iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59317

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 12 Issue III Mar 2024- Available at www.ijraset.com

Image Forgery Detection using ResNet50

Nalluri Brahma Naidu[1], Thokala Kavyasree[2], Tadikonda Ravi Teja[3], Pulimela Sushma Sarayu[4], Sivangula Sai[5]
[1]*Associate Professor,* [2,3,4,5]*UG Students, Department of CSE, Vasireddy Venkatadri Institute of Technology (Autonomous), Guntur, AP*

Abstract: ***Image forgery detection is crucial in ensuring the integrity of digital media. In this study, we propose a method for detecting image tampering using Error Level Analysis (ELA) and Convolutional Neural Networks (CNNs) with a ResNet50 architecture. Leveraging the CASIA 2.0 Image Tampering Detection Dataset, which consists of authentic (Au) and tampered (Tp) images, along with metadata and annotations provided in the CASIA 2 Ground truth dataset, we develop and evaluate our model. The dataset comprises 7492 authentic images, 5125 tampered images, and 5123 files of ground truth information. ELA transformations highlight compression discrepancies, aiding in the identification of tampered regions. Our ResNet50-based CNN model, augmented with Global Average Pooling, Dense layers, and Dropout regularization, is trained using Adam optimization and binary cross-entropy loss with early stopping. Evaluation metrics, including training and validation loss/accuracy curves and confusion matrices, are used to assess model performance. The trained model is saved for future use and tested on new images to demonstrate its classification capabilities. Our approach achieves a significant level of accuracy in distinguishing between authentic and tampered images, underscoring its potential for practical image forgery detection applications and contributing to advancements in digital media forensics***

Keywords: Image forgery detection, Error Level Analysis, Convolutional Neural Networks, ResNet50 architecture, CASIA 2.0

I. INTRODUCTION

It is a truth that the digital universe is acquiring tremendous prominence these days. Thus, visual content's authenticity and trustworthiness are on the rise. With the ever-increasing involvement of Photoshop, a responsible different professional must always have the ability to differentiate between the unaltered pictures and the ones which are modified, be it the professionals from the fields of law enforcement, journalism, science, or art. It is undoubtedly the most critical aspect of the overall concern. The foundations of information trustworthiness must be preserved at all costs.

Today's imaging forensic investigators not only employ cutting-edge technological innovations and advanced algorithms but also calls on their instincts which are tied to the realism of the image whether the images have been "enhanced" or "authentic." The creation of nuanced datasets and advances in deep learning make it possible that the contention with replica visual effects will able to be carried on. The main purpose of forgery detection in images is to maintain credibility of digital information in order to create a foundation of digital visual being trustworthy.

In our project, deep convolutional neural networks equipped with a high precision scheme for image forgery detection have been developed by us. This system is very accurate at the task of distinguishing between original images and forgeries which are intentionally compressed and use ELA artifacts which represent data dissimilarly. Our process is accompanied by discovering the pictures from certain places, re-sizing them for that very purpose, building EA representations, and after that, preprocessing the data. We selected ResNet50, which is a deep neural network architecture with a good transfer learning properties, as our base model. During training, there is Adam optimization and the cross-entropy loss function with early stopping that is utilized to prevent overfitting. The trained model is then put to the test using the validation dataset, which is used to determine the consistency and the precision of the model's results to produce excellent results.To make the detection algorithm for image forgery more accurate and efficient, we plan to explore several methods. It encompasses several approaches, such as designing better backbones, post-processing images via a wide library of authentic and tampered dataset, and tuning pre-trained models like ResNet50 via transfer learning. In our process, we make use of the "CASIA 2.0 Image Tampering Detection Dataset" for our input data, which can be divided into three major directories. The directory has a heap of real images and covers a spectrum of visual patterns and this is a reliable source of data for both the training and validation processes. It has the "Groundtruth" folder with 5123 files for reference and the "Tampered Images" directory with 5125 files demonstrating doctored visuals. Employing these methodology solutions coupled with the development methods of the latest deep learning technology, we seek to not only enhance the system reliability and accuracy but also extend its working fields and make it routine in many scenarios and environments while pushing forward the advancement of the worldwide fight against falsification and fallaciousness on the net.

II. LITERATURE REVIEW

In the age of digitalization, images are the strongest way of expression and representation. The authenticity of these systems is of significance to preserving the truthfulness and the reality of the information they communicate.Fake pictures can lead to a wrongful accusing, judicial problems, and ethical troubles. Detecting image manipulation helps a justice system to be effective and ethical since it prevents any kind of abuses during lawful or media proceedings and discussion.Image forgery detection then becomes a necessity for the sake of the authenticity of digital images in a scenario with the fast progress of computer manipulations when the manipulation can be harmful enough.

Studies on digital image forgery detection techniques, such as those conducted by Navpreet Kaur Gill, Ruhi Garg, and Er. Amit Doegar, [3] provide valuable insights into the challenges and advancements in the field. Their critical analysis of active and passive methods offers a foundation for understanding the complexities involved in detecting manipulated images, which directly informs the development of our project's detection algorithms.

Similarly, the systematic examination by B. Santhosh Kumar, S. Karthi, K. Krathika, and Rajan Cristin [2] sheds light on the methodologies and approaches used in image forgery detection. Understanding these methodologies enhances our understanding of both active and passive detection techniques, guiding our project's implementation and methodology section.

Authors Yuan Rao and Jiangqun Ni [1] introduce a new method for detecting image forgery using deep learning. Their approach utilizes a convolutional neural network (CNN) to automatically learn hierarchical representations from RGB color images, specifically for tasks like identifying image splicing and copy-move alterations. Unlike traditional methods, the authors initialize the network's first layer weights with a basic high-pass filter derived from the spatial rich model (SRM) instead of random initialization. This regularization technique helps suppress the influence of image contents while capturing subtle tampering artifacts. The pre-trained CNN then acts as a patch descriptor to extract dense features from test images, followed by feature fusion for SVM classification..

Authored by A. Kuznetsov [9], presented an algorithm designed to detect splicing, a prevalent form of digital image forgery. The approach is centered around utilizing the VGG-16 convolutional neural network architecture. The proposed algorithm processes image patches, determining whether they originate from original or forged sources. During training, emphasis is placed on selecting patches from original image regions and splicing borders. Experimental validation conducted using the CASIA dataset showcases the algorithm's efficacy in detecting splicing, without specifying accuracy metrics.

Authors N. B. A. Warif, M. Y. I. Idris, A. W. A. Wahab, and R. Salleh [8] delve into the intricate domain of digital image forensics, driven by the escalating sophistication of image tampering techniques. Their study focuses on the pivotal Error Level Analysis (ELA) technique, particularly in the context of the widely adopted Joint Photographic Experts Group (JPEG) image format. As JPEG remains the prevalent format supported by a myriad of devices and applications, it becomes a prime target for tampering activities. The authors meticulously evaluate ELA's efficiency across various types of image tampering, including JPEG compression, image splicing, copy-move, and image retouching.Moreover, by exploring ELA's performance across multiple forms of image tampering, the authors shed light on its versatility and applicability in real-world scenarios. This comprehensive evaluation underscores ELA's potential as a robust tool for detecting and analyzing tampered images, thereby advancing the state-of-the-art in digital image forensics.

Authors Hajar Moradi-Gharghani and Mehdi Nasri [11]tackle the formidable challenge of digital image forgery detection in their paper.

They propose a novel block-based method specifically designed to detect tampered regions in cases of copy-move forgery. The method involves extracting feature vectors using Discrete Cosine Transform (DCT) from non-overlapping blocks of the image. These feature vectors are then lexicographically sorted, enabling the identification of copied blocks based on certain criteria.

III. METHODOLOGIES

An image forgery detection model is developed, utilizing the cameras, a diverse set of forged and authentic images are captured to establish a foundational database for image forgery detection. Leveraging the ResNet50 model architecture with convolutional neural networks, the model learns intricate patterns within images to discern between authentic and forged content. By means of analyzing ELA (Error Level Analysis) images, the model reveals the difference in levels of compression that makes it possible to tell if an image is forgery.

This systems of categorization and classification allows the model to analyze and decide whether the image is false or not making amends of categorization as well as accuracy.

A. Structure of image forgery detection model

The model's operational flow is illustrated through a block diagram. Initially, the model receives datasets comprising images of forged and authentic content as input. The images undergo preprocessing steps, including resizing and noise reduction, to enhance their quality and clarity. Subsequently, the dataset is partitioned into training and validation subsets.The ResNet50 model architecture is then trained on the training dataset, leveraging convolutional neural networks to learn intricate patterns within the images. Performance metrics are applied to evaluate the model's efficacy in distinguishing between authentic and forged content.

1) *Dataset:* The dataset consists of images containing both authentic and forged examples. These images are used to train and validate the image forgery detection model.

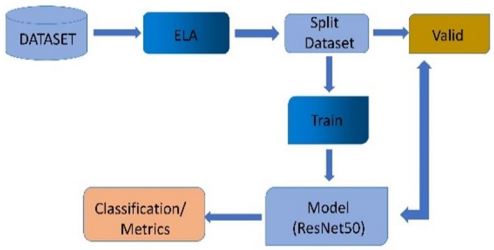


Fig. 1. Block diagram of proposed model

2) *ELA (Error Level Analysis):* ELA is applied to the images as part of the preprocessing step. It helps highlight areas of discrepancies in compression levels, aiding in the identification of potential image forgeries.
3) *Dataset Split:* The training set and the validation set are the two subsets that make up the dataset. The validation set is used to assess the model's performance during training, while the training set is used to train the ResNet50 model.
4) *Train-Validate:*The training dataset is used to train the ResNet50 model. Based on the attributes taken from the ELA photos, the model learns during training to differentiate between real and fake images. The purpose of the validation dataset is to keep an eye on the model's performance and guard against overtime.
5) *Model (ResNet50)*: ResNet50, a pre-trained convolutional neural network architecture, is utilized as the backbone for feature extraction. The model's parameters are fine-tuned using the image forgery dataset to adapt to the specific task of detecting image forgeries.
6) *Classification:* Once trained, the ResNet50 model is employed to classify new images as either authentic or forged. The model assigns a probability score to each class, enabling the identification of potential image manipulations or forgeries.
7) *Train_Valid split:* Splitting the data into training and validating sets based on the user's split ratio occurs after all preparation procedures have been completed. Afterwards, the models will be trained using this split train data, and validated using the valid data.

B. Structure of Resnet-50 model using CNN:

ResNet-50 is a specific type of CNN architecture that comprises 50 convolutional layers. Like other CNN designs, ResNet-50 undergoes training using the backpropagation technique to minimize a loss function that measures the disparity between predicted outputs and actual labels.

Here's how the training process for ResNet-50 unfolds:

1) *Data Preparation:* Input data, typically consisting of photographs, undergo preprocessing to standardize pixel values and enhance data diversity, thereby enriching the training dataset.
2) *Model Initialization:* ResNet-50's initial weights are randomly assigned, and these weights are adjusted during training iterations to enhance the network's performance.
3) *Forward Pass*: The layers of the ResNet-50 network are fed with input images. To evaluate the predicted accuracy of the model, the output activations of the final layer are compared with the real-world labels.
4) *Backward Pass:* In order to maximize the weights within the network, the difference between the expected and actual outputs is passed backwards through the network. Till the loss function converges to a minimum value, this process is repeated across a number of epochs.

5) *Evaluation:* The model's ability to make accurate predictions and its generalization performance are evaluated using a validation set..

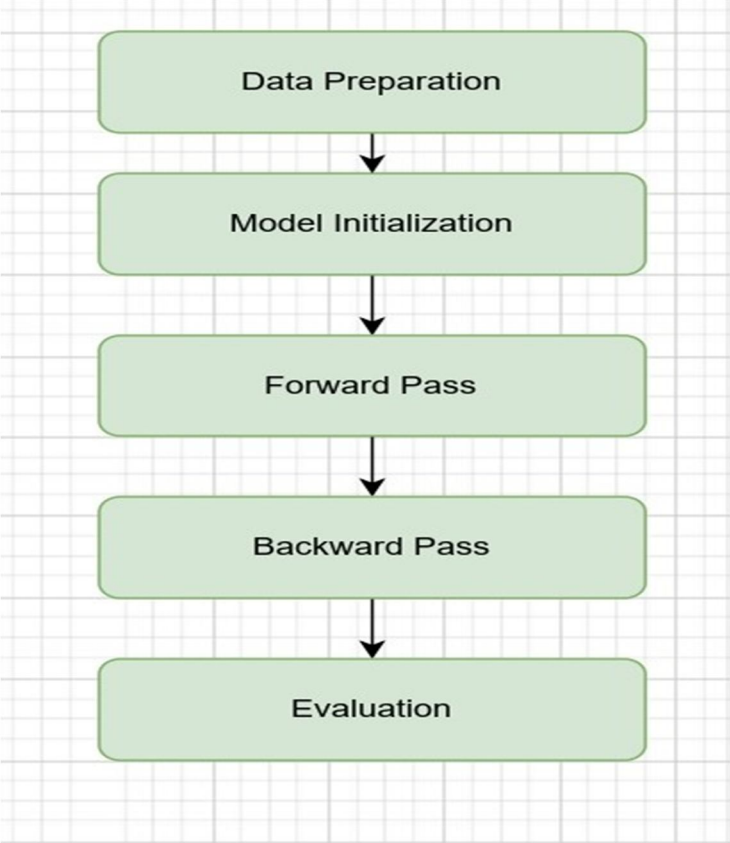


Fig. 2. CNN based resnet50

C. Image preprocessing

In this paper, the neural network is not trained by the transfer learning method at first. Ultimately, the accuracy of the training set was 90%. However, the loss trend and the results of the final test set make it clear that an over-fitting phenomenon exists. Analysis has shown that the most likely reason is the comparatively small size of the data collection.

Although data improvement helps the issue of uneven distribution to some extent, it does not entirely resolve the issue of over-fitting. This research then applies transfer learning to this data set. The training process will be carried out using the standard network; effective training only requires a slight tweak to the model.To sum up, transfer learning might result in higher initial accuracy, faster convergence speed and more accurate approximation accuracy for model.

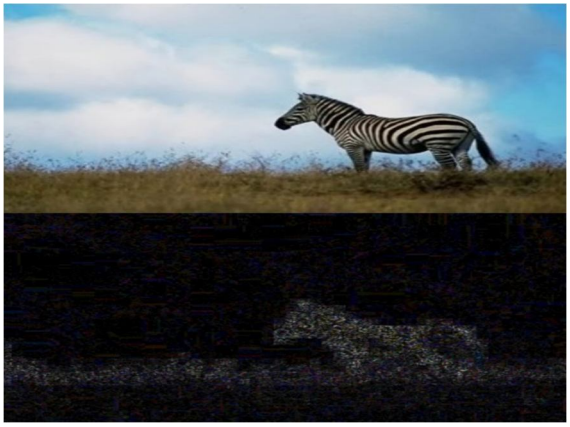


Fig. 3. Sample Picture before and after ELA

D. Convolutional Neural Systems

Convolutional Neural Networks (CNNs) are the main component of our detection system in our image forgery detection project. Our CNN architecture included convolutional, pooling, and fully linked layers, all of which were painstakingly designed. Convolutional layers were used to extract complex characteristics from the input images, while pooling layers were used to minimize spatial dimensions in order to avoid overfitting. We accurately predicted the legitimacy of the images by utilizing completely connected layers. Moreover, the incorporation of ResNet50, a pre-trained network, improved feature extraction, resulting in remarkable precision in distinguishing genuine from manipulated photos.

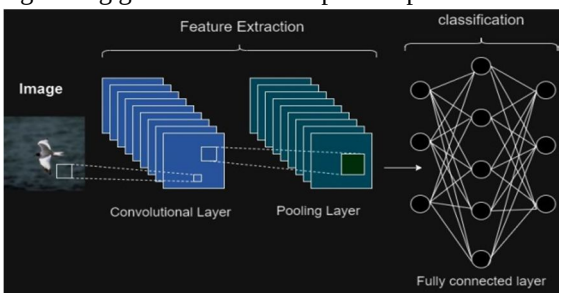


Fig. 4. CNN architecture for forgery detection

The Keras framework was used to implement the CNN model's perpetuation. The model was a convolutional neural network (CNN) architecture consisting of two fully connected layers after three convolutional layers. The input images were resized to 128x128 pixels and normalized. The convolutional layers consisted of 128 filter with a kernel size of 3x3, followed by max-pooling layers. ReLU activation functions were applied throughout the convolutional layers. The first fully connected layer had 512 neurons with a dropout probability of 0.5 to mitigate overfitting. The subsequent fully connected layer utilized a softmax activation function with output nodes corresponding to the number of classes in the dataset.Training was conducted for 100 epochs with early stopping based on validation loss. To enhance the model's capabilities, transfer learning was employed using the ResNet-50 architecture. The pre-trained weights of the ResNet-50 model were frozen during training to prevent overfitting.

E. Resnet50 architecture

ResNet50 is a powerful deep-learning model architecture commonly utilized in image processing tasks, including image forgery detection, object recognition, and scene understanding. It belongs to the ResNet family of models and is distinguished by its depth, consisting of 50 layers with residual connections.The architecture's deep layers enable it to capture both low-level and high-level features, making it adept at identifying subtle inconsistencies indicative of image manipulation or forgery.

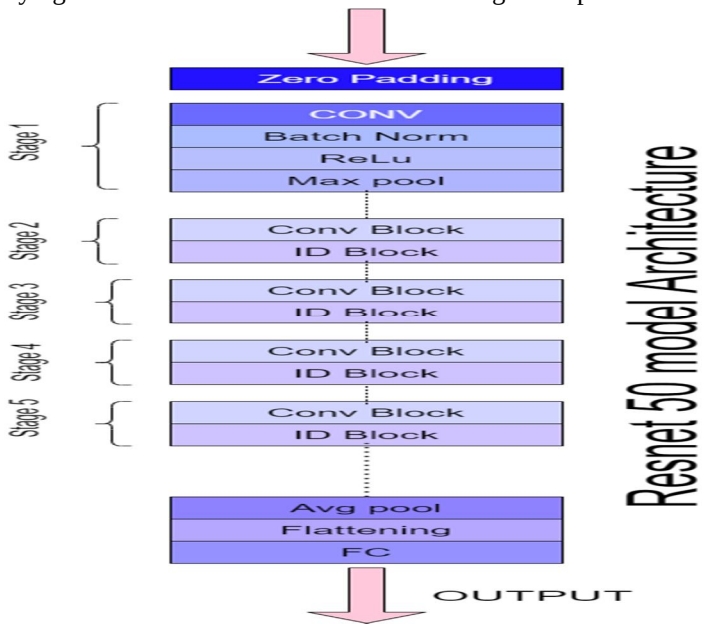


Fig. 5. Resnet50 architecture

In this project, the feature extraction process relies on a pre-trained ResNet50 model. Initially, the ResNet50 model is loaded, leveraging its capacity to capture a wide array of visual features from images. The crucial step involves extracting features from the final convolutional layer of the ResNet50 model. These features serve as rich representations of the input images. Subsequently, a fully connected neural network is constructed to process these extracted features and predict image labels effectively. To augment the diversity of the training dataset and improve model robustness, various data augmentation techniques are applied. These techniques include image flipping, both horizontally and vertically, and adjusting the brightness of images. During the training phase, the weights of the ResNet50 model are frozen to retain the learned features and prevent overfitting of the model.Once the model is trained, the selection process begins to identify the best-performing model based on validation accuracy. The CNN model consists of four layers: Conv1, ReLu(Rectified Linear Unit), POOL_1 (Pooling Layer), and FC1(Fully connected layer).

Conv1: The Conv1 layer serves as the initial stage in processing the input images to identify potential forged areas. This layer applies filters, typically small squares of information such as [3 x 3], to the input images. As the filters move across the image, they capture features and patterns pixel by pixel, reconstructing the image's components. The convolution operation involves multiplying the filter values with the corresponding pixel values in the image and summing them up.

$$(a * b) = \int_{-\infty}^{\infty} a(\tau) g(t-\tau) d\tau \qquad (1)$$

In the image forgery detection project, common activation functions such as ReLU (Rectified Linear Unit) or sigmoid functions may be used to achieve the non-linear response.

$$f(a) = \frac{e^a}{sum(e^a)} + In\left(\frac{1}{1+e^{-x}}\right) \qquad (2)$$

Pooling Layer: Uses techniques like L2 and normal connections to reduce border numbers in huge images; the maximum splice is the most popular use. Using a 2x2 channel size and stride length, it extracts the maximum value from each sub-circle and stacks the plates appropriately.

IV. IMPLEMENTATION

Each epoch is a full pass over the training dataset during the training of a machine learning model. The model is updated using an optimization approach such as gradient descent, which modifies the neural network weights to minimize the difference between the expected and actual outputs. The total number of epochs is a hyperparameter that may be adjusted to enhance the model's performance.

The model achieved a test loss of approximately 0.286 and a test accuracy of approximately 96.46% over 100 epochs. These metrics indicate that your model performed quite well on the test dataset. A low loss value and a high accuracy value suggest that your model's predictions are accurate and consistent with the ground truth lables.

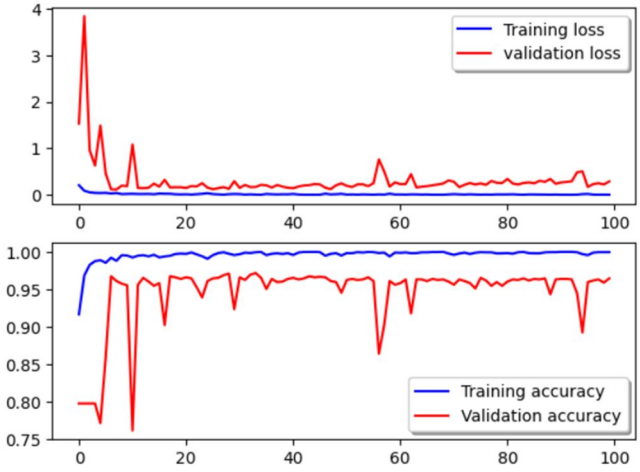


Fig. 6. Plotting Graph for accuracy

The model's predictions are thoroughly broken down in the confusion matrix, which differentiates between true positives (accurately predicted real images), true negatives (accurately predicted fake images), false positives (real images wrongly predicted as fake), and false negatives (fake images incorrectly predicted as real). By emphasizing particular kinds of prediction errors, it helps assess the model's performance and pinpoint areas in need of development.

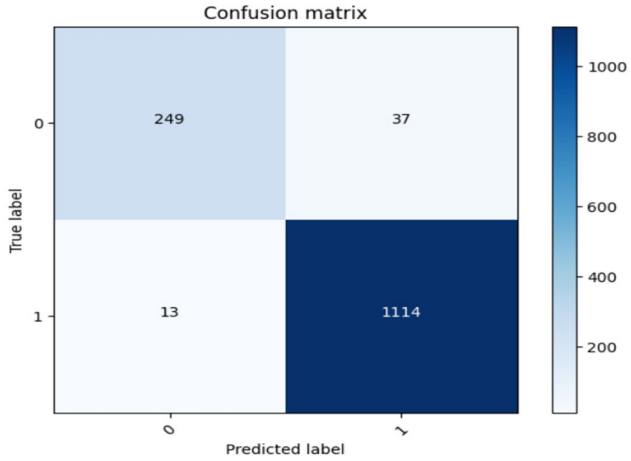


Fig. 7. Confusion matrix

Upon uploading an image to the model, the user interface enables detection of whether the image is forged or authentic. Following the upload, the system provides a detailed outcome indicating whether the image is fake or genuine, along with the corresponding confidence level expressed as a percentage.

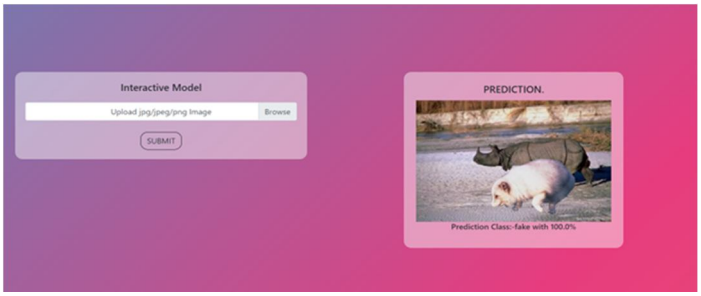


Fig. 8. Output for uploaded picture for fake.

Upon analysis, the system confidently asserts that the image provided is 100% authentic and has not undergone any form of forgery or alteration.

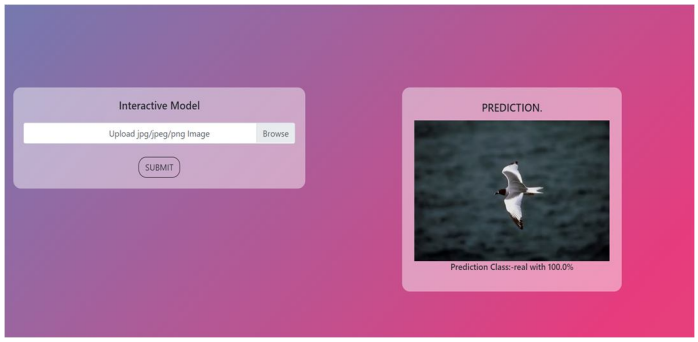


Fig. 9. Output for 100% real image

V. CONCLUSIONS

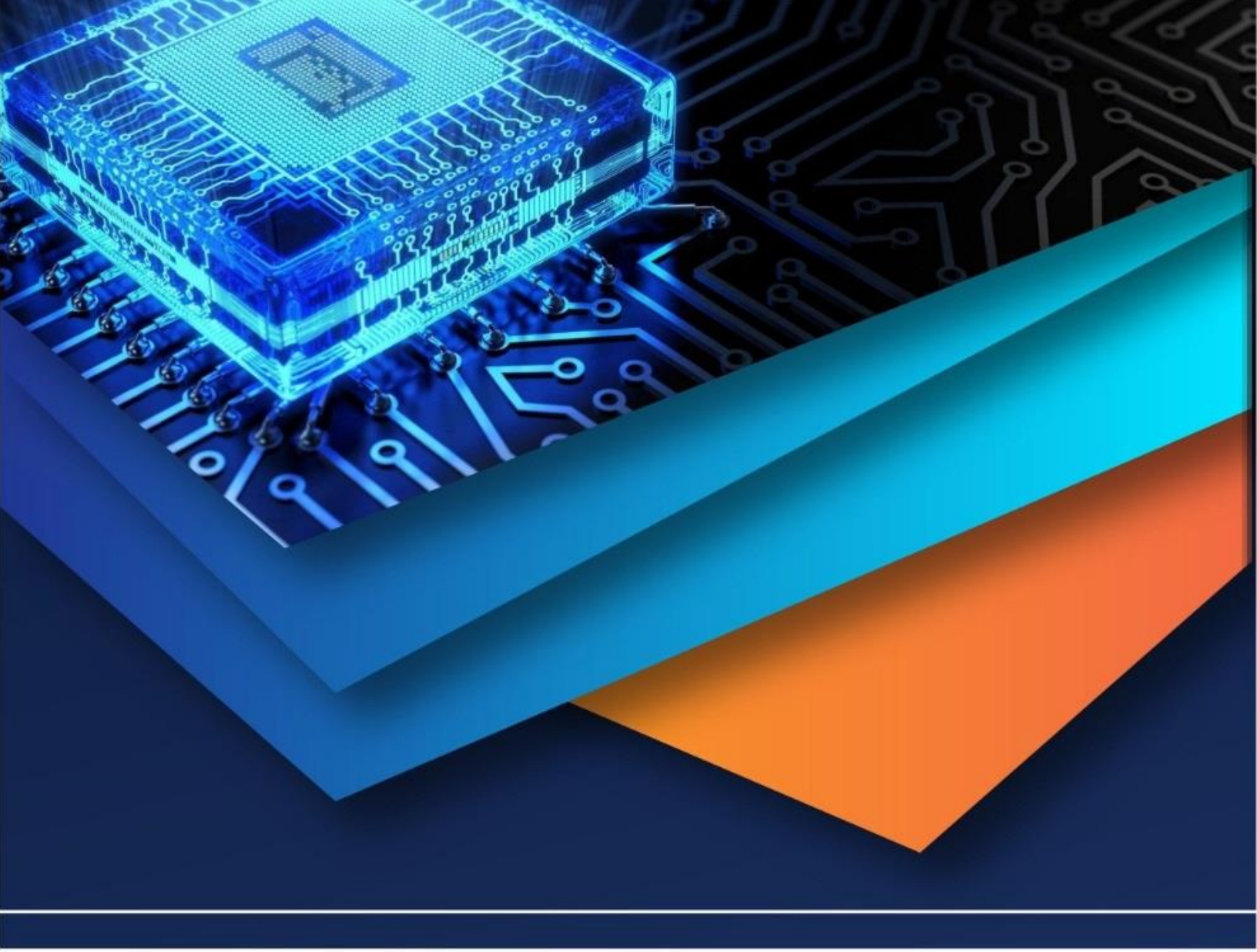
In conclusion, our project successfully achieved its objective of detecting forged images with high accuracy using ResNet50 as the underlying model. Through rigorous training and validation, we established a robust system capable of differentiating between authentic and forged images with confidence. The implementation of ResNet50, coupled with extensive data preprocessing and augmentation techniques, enabled us to attain a commendable level of accuracy in identifying forged content. Moving forward, the insights gained from this project could be instrumental in enhancing the security and authenticity of digital imagery across various domains.

VI. FUTURE WORK

1) *Advanced Model Architectures:* Experiment with more advanced neural network architectures beyond ResNet50, such as DenseNet, EfficientNet, or custom architectures tailored to specific characteristics of forged images.
2) *Expanding Dataset and Diversity:* Continuously expand and diversify the dataset used for training to encompass a broader range of forgery types, image qualities, and manipulation techniques encountered in real-world scenarios**.**
3) *Deployment and Integration:* Deploy the model into user-friendly applications and integrate it into existing platforms for seamless integration into forensic analysis tools, social media platforms, and image-sharing website.

REFERENCES

[1] Yuan Rao, Jiangqun Ni, ”A Deep Learning Approach to Detection of Splicing and copy-move forgeries in Images”, IEEE international workshop on Information Forensics and security doi:10.1109/ WIFS.2016. 7823911, 2016.
[2] B.Santhosh Kumar, S. Karthi, K. Karthika, and Rajan Cristin, “A Systematic study of Image Forgery Detection,” Vol. 15, pp. 2560-2564, Aug 2018.
[3] Navpreet Kaur Gill, Ruhi Garg, Er. AMit Doegar, ”A review paper on Digital Image Forgery Detection”, July 2017.
[4] Hany Farid, "Image forgery detection," Signal Processing Magazine, IEEE, vol. 26, pp. 16-25, 2009.
[5] Gajanan K Birajdar and Vijay H Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, pp. 226-245, 2013.
[6] Anushka Singh,Jyotsna Singh ,”Image Forgery Detection using Deep Neural Network,”January 2022, doi:10.1109/SPIN52536.2021.9565953.
[7] T.A.Kohale,S.D.Chede and P.R.Lakhe,”Forgery detection technique based on block and feature based method”,International Journal of Advanced research in computer and communication Engineering.,pp.7334-7335, 2014.
[8] Nor Bakiah Abd Warif, Mohd. Yamani Idna Idris, Ainuddin Wahid Abdul Wahab, Rosli Salleh, ” An Evaluation of Error Level Analysis in Image Forensics,IEEE International Conference on System and Technology, doi:10.1109/ICSEngT .20157412439 , August 2015.
[9] A Kuznetsov, “Digital image orgery detection using deep learning approach”,doi:10.1088/1742-6596/1368/3/032028 , 2019.
[10] C.Bayar, and M. C. Stamm. “A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer,” in Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, 2016, pp. 5–10.
[11] Hajar Moradhi-Gharghani, Mehdi Nasri,”A New Block-based Copy-Move Forgery Detection Method in Digital Images”,International Conference on Communication and Signal Processing, April 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY