phase 2

Importing essential libraries for data manipulation and constructing a deep learning model. In this context, manipulated images will be exclusively utilized, and for these corresponding masks are provided. These masks delineate the specific regions within the images that have undergone tampering. So essentially, the process involves reading each file individually and extracting the image path, assigning a label (in case, "fake"), and creating an image ID. For every manipulated image, there is a corresponding mask image (see figure3). Iterations will be run through the CASIA 2 folder in the dataset , which contains all the mask images.

Data Preprocessing:

In the image forgery detection process, a crucial step involves modifying the mask image to distinguish between tampered and non- tampered regions. This modification is achieved by representing the tampered region as black and the non-tampered region as white. Initially, the mask image contained pixel values ranging from 0 to 255. To ensure compatibility with the sigmoid activation function used in the output layer of the model, these values are scaled down to either 0 or 1. Specifically, all pixel values that were originally 255 (representing white) are converted to 0.0 (black), while pixel values that are not equal to 255 are converted to 1.0 (white). This transformation allows the model to interpret the mask image accurately and make informed decisions regarding the authenticity of the input image. The scaling of pixel values in the mask image is critical for the proper functioning of the model's output layer. The sigmoid activation function, commonly used in binary classification tasks, expects input values to be within a certain range.

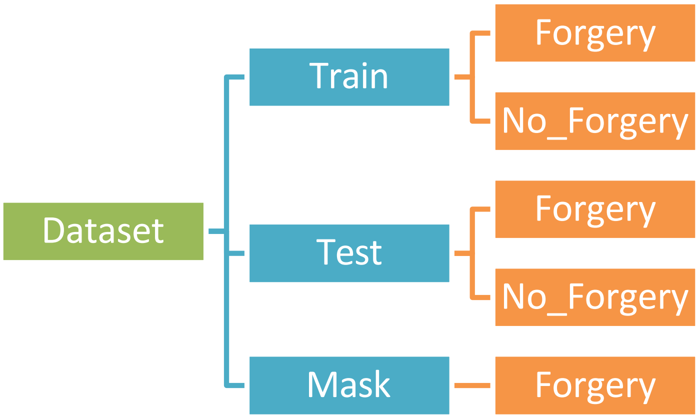


Figure3: Dataset Folder Structure

Architecture:

Currently, CASIA1, CASIA2 and CoMoFoD datasets are being utilized, both of these datasets are available on Kaggle for the project. The task is divided into two phases. Initially, the goal is to classify images as either real or fake, constituting a classification problem. Subsequently, in the second phase, the aim is to predict the tampered regions within the images, resembling a Binary-Image Segmentation problem. While there is no strict latency requirement for immediate results, it is essential that the model does not take an excessive amount of time to determine both the authenticity of the image and identify the tampered regions.

The Convolutional Neural Network (CNN) model used in this study is based on the datasets, a well-known benchmark dataset in the field of image manipulation detection (see figure4). The dataset contains a vast collection of both original and altered photos, making it ideal for training and testing the model's performance. Before feeding the images into the CNN model, numerous preprocessing processes are used to improve the data's quality and compatibility. Image Resizing: The images in the CASIA 1, 2 and CoMoFoD dataset vary in size, which can impair the model's performance. To remedy this, all photos are downsized to a common size (e.g., 256x256 pixels) using interpolation techniques that maintain the aspect ratio. Feature Selection: In addition to scaling, various feature selection techniques can be used to extract useful information from photos. This can include approaches like histogram equalization, which increases image contrast and allows the model to recognize minor variations.

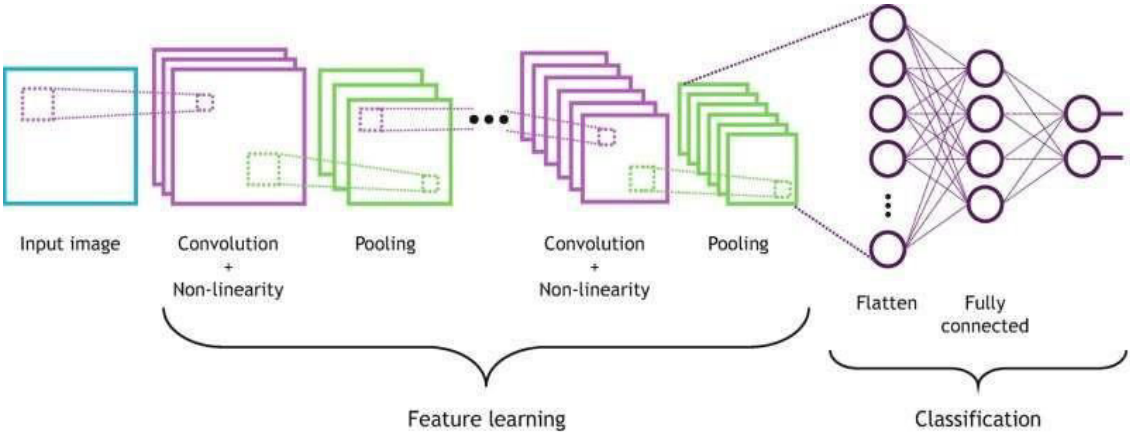


Figure4: Proposed CNN Architecture [11]

The U-Net architecture is a symmetric encoder-decoder deep learning network for picture segmentation. Convolutional and max- pooling layers are used by the encoder to extract features and shrink the image size , while upsampling and skip connections are used by the decoder to restore the image size while maintaining special details. The segmentation map is created by a final 1x1 convolution after a bottleneck layer catches the most abstract features (see figure5). U-Net is perfect for jobs like medical imaging, satellite mapping, and fraud detection because of its capacity to blend small features with global context. In this research paper the U-Net architecture is used along with CNN model to get a hybrid model which provides more efficient and optimistic accuracy. This architecture is extensively used in mask generation. The masked data is used to train the U-Net architecture with a batch size of 4. This makes the mask generation more accurate.

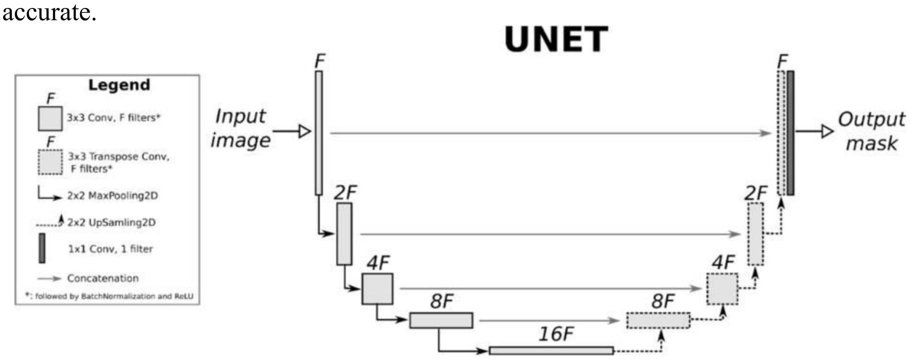


Figure5: Proposed U-Net Architecture [12]

IV. EXPERIMENTAL PROTOCOL

IMAGE SEGMENTATION:

- CNN: It's used in training the data and in that it is used for transforming the image. Along with training in CNN we produce binary classification as forgery or no forgery. This classification is based upon testing the saved CNN module weights upon an image which gives a score of forgery which is further binary classified[0,1].
- Modified CNN: It is fine tuned for our dataset Casia-1,Casia-2 and CoMoFoD and no limitations and drawbacks are carried forward by tuning crystal clearly.
- CNN+U-Net hybrid model: U-Net architecture is used to generate mask of the image where mask determines the forgery area based upon the percentage of masking the output mask is normalized and the forgery score is determined using the output mask value. This fogery score is used to classify images forgery or no forgery.

Development and Requirements

Since, it is a CNN it requires a heavy computational power to train the model and with the use of more and more big dataset consisting of more images there is a need for a heavy GPU enabled machine to train it efficiently and faster. Ensuring that the models generalize well to unseen data and can detect a wide range of image manipulations effectively can be challenging. Detecting complex manipulations such as splicing and retouching can difficult to identify (see figure6). Handling noise and distortion in images can affect the model's ability to detect forgeries accurately .

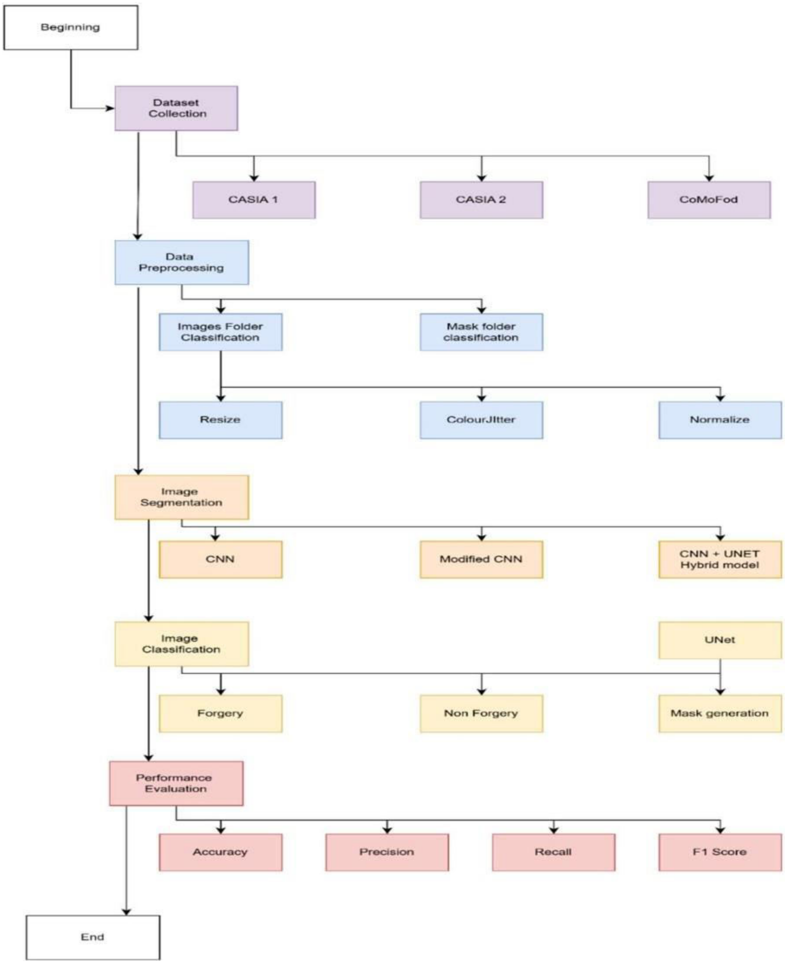


Figure 6: Workflow Diagram

SOFTWARE REQUIREMENTS:

The project has the following software requirements – Programming Language: Python 2.9 or Higher Integrated Development Environment (IDE): Visual Studio Code (VS Code), Jupyter Notebook CUDA 12.6 3.1.2

HARDWARE REQUIREMENTS:

The project has the following hardware requirements – Random Access Memory (RAM): 8 GB or Higher CPU Requirements: 2.5 GHz Operating System: Windows 10 pro GPU: Intel Arc B-Series GPUs 3.1.3

LIBRARY REQUIREMENTS:

- Numpy – Numpy is a fundamental library for numerical computations and handling array operations, especially in image processing tasks.
- OpenCV – It is used for image processing tasks like filtering and resizing images.
- Streamlit – It is used to create the web application interface for uploading images and displaying the results of the forgery detection model.
- Pytorch – Pytorch is utilized for deep learning tasks.
- Matplotlib – It is used to visualize images, ELA results, and performance graphs during model training.
- PiL (Pillow) – It is Employed for image processing tasks like ELA, image manipulation

V. RESULTS

The combination of both models produced an image forgery detection system capable of identifying two different types of image modifications with high accuracy. The splicing forgery detection model, which used a Dual-Stream UNet architecture with SRM filters, along with copy-move forgery detection model which used CNN will be validated after successful training of both the models in order to see how they are performing on the testing dataset. Training and validation loss and accuracy graphs: Continual decrease in training loss and initial decrease of validation loss but then gradual increase is a sign of overfitting. The validation accuracy starts to decrease while the training accuracy continues to increase which is also a sign of overfitting. The prediction accuracy and mask accuracy obtained from the proposed hybrid model is shown in table 1. It gives accuracy around 90.00% which is trained with the help of CNN architecture and with the help of masking and use of Grad-Cam the result will be enhanced and comofod databases are also used for it. Figure 7(a) and 7(b) shows the tampered images and 7(d) shows the authentic image

Table 1: Representation of Overall details of datasets

Dataset	Forgery images	No forgery images	Mask	Prediction accuracy	Mask accuracy
CASIA 1	800	807	807	51.48%	82.31%
CASIA 2	7492	4981	4981	52.01%	81.09%
CoMoFoD	200	200	200	55.58%	94.28%

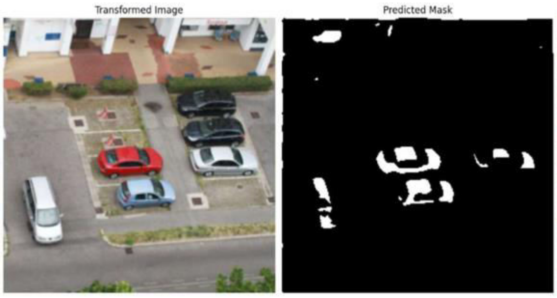


Figure 7.a Tampered Image

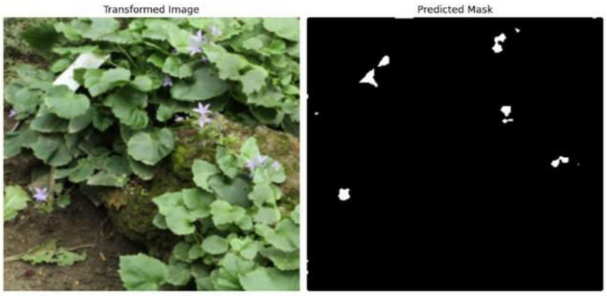


Figure 7.b Tampered Image

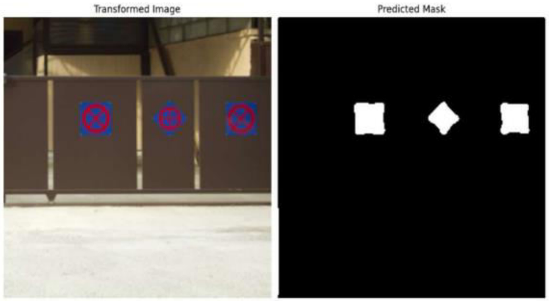


Figure 7.c Tampered Image

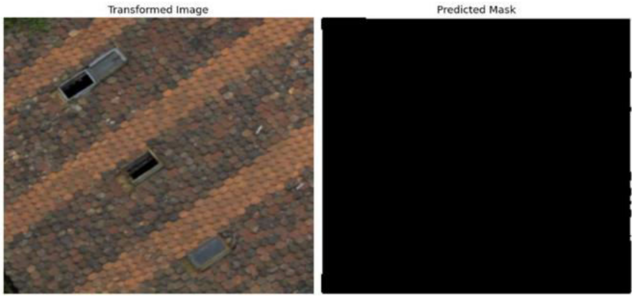


Figure 7.d Authentic Image

1. CASIA 1 evaluation metrics:

Table 2: Performance comparison for cassia 1 dataset

	accuracy	precision	recall	F1
CNN	49.86%	0.4356	0.4758	0.4548
Optimised CNN	51.48%	0.4985	0.5213	0.5096
CNN + UNet (hybrid model)	82.31%	0.8045	0.8235	0.8139

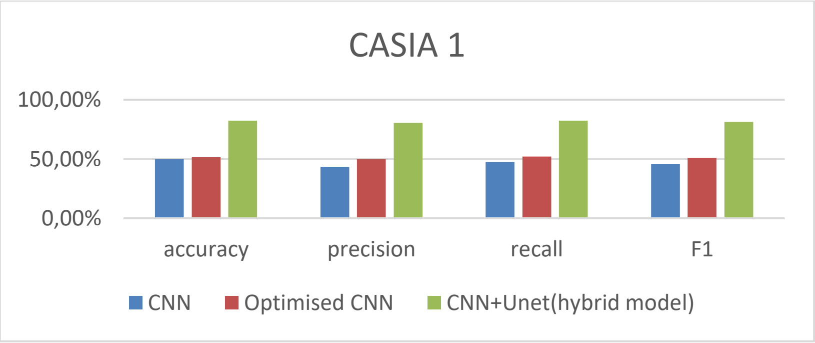


Figure 8: Graph representation of comparing various deep learning models

2. CASIA 2 evaluation metrics:

Table 3: Representing various evaluation metrics of casia 2

	accuracy	precision	recall	F1
CNN	50.68%	0.4856	0.4954	0.4905
Optimised CNN	52.01%	0.5102	0.5156	0.5129
CNN + UNet (hybrid model)	81.09%	0.8021	0.8145	0.8083

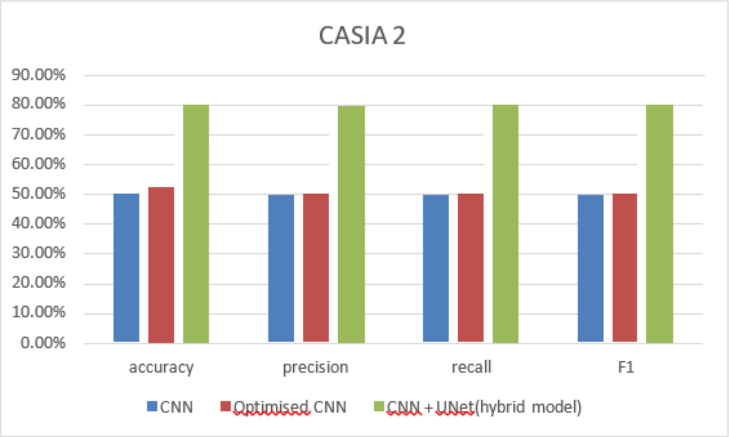


Figure 9: Graph representation of comparing various methods

3) CoMoFoD evaluation metrics:

Table 4: Representing various evaluation metrics of CoMoFoD

	accuracy	precision	recall	F1
CNN	52.35%	0.5135	0.5452	0.5292
Optimised CNN	55.58%	0.5321	0.5444	0.5382
CNN + UNet (hybrid model)	92.28%	0.9108	0.9218	0.9163

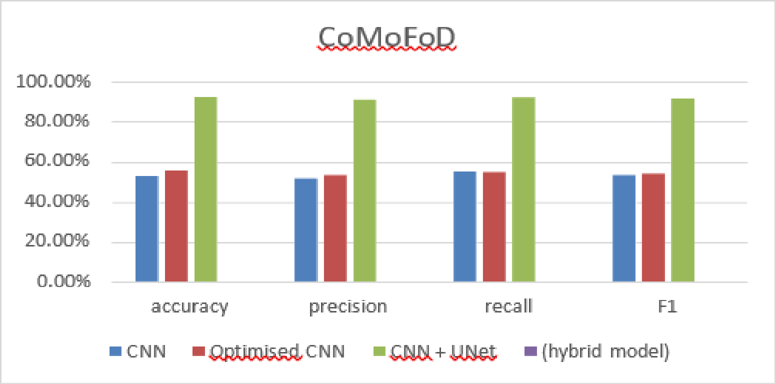


Figure 10: Graph representation of comparing various methods

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION AND FUTURE SCOPE

In this project, the two models utilized to detect weather the images have copy-move forgery or splicing forgery with the help of U-Net and CNN models. Commencing with the input image, the system generates an image, highlighting regions of interest through a comparison with re-shaped version. Subsequently, features, encompassing texture and color information, are extracted from the image. With an overall acuracy rate of 85.00% for the copy-move forgery. It even masks the images very efficiently and effectively for proper evaluation. This work can be further enhanced by the following procedures. Dataset Expansion and Complexity: Enlarge the dataset with diverse forgery scenarios, resolutions, and compression levels to strengthen the model's capability to detect a broader range of manipulations. The model can also be upgraded to detect more types of image forgeries such as Image resampling and Image retouching. Collaborate with fields like cryptography and blockchain to explore image authentication and tamper-proofing solutions, enhancing image integrity and traceability. GRAD-CAM can be used for mask generation of images without the help of U-Net architecture nor pretrained masked data. This method enhances the dataset by creating more images for increased training and testing rates.

REFERENCES

1. https://www.kaggle.com/datasets/sophatvathana/casia-dataset and http://www.vcl.fer.hr/comofod, 2021
2. N. P. Nethravathi, B. D. Austin, D. S. P. Reddy, G. V. N. S. P. Kumar, and G. K. Raju, "Image Forgery Detection Using Deep Neural Network," in Proc. 2023 6th Int. Conf. Intell. Comput. Control Syst. (ICICCS), pp. 216-221, doi: 10.1109/ICICCS54921.2023.9951952, 2023.
3. M. Zanardelli, F. Guerrini, R. Leonardi, et al., "Image forgery detection: a survey of recent deep-learning approaches," Multimed Tools Appl, vol. 82, pp. 17521–17566, 2023.
4. S. S. Ali, I. I. Ganapathi, N.-S. Vu, S. D. Ali, N. Saxena, and N. Werghi, "Image Forgery Detection Using Deep Learning by Recompressing Images," in Proc. 2019 IEEE Int. Conf. Image Process. (ICIP), Taipei, Taiwan, pp. 4046-4050, doi: 10.1109/ICIP.2019.8803393, 2019.
5. J. Ega, D. S. S. Krishna, and V. M. Manikandan, "A Review on Digital Image Forgery Detection," in Proc. 2017 IEEE Int. Conf. Signal Process., Informatics, Commun. Energy Syst. (SPICES), Kozhikode, India, pp. 1-6, doi: 10.1109/SPICES.2017.8076270, 2017.
6. N. K. Rathore, N. K. Jain, P. K. Shukla, U. S. Rawat, and R. Dubey, "Image Forgery Detection Using Singular Value Decomposition with Some Attacks," in Proc. 2018 5th Int. Conf. Signal Process., Comput. Control (ISPCC), pp. 41-46, doi: 10.1109/ISPCC.2018.8663238, 2018.
7. A. Kuznetsov, "Digital image forgery detection using deep learning approach," J. Phys.: Conf. Ser., vol. 1368, no. 3, p. 032028, doi: 10.1088/1742-6596/1368/3/032028, 2019.
8. A. Doegar, M. Dutta, and G. Kumar, "CNN based Image Forgery Detection using pre-trained AlexNet Model," in Proc. 2019 IEEE 8th Int. Conf. Commun. Electron. Syst. (ICCES), 2019, pp. 1555-1559, doi: 10.1109/ICCES46393.2019.8924430, 2019.
9. Sabeena and Dr. Lizy Abraham, "Digital image forgery detection approaches: A review and analysis," in Proc. 2nd Int. Conf. IoT, Social, Mobile, Analytics & Cloud Computing, 2023.
10. C. D. Kaur and N. Kanwal, “An analysis of image forgery detection techniques,” Stat. Optim. Inf. Comput., vol. 7, 2022.
11. M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-based image forgery detection: A review," IETE J. Educ., vol. 55, no. 1, 2022.
12. https://www.ncbi.nlm.nih.gov/books/NBK597497/figure/ch3.Fig18/, 2021
13. https://nchlis.github.io/2019_10_30/page.html, 2022

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details