Detection Of Image Forgery Using Error Level Analysis

Chandana S
Department of AI and ML
BNM Institute of Technology and Management
Bangalore, India
shivakumarchandana2002@gmail.com

Nagarathna C R
Department of AI and ML
BNM Institute of Technology and Management
Bangalore, India
nagarathna.binu@gmail.com

Amrutha A
Department of AI and ML
BNM Institute of Technology and Management
Bangalore, India
amrutha.amar21@gmail.com

Jayasri A
Department of AI and ML
BNM Institute of Technology and Management
Bangalore, India
jayasria45@gmail.com

2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) | 979-8-3503-0641-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/IITCEE59897.2024.10467523

Abstract—**Image forging is the manipulation of digital images using methods like copy-move, splicing, image removal etc. This paper provides an overview of the system's architecture, highlighting the integration of digital image processing, OpenCV, and machine learning algorithms Image forgery detection is the process of identifying a modified image from the original. In the realm of digital image processing, image forgery detection is a critical task. The amount of altered and faked photographs has increased as digital imaging has become more prevalent and is used in a variety of fields, including forensics, media, and scientific study. They must guard the veracity of photos and stop the dissemination of false information and fake news. The detection of picture forgeries, however, is fraught with technological difficulties, including the requirement for reliable and accurate image features, the capacity to differentiate between various types of image alteration, and effective algorithms that can analyze enormous quantities of digital images. To meet these problems, the error level analysis image processing technique and convolutional neural network are used to create a model that can predict the input images as forged ad unforged. The proposed model shows a better performance by giving an accuracy of 87%.**

Keywords— Error Level Analysis (ELA), Convolutional Neural Networks (CNN), Forgery Detection, Digital Image Processing, Machine Learning Algorithms.

I. INTRODUCTION

Image forgery has increased because of the widespread usage of digital images in industries such as forensic analysis, criminal investigation, surveillance systems, intelligence systems, legal services, medical imaging and many more. The widespread use of computers, the proliferation of smart devices with ever evolving cameras and image processing apps, and the fact that all these devices have made it possible for regular people to gather, store, and process vast amounts of digital visual data. The idea of image manipulation is not new; it first appeared around 1840. The earliest altered photograph was made by French photographer Hippolyte Bayard and was named “Self Portrait as a Drowned Man” in which Bayard claims to have committed himself. The use of altered photographs as material evidence in various trials and the weakening of trust in visual imagery are just two severe effects of image forgery [14]. Images can now be quickly changed without leaving any visible signs of editing because to the quick development of sophisticated image manipulation technology [11]. Good forgeries are so good that they are undetectable to the naked eye and do not show signs of tampering to conventional methods. There are two types of detection methods: active forgery detection and passive forgery detection. The digital image undergoes some sort of pre- processing in an active method, such as watermark or signatures produced when the image was created. Passive forgery further can be categorized as a dependent and independent forgery. Copying and splicing can be used to altera picture in passive forgery. As most of the people cannot discriminate the real and fake images, therefore, the importance and relevance of digital image forensics has led to establishment of different techniques for detection in image forensics.

In today’s digital world, images play a significant role in communication, journalism, and various domains. Ensuring the authenticity and trustworthiness of images is crucial for maintaining credibility and preventing the dissemination of false or misleading information. The motivation behind this research lies in promoting authenticity, trust, and ethical practices in the digital realm, while safeguarding individuals, organizations and society from the negative consequences of

image manipulations and fraudulent activities and need for reliable and efficient forgery detection techniques like copy-move, splicing, removal of parts of image etc. In conclusion, the fusion of digital image processing and machine learning algorithms offers a transformative approach to detect forgery of images.

The motivation behind this research lies in promoting authenticity, trust, and ethical practices in the digital realm, while safeguarding individuals, organizations and society from the negative consequences of image manipulations and fraudulent activities and need for reliable and efficient forgery detection techniques like copy- move, splicing, removal of parts of image etc.

The epidemic of image forgery has recently had a detrimental impact on many facets of our lives, including phone pictures, extortion, internet rumours, etc. However, most image faking situations go undetected. These days, even a layperson can alter an image without leaving any evidence that the human visual system can detect. Algorithms for spotting photos that have been altered are becoming increasingly important as editing software and the spread of

979-8-3503-0641-5/24/$31.00 ©2024 IEEE

edited images on the web both develop annually. By enabling humans to recognize and differentiate between real and altered images, image fraud techniques protect the accuracy and reliability of visual information. Identifying forgeries aids in the fight against the spread of false information and fake news. We can stop the spread of misleading narratives and make sure that proper information is communicated by confirming the authenticity of photographs. Obama and Rouhani never met face- to-face during the former's term of office, and the image of the two men tweeted by Gosar was a fake created by altering a 2011 photograph of Obama's meeting with former Indian Prime Minister Manmohan Singh.

The goal of this project is to develop a model that can recognize copy-move and splicing forgeries using machine learning and digital image processing techniques. The objective is to create a trustworthy system that can evaluate, categorize, and pinpoint photo manipulations that have been digitally altered. We approached the problem by using machine learning and neural networks to detect almost all sorts of picture alteration.

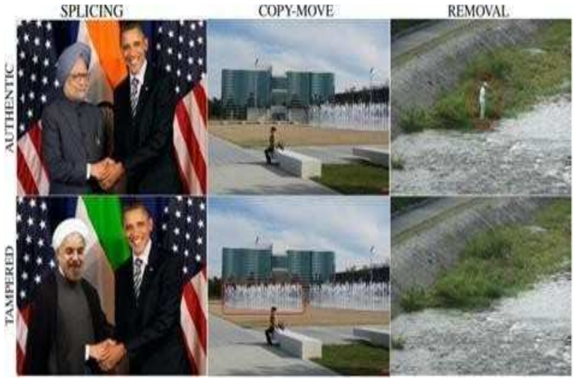

Fig 1. Example of types of Image forgery

LITERATURE SURVEY

Currently used pre-processing approaches for image fraud detection include grayscale image conversion [2], image normalization [2], image compression [4], image resizing, and super pixel segmentation [5]. Utilizing tools like CNN [4][10][8][3], LCA [13], SURF [5][9], etc., the features are extracted. Following that, the photos are categorized using methods such binary classification [6], SVM [4][12][1], and ELM. Several datasets, including Dresden [6][13], FAU [4][5], CASIA [1], and MICC- F2000[10][8], are used to assess the performance of the approaches. The techniques have a 98.95% accuracy rate. Below is a full summary of the methods that are currently in use.

In a copy-and-paste fake, a section of the image is copied and pasted into another area of the image. Copy move forgery detection (CMFD) can be performed using a variety of detection methods. In contrast to Koul, S., Kumar, M., Khurana, S.S., et al. and Goel, N., Kaur, S., Bala, R [8], the authors Nitish Kumar & Toshanlal Meenpal [12] employed SIFT and KAZE algorithms to extract the features. Discrete Cosine Transforms (DCT) based on overlapping block technology have been employed by Paul, S., Pal, A.K have used overlapping block based Discrete Cosine Transforms (DCT). C. Wang, Z. Zhang, Q. Li and X. Zhou have used SURF in combination with PCET algorithms whereas Jixiang Yang, Zhiyao Liang, Yanfen Gan, Junliu Zhong [11] have proposed a novel method using two-stage filtering which uses SURF along with SIFT. Splicing entails pasting a portion of one image onto another. It is common for the approaches employed for CMFD and image splicing detection to not overlap. Authors Muhammad Hameed Siddiqi, Khurshed Asghar, Umar Draz, Amjad Ali, Madallah Alruwaili, Yousef Alhwaiti, Saad Alanazi, M. M. Kamruzzaman, and Usman Habib[13] used Discrete Wavelet Transform (DWT) and Edge Weighted Local Binary Patterns (EW-LBP); Bo Liu, Chi-Man Punused Deep fusion network; Patrick Niyishaka and Chakravarthy Bhagvati proposed a methodology using Local Binary Pattern (LBP) and Bin Xiao, Yang Wei, Xiuli Bi, Weisheng Li, Jianfeng Maused Cascaded convolutional neural network (C2RNet) for splicing detection.

Deep learning models used in this sector undergo intricate changes, train on enormous amounts of data, and utilize pricy GPUs to perform better. According to a study by Zheng et al. (2018), it is particularly difficult to spot false news and images since it is still impossible to confirm the accuracy of news on a pure basis and because there are few models that can be used to do so. Nidhi Goel, Samarjeet Kaur, Ruchika Bala used Dual branch CNN that combines the outputs of the two CNN models [10,21]. Most of the works discussed here employ both machine learning and manually built features. This, however, is not helpful in situations where the application's reach is too broad, and the unpredictability of the incoming data cannot be foreseen.

This suggests that simple and computationally effective forgery detection methods are still required in the industry.

II. METHODOLOGY

The method used in this paper combines an error level analysis (ELA) and convolution neural network (CNN). ELA is a widely used method for locating altered areas of an image based on variations in the error levels brought on by compression. On the other hand, CNNs have great feature extraction capabilities for image analysis. ELA is a forensic method for examining photos at various levels of compression. It is predicated on the idea that a picture's compression level is not constant, and that portions that have undergone modification will have a different compression level than the remainder of the image. The original image and a compressed version of the same image are compared by ELA to determine how well it performs. CNN's underlying idea is convolution, which involves combining several filters with the input image in order to extract features. The image is then classified using the retrieved features.

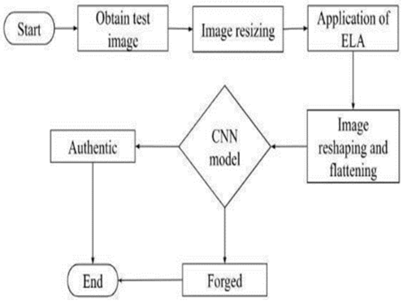

Fig 2. The proposed solution model

A. Image Acquisition

Dataset used CASIA v2.0 (CASIA2) (https://www.kaggle.com/datasets/sophatvathana/casia-dataset?resource=download). There are two types of images which should be use Authenticated images are the images which are original images without forgery. It comprises of 7492 original images. The other is Tampered images which are the forged images which has all types of forgery such as copy-move, splicing, remove there are 5125number of forged images. In total CASIA2dataset has 12,617 images. The dataset used has obtained informed consent from individuals whose images are included in the dataset and have taken steps to ensure that individuals are aware of the purpose of the study and have given explicit permission for the analysis of their images. Only the necessary data for the study is considered, avoiding unnecessary intrusion into individuals' private lives. We have made efforts to ensure that the dataset used for training and testing is representative and unbiased.

B. Image preprocessing

The identification of image forgeries depends heavily on image preprocessing. Our process reduces the size of the photographs to 90% of the original size because we are utilizing two different types of images in the dataset, and then the reduced image is stored as resaved in a different folder to discover anomalies and then compare them with the original image using the CNN model. For applying ELA, the captured images are shrunk and then made grayscale. Our method shrinks the photographs to 90% of their original size before saving them as newly saved.

C. Error Level Analysis (ELA)

We create a method called img_difference that requires both the original and the saved versions of the image. The photos are subjected to error level analysis. List form is obtained for the edge discrepancies between the images. From this, the greatest difference is obtained. The image is perfect or real if the maximum difference is 0. In the event where the maximum difference is 0, we set it to 1 in order to show the edges of the perfect image in white. The discrepancies in altered photos are otherwise visible in the photograph. To produce a crisper result, we additionally improve the brightness and sharpness of the image.

D. Preparing dataset for CNN Model

We apply ELA to all of the photos and flatten them to prepare the dataset for the CNN model. After being flattened, the image is then kept in a list. Additionally, we keep a list with the image labels. The resulting dataset is divided into training and testing datasets. 80% of the data were utilized for training, and 20% were used for testing. Utilizing the image's labels, the split is stratified.

E. Building the CNN Model

The data is initially molded into a 128*128 RGB picture. In order to develop the neural network model layer by layer, we establish a sequential model object. A convolutional layer with 32 filters, each with a 3x3 kernel size, is then added. ReLU is the activation function in use. The image's input shape is set to (128, 128, 3). By choosing the largest value within each pool, the max-pooling layer, which has a pool size of 2x2, decreases the spatial dimensions of the input. ReLU activation is added, followed by a max- pooling layer with a 2x2 pool size and another convolutional layer with 64 filters and a 3x3 kernel size. The 3D feature map is flattened toa 1D vector using an additional layer. To process the flattened feature vector acquired from the preceding layer, a fully connected layer with 64 units/neurons and ReLU activation is added. Finally, a dense layer with two units and SoftMax activation is implemented. Two classifications (Forged and not forged) are predicted by this layer, which produces the classification result.

F. Compiling the CNN Model

To update the model weights during training, the Adam optimizer is employed when building the CNN model. It is an adaptive optimization technique that modifies the learning rate according to the magnitudes of the gradients. Measurement of the discrepancy between expected probability and actual labels is done using the categorical cross-entropy loss function. The performance of the model is tracked using accuracy measures throughout training and evaluation. It figures out what percentage of all samples are accurately predicted out of the total samples. 15 epochs of the CNN model are run.

G. Testing a new instance

By using ELA, a new picture is predicted to be fabricated or not. This is followed by flattening and resizing the image to 1128*128 pixels. A new form is applied to the flattened image before it is sent to the model for forecasting. Two values are given by the forecast. If the first value is higher than the second value, the image is not forged; otherwise, it is.

If the image is faked, coloured lines will be drawn around the image's edges to draw attention to them. If the image is original, the edges will be highlighted in white lines. For the altered photos, it even draws attention to the forged part by making it darker.

III. RESULTS

The proposed approach successfully determined the ELA between the original and scaled images. The features retrieved from the ELA were used to train the CNN model, which also produced results with great accuracy. The model's effectiveness is assessed based on its precision, recall, and accuracy.

The fig 3 shows the authentic image which we are displaying the error level analysis. After error level analysis we flatten the image and resize it and we pass it to the CNN model it tells weather the image is forged or not forged.

The fig 4 illustrate the tampered image where copy move tampering is done for the image. So, after applying the CNN model it is detecting the forged part and saying that the image is forged.

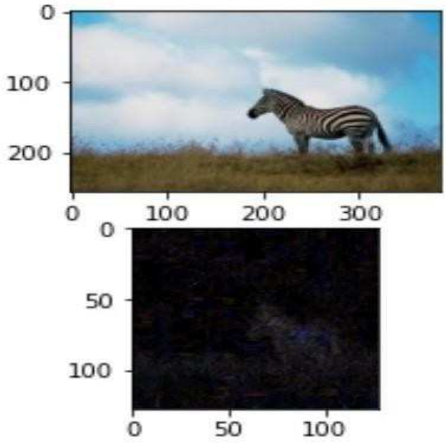

Fig 3. Result for non-forged image

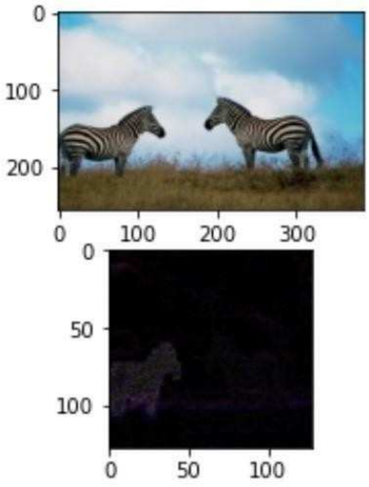

Fig 4: Result for Forged Image

The highest accuracy obtained by the model is 97.18% on the training data and 87.75% on the test data and it is showing in table 1.

TABLE 1: PERFORMANCE TABLE

	Accuracy score	Precision score	Recall score
Train set	0.9718	0.9620	0.9825
Test set	0.8775	0.8911	0.86

The accuracy of the model and the loss over the 15 epochs are represented in the graph below:

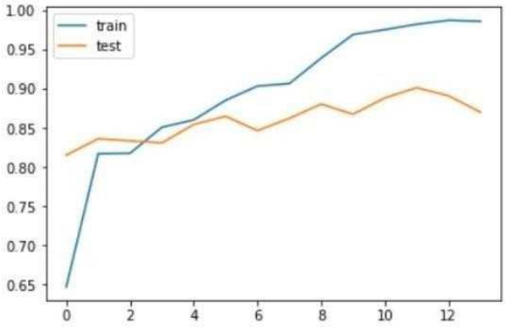

Fig 5: Variation in Accuracy for train and test

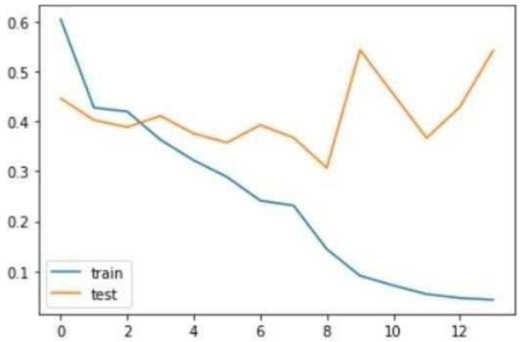

Fig 6: Variation in Loss for train and test

Adversarial testing was conducted, where the model was subjected to intentionally manipulated images designed to deceive it. The model exhibited a certain degree of resilience, accurately detecting forged regions even in the presence of sophisticated adversarial manipulations. The model maintained its high accuracy when applied to datasets such as CAT-Net compRAISE datasets with varied characteristics and manipulation techniques.

IV. CONCLUSION

Image forgery detection is an extremely difficult subject to solve. We must be able to distinguish between authentic and altered photographs in this age of technological innovation. In this paper, we suggested an approach for detecting image forgeries that is based on deep learning. The suggested model is based on the combination of ELA (Error Level Analysis) and CNN (Convolutional Neural Networks), where this combination analyses images through various levels of compression and other delivers great features for image analysis. As a result, the architecture is more effective, and the model's complexity and training time were lowered. On the CASIA v2 Dataset, we assessed the suggested architecture. With the CASIA v2 dataset, we were able to detect forgeries with an accuracy of 97.15 percent. The comparison findings between the suggested system and the existing approaches demonstrate its superiority. The proposed approach will assist in the area of picture manipulation detection and also pave the way for further investigation into detecting other sorts of image forgery modifications.

REFERENCES

[1] A. Ghoneim, G. Muhammad, S. U. Amin and Gupta, "Medical Image Forgery Detection for Smart Healthcare," in IEEE Communications Magazine, vol. 56, no. 4, pp. 33-37, April2018, doi: 10.1109/MCOM.2018.1700817

[2] alZahir, S., Hammad, R. “Image forgery detection using image similarity.” Multimed Tools Appl 79, 28643 –28659(2020).

https://doi.org/10.1007/s11042- 020-09502-4.

[3] Bo Liu, Chi-Man Pun, “Exposing splicing forgery in realistic scenes using deep fusion network”, Information Sciences, Volume 526, 2020, Pages 133-150, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2020.03.099.

[4] Boubacar Diallo, Thierry Urruty, Pascal Bourdon, Christine Fernandez- Maloigne, “Robust forgery detection for compressed images using CNN supervision,” Forensic Science International: Reports, Volume 2, 2020, 100112, ISSN 2665-9107, https://doi.org/10.1016/j.fsir.2020.100112

[5] C. Wang, Z. Zhang, Q. Li and X. Zhou, "An Image Copy-Move Forgery Detection Method Based on SURF and PCET," in IEEE Access, vol. 7, pp. 170032-170047, 2019, doi:10.1109/ACCESS.2019.2955308.

[6] F. Marra, D. Gragnaniello, L. Verdoliva and G. Poggi, "A Full-Image Full- Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," in IEEE Access, vol. 8, pp. 133488-133502, 2020, doi: 10.1109/ACCESS.2020.3009877.

[7] F. Matern, C. Riess and M. Stamminger, "Gradient-Based Illumination Description for Image Forgery Detection," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1303-1317, 2020, doi: 10.1109/TIFS.2019.2935913.

[8] Goel, N, Kaur, S, Bala, R. "Dual branch convolutional neural network for copy move forgery detection". IET Image Process. 2021; 15:656–665. https://doi.org/10.1049/ipr2.12051

[9] Jixiang Yang, Zhiyao Liang, Yanfen Gan, Junliu Zhong, "A novel copy-move forgery detection algorithm via two-stage filtering", Digital Signal Processing, Volume 113, 2021, 103032, ISSN1051051-2004, https://doi.org/10.1016/j.dsp.2021.103032

[10] Koul, S., Kumar, M., Khurana, S.S. et al. "An efficient approach for copy-move image forgery detection using convolution neural network". Multimed Tools Appl 81, 11259–11277(2022). https://doi.org/10.1007/s11042-022-11974- 5

[11] Nitish Kumar & Toshanlal Meenpal (2022) "Salient keypoint-based copy–move image forgery detection", Australian Journal of

Forensic Sciences, DOI: 10.1080/00450618.2021.2016964

[12] Njood Mohammed AlShariah and Abdul Khader Jilani Saudagar, "Detecting Fake Images on Social Media using Machine Learning" International Journal of Advanced Computer Science and Applications (IJACSA), 10 (12), 2019. http://dx.doi.org/10.14569/IJACSA.2019.001 2 2 4

[13] O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1762-1777, July 2018, doi:10.1109/TIFS.2018.2799421.

[14] Paul, S., Pal, A.K. "A fast copy-move image forgery detection approach on a reduced search space". Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-022- 14224-w

[15] Nagarathna C R, Jayasri A, Chandana S, Amrutha A. "Identification of Image Forgeries using Machine Learning - A Review". Journal of Innovative Image Processing,5(3),323-336. doi:10.36548/jiip.2023.3.007